DISERTASI – EE186601

SKEMA SECRET KEY GENERATION (SKG) UNTUK KEAMANAN PADA SISTEM KOMUNIKASI DI LINGKUNGAN WIRELESS

MIKE YULIANA
07111660010005

Dosen Pembimbing
Dr. Ir. Suwadi, MT.
Dr. Ir. Wirawan, DEA.

Departemen Teknik Elektro
Fakultas Teknologi Elektro
Institut Teknologi Sepuluh Nopember
2019

DISERTASI – EE186601

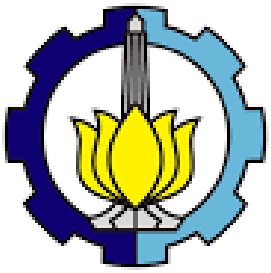
SKEMA *SECRET KEY GENERATION* (SKG) UNTUK KEAMANAN PADA SISTEM KOMUNIKASI DI LINGKUNGAN WIRELESS

MIKE YULIANA
07111660010005

Dosen Pembimbing
Dr. Ir. Suwadi, MT.
Dr. Ir. Wirawan, DEA.

Departemen Teknik Elektro
Fakultas Teknologi Elektro
Institut Teknologi Sepuluh Nopember
2019

--Halaman ini sengaja dikosongkan--



DISERTASI – EE186601

SECRET KEY GENERATION (SKG) SCHEME FOR COMMUNICATION SYSTEM SECURITY IN WIRELESS ENVIRONMENT

MIKE YULIANA
07111660010005

Supervisor
Dr. Ir. Suwadi, MT.
Dr. Ir. Wirawan, DEA.

Department of Electrical Engineering
Faculty of Electrical Technology
Institut Teknologi Sepuluh Nopember
2019

--Halaman ini sengaja dikosongkan--

PERNYATAAN KEASLIAN DISERTASI

Yang bertanda tangan dibawah ini :

Nama	: Mike Yuliana
Program Studi	: Teknik Elektro
NRP	: 0711166001005

Dengan ini menyatakan bahwa isi sebagian maupun keseluruhan disertasi dengan judul:

SKEMA *SECRET KEY GENERATION* (SKG) UNTUK KEAMANAN PADA SISTEM KOMUNIKASI DI LINGKUNGAN *WIRELESS*

Adalah benar-benar hasil karya intelektual mandiri, diselesaikan tanpa menggunakan bahan-bahan yang tidak diijinkan dan bukan merupakan karya pihak lain yang saya akui sebagai karya saya sendiri.

Semua referensi yang dikutip maupun dirujuk telah ditulis secara lengkap pada daftar pustaka.

Apabila ternyata pernyataan saya ini tidak benar, saya bersedia menerima sangsi sesuai peraturan yang berlaku.

Surabaya, 13 Agustus 2019

Yang membuat pernyataan

Mike Yuliana

NRP. 0711166001005

--Halaman ini sengaja dikosongkan--

LEMBAR PENGESAHAN DISERTASI

Disertasi disusun untuk memenuhi salah satu syarat memperoleh gelar
Doktor (Dr.)
di
Institut Teknologi Sepuluh Nopember
Oleh:

MIKE YULIANA
NRP: 07111660010005

Tanggal Ujian: 12 Juli 2019
Periode Wisuda: September 2019

Disetujui oleh:
Pembimbing:

1. Dr. Ir. Suwadi, MT ..... .
   NIP: 196808181993031002

2. Dr. Ir. Wirawan, DEA .....
   NIP: 196311091989031011

Penguji:

1. Prof.Dr.Ir.Dadang Gunawan, M.Eng .....
   NIP: 195810141985031005

2. Prof.Ir.Gamantyo Hendrantoro, M.Eng, Ph.D .....
   NIP: 197011111993031002

3. Dr.Ir.Achmad Affandi, DEA .....
   NIP: 196510141990021001

Kepala Departemen Teknik Elektro
Fakultas Teknologi Elektro

Dr. Eng. Ardyono Priyadi, ST., M.Eng.
NIP: 197309271998031004

--Halaman ini sengaja dikosongkan--

SKEMA *SECRET KEY GENERATION* (SKG) UNTUK KEAMANAN PADA SISTEM KOMUNIKASI DI LINGKUNGAN *WIRELESS*

Nama Mahasiswa : Mike Yuliana
NRP : 07111660010005
Pembimbing : Dr. Ir. Suwadi, MT
Dr. Ir. Wirawan, DEA

ABSTRAK

Skema *Secret Key Generation* (SKG) yang mengeksploitasi sifat *reciprocity* dan keacakan kanal *wireless* untuk membangkitkan *secret key* telah menjadi area penelitian yang semakin menarik dan menjanjikan. Terdapat 3 permasalahan utama dalam pembangunan skema SKG yang efisien yang harus diatasi, yaitu *trade-off* antara parameter performansi *Key Disagreement Rate* (KDR) dan *Key Generation Rate* (KGR), tingginya kompleksitas implementasi karena banyaknya tahapan yang harus dilalui, serta tidak efisiennya skema SKG yang dibangun sehingga tidak sesuai jika diimplementasikan pada perangkat *Internet of Things*(IoT) yang memiliki keterbatasan sumber daya. Disertasi ini berkontribusi dalam mengatasi ketiga permasalahan tersebut. Kontribusi pertama yang dilakukan untuk mengatasi *trade-off* antara parameter performansi KDR dan KGR adalah didapatkannya kombinasi yang optimal antara metode pra proses yaitu Kalman Filter, *Modified Polynomial Regression* (MPR), serta *Savitzky Golay Filter* dan kuantisasi multilevel. Hasil yang didapat adalah penurunan KDR dan peningkatan KGR dibandingkan dengan skema yang eksisting. Kontribusi kedua dari disertasi ini adalah mekanisme penyederhanaan skema SKG dengan kombinasi metode *Modified* Kalman (MK) serta *Combined Multilevel Quantization* (CMQ) sehingga bisa dihasilkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi. Hasil pengujian yang dilakukan menghasilkan 4 blok 128-bit data di lingkungan tanpa halangan serta 2 blok 128-bit data yang memiliki KDR sebesar 0 sehingga tidak memerlukan koreksi untuk mendapatkan *secret key* yang identik. Kontribusi ketiga dari disertasi ini adalah didapatkannya skema SKG *Signal Strength Exchange* (SSE) yang efisien dalam hal waktu komputasi dan *overhead* komunikasi dengan menggunakan metode *Synchronized Quantization* (SQ) sebagai bagian dari skema SKG SSE. Hasil yang didapat menunjukkan penurunan waktu komputasi menjadi sebesar 3.8% dan *overhead* komunikasi menjadi sebesar 34% skema yang eksisting. Kontribusi yang dihasilkan dalam disertasi ini diharapkan dapat menjadi salah satu solusi alternatif pembentukan kunci simetris yang tidak membutuhkan kompleksitas komputasi serta *Trusted Third Party* (TTP), sehingga cocok jika digunakan pada berbagai aplikasi IoT.

Kata kunci : SKG, *reciprocity*, efisien, pra proses, kuantisasi multilevel.

--Halaman ini sengaja dikosongkan--

SECRET KEY GENERATION (SKG) SCHEME FOR COMMUNICATION SYSTEM SECURITY IN WIRELESS ENVIRONMENT

By	:	Mike Yuliana
Student identity Number	:	07111660010005
Supervisor	:	Dr. Ir. Suwadi, MT
		Dr. Ir. Wirawan, DEA

ABSTRACT

Secret Key Generation (SKG) schemes that exploit the reciprocity and randomness of wireless channels have become increasingly interesting and promising areas of research. There are three main problems that must be solved in the development of an efficient SKG scheme, i.e. the performance parameters trade-off between Key Disagreement Rate (KDR) and Key Generation Rate (KGR), the high complexity of implementation because of the many stages that must be passed, and inefficient SKG scheme so that it is not suitable for the Internet of Things (IoT) device that has limited resources. This dissertation contributes to solving these three problems. The first contribution is the optimal combination of pre-processing methods, i.e. Kalman Filter, Modified Polynomial Regression (MPR), and Savitzky Golay Filter with multilevel quantization to overcome the trade-off between KDR and KGR performance parameters. The results obtained were a decrease in KDR and an increase in KGR compared to the existing scheme. The second contribution is the simplification mechanism of the SKG scheme with a combination of the Modified Kalman (MK) method and the Combined Multilevel Quantization (CMQ) so that identical secret keys can be produced without going through the information reconciliation stage. The results of the conducted tests are four 128-bit blocks of data in an unobstructed environment and two 128-bit blocks of data in an obstacle environment that had a KDR value of 0 so that it did not require correction to get an identical secret key. The third contribution is the acquisition of a Signal Strength Exchange (SSE) SKG scheme that is efficient in terms of computing time and communication overhead using the Synchronized Quantization (SQ) method as part of the SSE SKG scheme. The results show a decrease in computing time up to 3.8% and communication overhead up to 34% compared to existing schemes. The contribution in this dissertation is expected to be one of the alternative solutions for a symmetrical key generation that does not require computational complexity and Trusted Third Party (TTP) so that it is suitable for use on various IoT applications.

Keyword: SKG, *reciprocity*, efficient, pre-processing method, multilevel quantization.

--Halaman ini sengaja dikosongkan--

KATA PENGANTAR

Puji syukur ke hadirat Allah Subhanahu Wa Ta'ala yang telah memberikan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan disertasi ini yang merupakan hasil penelitian selama menempuh studi program doktor di Departemen Teknik Elektro Fakultas Teknologi Elektro, Institut Sepuluh Nopember Surabaya. Tak lupa pula teriring salam dan shalawat selalu tercurah pada Nabi Muhammad Shallallahu 'alaihi Wa Sallam.

Pada kesempatan kali ini, penulis mengucapkan terima kasih yang tulus kepada Bapak Dr. Ir. Suwadi, MT dan Bapak Dr. Ir. Wirawan, DEA selaku promotor dan co-promotor yang telah membimbing, memotivasi, mengarahkan, dan mendorong untuk menyelesaikan disertasi ini. Ucapan terima kasih juga penulis sampaikan kepada Bapak Prof. Dr. Ir. Dadang Gunawan, M.Eng, Bapak Prof. Ir. Gamantyo Hendrantoro, M.Eng., Ph.D, dan Dr. Ir. Achmad Affandi, DEA selaku tim penguji yang memberikan saran dan masukan pada disertasi ini.

Penulis juga menyampaikan terima kasih pada pihak manajemen Pascasarjana, yaitu Bapak Dr. Ir. Wirawan, DEA dan Bapak Dr. Rony Seto Wibowo, ST, MT selaku koordinator dan sekretaris Program Studi Pascasarjana Teknik Elektro ITS serta staf administrasi Bapak Hartono. Ucapan terima kasih juga disampaikan pada Politeknik Elektronika Negeri Surabaya yang telah memberikan ijin dan kesempatan untuk menempuh program doktor. Tidak lupa Kementrian Riset, Teknologi dan Pendidikan Tinggi Republik Indonesia (Kemristekdikti) serta Kementrian Keuangan Republik Indonesia yang telah memberikan bantuan dan beasiswa Lembaga Pengelola Dana Pendidikan (LPDP) selama menempuh program doktor ini.

Terima kasih penulis ucapkan pada Ketua Departemen Teknik Elektro, Ketua Program Studi Teknik Telekomunikasi serta seluruh dosen Teknik Telekomunikasi Politeknik Elektronika Negeri Surabaya (PENS) atas dukungan serta motivasinya. Penulis juga mengucapkan terima kasih pada teman-teman di Laboratorium

Telekomunikasi Multimedia ITS dan Laboratorium Komunikasi Digital PENS yang tidak bisa penulis sebutkan satu persatu atas dukungan, motivasi serta bantuannya selama tiga tahun terakhir. Tidak lupa penulis sangat berterima kasih pada suamiku David Noor Mubarok, permata hatiku Helga Anindya Mubarok dan Naila Khansa Yumna, Ayahku Nurhasan, Ibuku Eny Sutiyarti, serta seluruh keluargaku. Tidak ada satu katapun yang dapat mewakili terima kasihku atas segala pengertian, pengorbanan, kasih sayang dan doa yang telah diberikan untuk penulis selama ini.

Surabaya, 13 Agustus 2019

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

--Halaman ini sengaja dikosongkan--

DAFTAR NOTASI

y^A	Parameter kanal RSS yang diukur oleh Alice
y^B	Parameter kanal RSS yang diukur oleh Bob
y^E	Parameter kanal RSS yang diukur Eve dari Alice
$y^{E'}$	Parameter kanal RSS yang diukur Eve dari Bob
$R_{y^u}(t,\Delta)$	*Autocorrelation Function (ACF)*
$\rho_{y^A y^B}$	Koefisien korelasi Pearson
$\sigma^2_{y^u}$	Varian
μ_{y^u}	Rata-rata
r_p	*Probing rate*
r_s	*Sampling rate*
T_c	*Coherence time*
x_k	Estimasi parameter kanal RSS hasil pengukuran
A	Matrik nxn yang menunjukkan *state* di waktu sebelumnya
u	Kontrol input
B	Matrik nxl yang menunjukkan opsional kontrol input
H	Matrik mxn yang menunjukkan *state* pengukuran pada waktu sekarang
w_k	*Noise* proses
v_k	*Noise* pengukuran
Q	Kovarian *noise* proses
R	Kovarian *noise* pengukuran
$\hat{x}_k^-$	Estimasi parameter kanal apriori
P_k^-	*Error* kovarian apriori
K_k	Kalman Gain
$\hat{x}_k$	Estimasi parameter kanal aposterori
P_k	*error* kovarian aposteriori
z	Parameter kanal hasil *pre process*
a_m	Koefisien Polinomial
m	Orde Polinomial
L	Jumlah level kuantisasi
C	Jumlah ekstraksi bit

$Q(y)$	Mekanisme kuantisasi parameter kanal
K^u	*Preliminary key*
S^u	*Synchronized key*
ε^u	*Secret key*
Key^u	Rangkaian bit hasil sinkronisasi

DAFTAR SINGKATAN

TTP	*Trusted Third Party*
SKG	*Secret Key Generation*
RSS	*Received Signal Strength*
KDR	*Key Disagreement Rate*
LDPC	*Low-density parity-check*
BCH	Bose-Chaudhuri-Hocquenghem
KGR	*Key Generation Rate*
DoS	*Denial of Service*
IoT	*Internet of Thing*
PLS	*Physical Layer Security*
CSI	*Channel State Information*
CIR	*Channel Impulse Response*
CFR	*Channel Frequency Response*
UWB	*Ultra Wideband*
NICs	*Network Interface Cards*
USRP	*Universal Software Radio Peripheral*
WARP	*Wireless Open-Access Research Platform*
ACF	*Autocorrelation Function*
TDD	*Time Division Duplexing*
DSSS	*Direct Sequence Spread Spectrum*
FHSS	*Frequency Hopping Spread Spectrum*
MMB	*Modified Multi Bit*
MAQ	*Multi-bit Adaptive Quantization*
PRNG	*Pseudo-Random Number Generator*
NIST	*National Institute of Standards and Technology*
AP	*Access Point*
Ack	*Acknowledgement*
SNR	*Signal to Noise Ratio*

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perangkat *wireless* telah berkembang sangat pesat dalam beberapa tahun terakhir ini. Tidak seperti komunikasi yang tradisional, perangkat *wireless* dapat berkomunikasi dengan perangkat yang lain dalam jangkauan tertentu. Hal ini menyebabkan komunikasi *wireless* rentan terhadap adanya serangan, karena semua perangkat lain yang berada dalam jangkauan pemancar dapat juga dapat menerima sinyal dari pemancar tersebut. Karenanya penyadapan merupakan salah satu masalah keamanan utama dalam komunikasi *wireless*. Secara intuitif, komunikator akan berbagi *secret key* sehingga komunikasi yang dilakukan dapat diacak dan aman dari penyadap.

Pendekatan tradisional untuk membangkitkan *secret key* kebanyakan didasarkan pada skema pra-distribusi kunci (skema enkripsi simetris) dan kriptografi kunci publik (skema enkripsi asimetris). Pada pra-distribusi kunci dibutuhkan *trusted third party* (TTP) untuk membangkitkan, memelihara, dan mendistribusikan *secret key* dengan komunikator. Skema tersebut memiliki kompleksitas yang tinggi untuk jaringan *wireless* dengan skala yang besar, karena dibutuhkannya distribusi kunci yang intensif untuk mendukung pembentukan kunci antar setiap pasang *node*. Di sisi lain pendekatan kunci publik biasanya membutuhkan kompleksitas komputasional. Misal, Algoritma Diffie-Helman (Wei dkk, 2013), yang merupakan algoritma kriptografi paling popular untuk membentuk *secret key* antara dua pengguna, membutuhkan operasi eksponensial dengan jumlah yang besar. Sehingga algoritma tersebut tidak cocok jika digunakan untuk membangun *secret key* pada perangkat *wireless* yang *low end* (memiliki daya tahan baterai yang rendah dan kemampuan komputasi yang terbatas). Hal inilah yang menjadi dasar lahirnya penelitian metode-metode yang tidak menggunakan kunci publik. Kriptografi Quantum (Bregman, 2008) adalah salah satu contoh inovasi yang tidak menggunakan kunci publik. Kriptografi tersebut menggunakan hukum dari teori

kuantum, terutama prinsip ketidakpastian Heisenbeirg, untuk *sharing* kunci antara dua perangkat. Meskipun aplikasi kriptografi Quantum telah mulai ada beberapa tahun terakhir ini, namun mereka masih sangat jarang dan mahal.

Solusi yang lebih murah dari permasalahan tersebut adalah skema *Secret Key Generation* (SKG) yang menggunakan keacakan dari kanal *wireless* sebagai sumber ekstraksi bit *secret key* antar pengguna (Premnath dkk, 2013; Mathur dkk, 2008; Ren dkk, 2011). Skema tersebut mengeksploitasi sifat *reciprocity*, keacakan, dan keunikan lokasi dari kanal *wireless fading*, sehingga mendapatkan korelasi kanal yang tinggi dan bisa digunakan untuk menghasilkan *secret key*. *Received Signal Strength* (RSS) merupakan salah satu jenis kanal *wireless* yang banyak digunakan sebagai sumber ekstraksi untuk membangkitkan *secret key* dalam berbagai implementasi dan eksperimen (Guillaume dkk, 2015). Pada penelitian ini, kami menggunakan RSS sebagai parameter pembangkitan *secret key* karena mudah didapat dengan menggunakan *wireless driver* yang sudah ada tanpa modifikasi, dan kebanyakan perangkat *wireless* juga memiliki kemampuan untuk melakukan pengukuran RSS.

Secara umum terdapat 4 tahap yang digunakan untuk membangkitkan *secret key*, dimana tahap tersebut meliputi *channel probing*, kuantisasi, rekonsiliasi informasi, serta *privacy amplification*. Tahap *channel probing* bertujuan untuk mendapatkan sejumlah RSS yang akan diekstrak menjadi *secret key*. RSS yang didapat akan dikonversi menjadi bit pada tahap kuantisasi. Akibat pengukuran yang *half duplex* maka dimungkinkan timbulnya perbedaan bit yang dihasilkan di kedua pengguna dan tahap rekonsiliasi informasi digunakan untuk melakukan koreksi terhadap perbedaan tersebut. Terdapat 2 proses yang dilakukan pada tahap *privacy amplification* yaitu proses perubahan bit hasil rekonsiliasi ke dalam bentuk bit yang memenuhi persyaratan keacakan serta proses verifikasi. Proses verifikasi dilakukan untuk memastikan bahwa *secret key* yang digunakan adalah identik antara kedua pengguna. Kelemahan dari penggunaan 4 tahap SKG ini adalah tingginya ketidakcocokan bit yang dihasilkan antara dua pengguna (Ambekar dkk, 2012). Ketidakcocokan bit tersebut ditunjukkan dengan parameter *Key Disagreement Rate* (KDR).

Salah satu upaya yang dapat dilakukan untuk mengatasi permasalahan tersebut adalah penambahan metode *post* proses setelah kuantisasi (Mathur dkk, 2008). Metode tersebut bekerja dengan mencari beberapa bit yang berurutan sepanjang parameter tertentu dan menggantinya dengan bit 1 atau 0. Hasil yang didapat menunjukkan penurunan yang signifikan dari KDR antara pengguna namun kecepatan pembangkitan kunci yang ditunjukkan dengan parameter *Key Generation Rate* (KGR) juga mengalami penurunan secara signifikan. Peneliti lain (Ambekar dkk, 2015; Yuliana dkk, 2017b) menggunakan metode pra proses yang diletakkan sebelum kuantisasi untuk mengurangi KDR. Metode ini bekerja dengan cara mengolah RSS hasil pengukuran sebelum kuantisasi menggunakan beberapa pendekatan diantaranya *curve fitting* (Ambekar dkk, 2012), filtering (Ali dkk, 2010), serta Kalman Filter (Ambekar dkk, 2015). Hasil yang didapat menunjukkan peningkatan *reciprocity* yang diukur dengan koefisien korelasi Pearson. Semakin tinggi nilai koefisien korelasi Pearson yang didapat maka semakin rendah nilai KDR yang diperoleh. Namun beberapa penelitian menunjukkan adanya metode pra proses yang digabung dengan kuantisasi yang berisi single bit sehingga KGR yang didapat tidak optimal.

Peningkatan parameter KGR dapat dilakukan dengan menggunakan kuantisasi multilevel (Patwari dkk, 2010; Liu dkk, 2014; Jana dkk, 2009; Ambekar dkk, 2015; Zhang dkk, 2017; Zeng dkk, 2010), namun peningkatan parameter tersebut juga diikuti dengan peningkatan KDR. Beberapa penelitian menggabungkan metode pra proses tersebut dengan kuantisasi multi level (Ambekar dkk, 2015; Ambekar dkk, 2012; Guillaume dkk, 2015) sebagai salah satu upaya untuk mengatasi *trade-off* parameter performansi KDR dan KGR. Keterbatasan dari penelitian tersebut adalah perbandingan performansi dilakukan terhadap kuantisasi yang berisi *single* bit dan multi bit, dimana perbandingan ini bukan merupakan perbandingan yang setara karena KGR yang dihasilkan pasti lebih banyak kuantisasi yang berisi multi bit. Beberapa metode pra proses (Patwari dkk, 2010; Jiang dkk, 2018) juga membutuhkan waktu komputasi yang tinggi karena kompleksnya proses yang harus dilakukan sehingga akan mengurangi nilai KGR. Hal inilah yang mendasari diperlukannya penelitian lanjutan tentang

kombinasi metode pra proses serta kuantisasi multi level yang optimal sehingga mampu mengatasi *trade-off* parameter performansi antara KDR dan KGR dari skema SKG yang dibangun.

Dari beberapa penelitian yang memanfaatkan metode pra proses terlihat bahwa pemanfaatan metode ini dapat meningkatkan *reciprocity* dan mengurangi ketidakcocokan bit yang dihasilkan sehingga mampu menurunkan KDR antara kedua pengguna. Namun salah satu kelemahan dari penambahan metode tersebut adalah semakin tingginya waktu komputasi yang dibutuhkan jika dibandingkan dengan skema SKG yang eksisting karena semakin banyaknya tahapan yang harus dilalui serta masih adanya perbedaan bit dari kunci yang dihasilkan sehingga masih dibutuhkan tahap rekonsiliasi informasi untuk melakukan koreksi terhadap perbedaan bit yang dihasilkan. Peningkatan waktu komputasi dari tahap tersebut sangat dipengaruhi oleh banyaknya ketidakcocokan bit antara kedua pengguna serta keberhasilan pengiriman *parity*. Semakin banyak ketidakcocokan bit maka waktu yang dibutuhkan untuk melakukan koreksi juga semakin lama. Keberhasilan pengiriman *parity* juga sangat dipengaruhi oleh kondisi jaringan. Jika jaringan putus atau buruk maka waktu yang dibutuhkan untuk pengiriman *parity* juga semakin lama. Dari segi keamanan, pertukaran *parity* juga memicu bocornya informasi ke penyadap sehingga mempermudah penyadap untuk mendapatkan *secret key* yang sama. Hal ini memicu upaya untuk membangun skema SKG yang sederhana dengan menghilangkan tahap rekonsiliasi informasi namun tetap mampu menghasilkan kunci yang identik antara kedua pengguna.

Beberapa penelitian lain fokus pada upaya untuk membangun skema SKG pada perangkat *Internet of Things* (IoT) yang merupakan perangkat dengan keterbatasan sumber daya (Zhang dkk, 2017; Guillaume dkk, 2015; Margelis dkk, 2018; Zenger dkk, 2015). Penelitian tersebut menggunakan 5 tahap dengan adanya penambahan tahap pra proses dengan tujuan untuk mengurangi ketidakcocokan bit antara dua pengguna yang dinyatakan dengan KDR. Namun dibandingkan dengan (Yuliana dkk, 2019a), peneliti yang menggunakan 5 tahap dalam pembangkitan kunci cenderung

lebih tidak efisien karena adanya penambahan tahap pra proses serta rekonsiliasi informasi yang akan meningkatkan waktu komputasi. Semakin tinggi nilai KDR yang dihasilkan maka semakin tinggi waktu komputasi yang dibutuhkan karena semakin banyak blok data yang harus dikoreksi. Peneliti (Yuliana dkk, 2019) memodifikasi metode pra proses dengan melakukan kombinasi metode Regresi Polinomial dengan Kalman Filter yang telah dimodifikasi untuk meningkatkan *reciprocity* parameter kanal RSS serta menghilangkan tahap rekonsiliasi informasi. Pra proses dilakukan di setiap blok data yang masing-masing berisi 128 parameter kanal. Hasil pengujian yang dilakukan menunjukkan bahwa pemanfaatan modifikasi pra proses tersebut mampu untuk menghasilkan 128 bit *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi. Namun metode tersebut membutuhkan waktu komputasi yang tinggi karena dilakukan di setiap blok data. Semakin banyak data maka semakin tinggi pula waktu komputasi yang dibutuhkan. Parameter performansi yang sering digunakan untuk menentukan performansi dari skema SKG yang dibangun meliputi koefisien korelasi, KDR, KGR serta keacakan. Beberapa penelitian tentang skema SKG untuk perangkat IoT (Guillaume dkk, 2015; Sudarsono dkk, 2018) juga menggunakan parameter tersebut untuk menentukan performansi dari skema yang dibangun. Seharusnya beberapa parameter seperti waktu komputasi dan *overhead* komunikasi juga digunakan untuk menentukan efisiensi dari sistem yang dibangun. Semakin rendah waktu komputasi dan *overhead* komunikasi yang dihasilkan maka semakin efisien skema yang dibangun sehingga sesuai untuk perangkat IoT. Dengan semakin berkembangnya kebutuhan akan keamanan komunikasi perangkat IoT mendorong pentingnya penelitian lanjutan untuk menghasilkan skema SKG yang lebih efisien dan sesuai untuk perangkat IoT.

Penelitian ini ditujukan untuk mengatasi 3 permasalahan utama dalam pembangunan skema SKG yang efisien. Permasalahan tersebut meliputi *trade-off* antara parameter performansi KDR dan KGR, tingginya kompleksitas implementasi karena banyaknya tahapan yang harus dilalui, serta tidak efisiennya skema SKG yang dibangun sehingga tidak sesuai jika diimplementasikan pada perangkat IoT yang

memiliki keterbatasan sumber daya. Skema SKG yang efisien ditunjukkan dengan berkurangnya tahapan yang harus dilalui untuk mendapatkan *secret key* sehingga mampu mengurangi waktu komputasi serta *overhead* komunikasi. Skema yang efisien tersebut sangat sesuai jika diimplementasikan pada perangkat IoT yang memiliki keterbatasan sumber daya.

1.2 Perumusan Masalah

Peningkatan *reciprocity* parameter kanal yang ditunjukkan dengan peningkatan nilai koefisien korelasi belum signifikan sehingga perlu dilakukan pengembangan terhadap metode pra proses yang eksisting. Selain itu pemanfaatan kuantisasi multilevel akan meningkatkan KGR namun peningkatan tersebut juga akan diikuti dengan peningkatan KDR. Dibutuhkan pengembangan metode pra proses serta investigasi yang lebih detil untuk mendapatkan kombinasi optimal dari metode pra proses dengan kuantisasi multilevel sehingga dapat mengatasi *trade-off* parameter performansi KDR dan KGR.

Tingginya kompleksitas implementasi karena banyaknya tahapan yang harus dilalui serta adanya tahap rekonsiliasi informasi memicu meningkatnya waktu komputasi. Semakin banyak ketidakcocokan bit yang dihasilkan maka waktu yang dibutuhkan untuk melakukan koreksi juga semakin lama. Keberhasilan pengiriman *parity* juga sangat dipengaruhi oleh kondisi jaringan. Jika kondisi jaringan putus atau buruk maka waktu yang dibutuhkan untuk pengiriman *parity* juga semakin lama. Dibutuhkannya skema SKG yang lebih sederhana dengan menghilangkan tahap rekonsiliasi namun tetap dapat menghasilkan *secret key* yang identik antara kedua pengguna .

Tidak efisiennya skema SKG yang dibangun karena tingginya waktu komputasi yang dibutuhkan serta banyaknya *overhead* komunikasi yang digunakan untuk sinkronisasi antara kedua pengguna mengakibatkan tidak sesuainya skema tersebut jika diimplementasikan pada perangkat IoT. Untuk itu perlu didesain skema SKG yang efisien dengan mengurangi tahapan yang dilakukan untuk mendapatkan *secret key*

sehingga mampu mengurangi waktu komputasi yang dibutuhkan. Sedangkan pengurangan *overhead* komunikasi dilakukan dengan menghilangkan tahap rekonsiliasi informasi sehingga tidak ada pengiriman *parity* serta mengurangi tahap sinkronisasi yang dilakukan antara kedua pengguna.

Berdasarkan ketiga permasalahan tersebut, maka perumusan masalah dari penelitian ini meliputi :

1. Upaya untuk mendapatkan kombinasi optimal dari metode pra proses dan kuantisasi multilevel sehingga dapat mengatasi *trade-off* parameter performansi KDR dan KGR.
2. Mekanisme pengembangan metode pra proses sehingga mampu meningkatkan *reciprocity* secara signifikan dan menghasilkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi.
3. Efisiensi skema SKG yang dalam hal waktu komputasi dan *overhead* komunikasi sehingga sesuai jika diimplementasikan perangkat IoT dengan keterbatasan sumber daya.

1.3 Tujuan dan Manfaat Penelitian

1.3.1 Tujuan Penelitian

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Mendapatkan kombinasi yang optimal dari metode pra proses dan kuantisasi multilevel sehingga dapat mengatasi *trade-off* parameter performansi KDR dan KGR.
2. Menyederhanakan tahapan skema SKG sehingga bisa didapatkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi.
3. Mendesain skema SKG yang efisien sehingga bisa mengurangi waktu komputasi dan *overhead* komunikasi dan sesuai untuk diimplementasikan pada perangkat IoT dengan keterbatasan sumber daya.

1.3.2 Manfaat Penelitian

Manfaat dari penelitian ini adalah didapatkannya referensi untuk kombinasi yang optimal dari metode pra proses dan kuantisasi multilevel sehingga dapat dijadikan acuan dalam pengembangan skema SKG. Selain itu penyederhanaan tahapan pembangkitan *secret key* serta efisiensi dari skema SKG yang dibangun juga dapat dijadikan acuan dalam peningkatan keamanan komunikasi perangkat IoT. Secara umum luaran dari penelitian ini diharapkan dapat menjadi salah satu solusi alternatif pembentukan kunci simetris yang tidak membutuhkan kompleksitas komputasi serta TTP, sehingga cocok jika digunakan pada berbagai aplikasi IoT.

1.4 Kontribusi dan Orisinalitas Penelitian

Kontribusi dan originalitas dari penelitian ini adalah sebagai berikut:

1. Didapatkannya kombinasi yang optimal dari metode pra proses dan kuantisasi multilevel.

   Pada disertasi ini dilakukan pengembangan metode pra proses Kalman serta Regresi Polinomial yang dikombinasikan dengan kuantisasi multilevel. Pengembangan metode pra proses kalman didapatkan dengan membagi parameter kanal RSS hasil pengukuran menjadi beberapa blok sehingga didapatkan peningkatan *reciprocity* dibandingkan dengan pengolahan metode pra proses Kalman yang sebelumnya. Kami juga mengusulkan metode *Modified Polynomial Regression* (MPR) sebagai pengembangan dari metode Regresi Polinomial. Metode ini bekerja dengan melakukan pemrosesan kembali parameter kanal RSS hasil pra proses dengan metode Regresi polinomial menggunakan metode Moving Average. Usulan lain adalah kombinasi dari metode Savitzky Golay Filter dengan kuantisasi multilevel. Hasil dari disertasi ini menunjukkan bahwa kombinasi tersebut mampu mengatasi *trade-off* antara parameter performansi KDR dan KGR dibandingkan dengan skema SKG yang eksisting.
2. Pengembangan metode pra proses sehingga bisa dihasilkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi.

Pada disertasi ini diusulkan metode pra proses Modified Kalman (MK) yang merupakan pengembangan dari metode Kalman. Metode ini mampu meningkatkan *reciprocity* secara signifikan sehingga mampu mencapai koefisien korelasi mendekati 1. Kombinasi antara metode MK dengan *Combined Multilevel Quantization* (CMQ) mampu menghasilkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi. Kontribusi yang didapatkan pada bagian ini bertujuan untuk menyederhanakan tahapan skema SKG sebagai bagian dari upaya untuk mendapatkan skema SKG yang efisien.

3. Skema SKG yang efisien dalam hal waktu komputasi dan *overhead* komunikasi.
   Pada disertasi ini diusulkan skema SKG *Signal Strength Exchange* (SSE) dan metode *Synchronized Quantization* (SQ) sebagai bagian sistem SSE yang melakukan sinkronisasi blok data pada fase kuantisasi. Pemanfaatan metode SQ mampu menghilangkan tahap pra proses dan rekonsiliasi informasi. Kontribusi yang didapatkan pada bagian ini bertujuan untuk mendapatkan skema SKG yang efisien dalam hal waktu komputasi dan *overhead* komunikasi sehingga sesuai jika diimplementasikan pada perangkat IoT dengan keterbeatasan sumber daya.

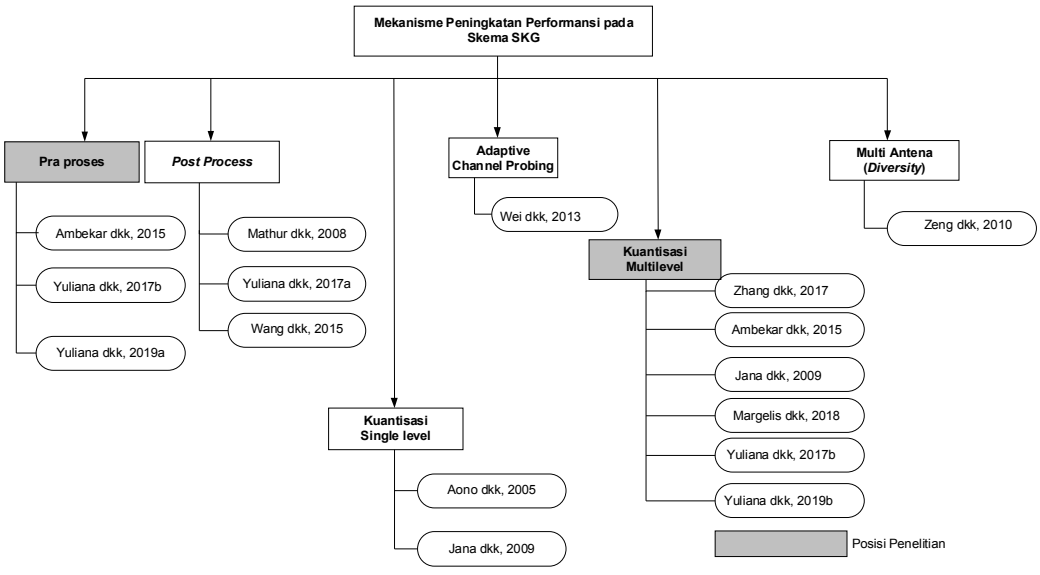
1.5 Posisi dan *Roadmap* Penelitian

Pada bagian ini akan dijelaskan tentang posisi dan *roadmap* dari penelitian yang dilakukan. Posisi penelitian ditunjukkan dengan klasifikasi dari berbagai mekanisme peningkatan performansi sedangkan *roadmap* penelitian berisi tahapan yang dilakukan untuk mendapatkan skema SKG yang efisien.

1.5.1 Posisi Penelitian

Gambar 1.1 menunjukkan diagram posisi penelitian terhadap sebagian penelitian sejenis yang telah dilakukan. Berbagai upaya yang dapat dilakukan untuk meningkatkan performansi sehingga didapatkan skema SKG yang efisien meliputi pengembangan kuantisasi multilevel, *adaptive channel probing*, multi antenna (*diversity*), metode pra proses, *post process*, serta kuantisasi *single level*. Peningkatan KGR dapat dilakukan dengan beberapa cara diantaranya dengan pengembangan

kuantisasi multilevel (Patwari dkk, 2010; Liu dkk, 2014; Jana dkk, 2009; Ambekar dkk, 2015; Zhang dkk, 2017; Zeng dkk, 2010; Yuliana dkk, 2019b; Yuliana dkk, 2019c), *adaptive channel probing* (Wei dkk, 2013) serta multi antenna (*diversity*) (Zeng dkk, 2010). Pengembangan kuantisasi multilevel dilakukan dengan merubah mekanisme pembagian level serta variasi parameter yang digunakan untuk menentukan *threshold*. Semakin tinggi level kuantisasi maka KDR yang dihasilkan juga semakin meningkat terutama di lingkungan dengan *Signal to Noise Ratio* (SNR) yang rendah. Beberapa metode kuantisasi multilevel (Ambekar dkk, 2015; Zeng dkk, 2010) merupakan skema kuantisasi yang lossy dimana ada bit yang terbuang karena berada di *threshold* sedangkan skema kuantisasi yang *lossless* memproses semua parameter kanal RSS yang ada sehingga tidak ada bit yang terbuang. Pemanfaatan skema kuantisasi yang *lossless* mampu meningkatkan KGR namun juga meningkatkan KDR. Semakin tinggi jumlah bit yang digunakan untuk ekstraksi *secret key* maka semakin tinggi juga KDR yang dihasilkan. *Probing rate* yang tinggi tidak hanya menghasilkan KGR yang tinggi, namun juga akan meningkatkan *redundancy*. Penggunaan multi antenna juga dapat meningkatkan KGR, namun kita harus mengembangkan protokol dan *software* yang digunakan untuk mengumpulkan parameter kanal RSS sebagai sumber ekstraksi *secret key*.



Gambar 1.1 Posisi Penelitian

Penurunan KDR dapat dilakukan dengan beberapa cara diantaranya dengan menggunakan metode pra proses (Ambekar dkk, 2015; Yuliana dkk, 2017b), *post process* (Mathur dkk, 2008; Yuliana dkk, 2017a; Wang dkk, 2015) serta pengembangan kuantisasi *single* level (Aono dkk, 2005; Jana dkk, 2009). Metode pra proses bekerja dengan cara mengolah RSS hasil pengukuran sebelum kuantisasi menggunakan beberapa pendekatan diantaranya *curve fitting* (Ambekar dkk, 2012), filtering (Ali dkk, 2010), serta Kalman Filter (Ambekar dkk, 2015). Hasil yang didapat menunjukkan peningkatan *reciprocity* yang diukur dengan koefisien korelasi Pearson. Semakin tinggi nilai koefisien korelasi Pearson yang didapat maka semakin rendah nilai KDR yang diperoleh. Penambahan metode pra proses selain menurunkan KDR juga akan meningkatkan waktu komputasi karena banyaknya tahapan yang harus dilalui serta masih adanya tahap rekonsiliasi informasi. Adanya mekanisme sinkronisasi pada tahap rekonsiliasi informasi serta *privacy amplification* juga akan mempengaruhi banyaknya *overhead* komunikasi yang dikirimkan antara kedua pengguna. Penggunaan kuantisasi *single bit* juga dapat menurunkan KDR namun juga menghasilkan KGR yang rendah. Metode *post process* bekerja dengan cara mengolah bit hasil kuantisasi sehingga didapatkan KDR yang lebih rendah. Pengolahan bit hasil kuantisasi diantaranya dilakukan dengan mencari bit yang berurutan dan merubahnya menjadi bit 1 atau 0 sehingga KDR menjadi rendah namun KGR juga mengalami penurunan.

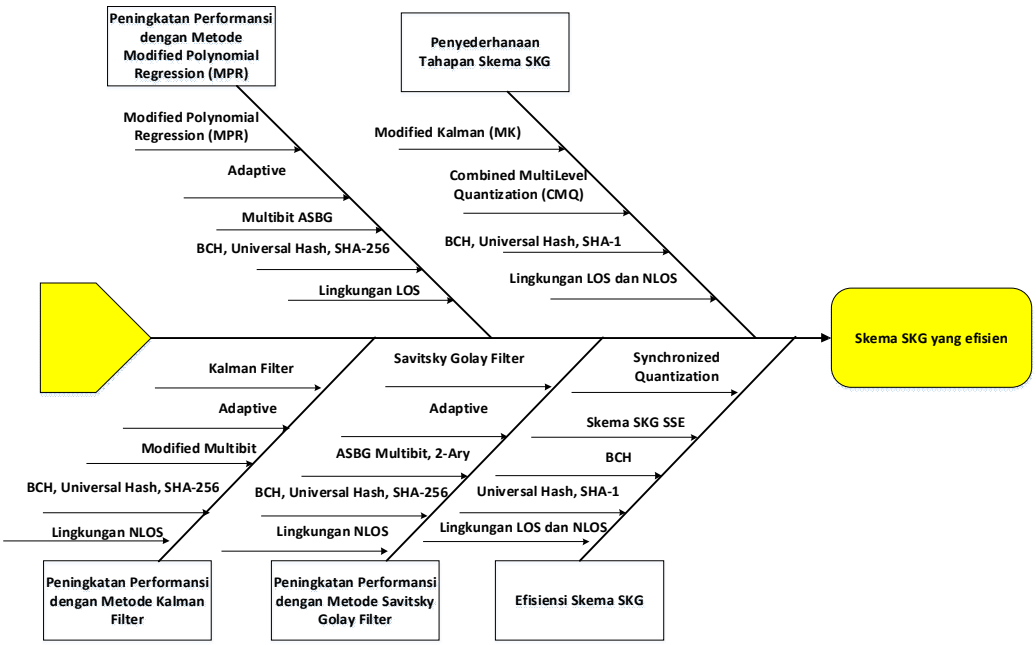
Penelitian yang dilakukan oleh penulis adalah upaya untuk mendapatkan kombinasi yang optimal antara metode pra proses dan kuantisasi multilevel sehingga didapatkan skema SKG mampu mengatasi *trade-off* antara parameter performansi KDR dan KGR. Selain itu upaya lain yang dilakukan adalah penyederhanaan tahapan pembangkitan *secret key* serta efisiensi skema SKG yang dibangun sehingga sesuai untuk diimplementasikan pada perangkat IoT dengan keterbatasan sumber daya.

1.5.2 *Roadmap* Penelitian

Roadmap atau jalan penelitian secara keseluruhan ditunjukkan dengan diagram tulang ikan seperti terlihat pada Gambar 1.2. Untuk mencapai target skema SKG yang efisien terdapat 3 sub topik yang mendukung, dimana sub topik tersebut meliputi peningkatan performansi untuk mengatasi *trade-off* antara parameter performansi KDR dan KGR dengan menggunakan pengembangan beberapa metode pra proses serta kombinasi antara metode pra proses dengan kuantisasi multilevel, penyederhanaan tahapan skema SKG dengan menghilangkan tahap rekonsiliasi informasi, serta efisiensi skema SKG. Detil tahapan yang dilakukan untuk mendapatkan skema yang efisien meliputi:

1) Peningkatan performansi dengan kombinasi metode pra proses Kalman Filter dengan kuantisasi multilevel Adaptive. Dilakukan pengembangan terhadap mekanisme pra proses parameter kanal RSS hasil pengukuran. Pengujian dilakukan dengan membandingkan performansi dari kombinasi metode pra proses dengan beberapa kuantisasi multilevel yaitu Adaptive, 2-Ary dan MMB.
2) Peningkatan performansi dengan kombinasi pengembangan metode pra proses Modified Polynomial Regression (MPR) dengan kuantisasi multilevel Adaptive. Pengujan dilakukan dengan membandingkan performansi dari kombinasi metode pra proses dengan beberapa kuantisasi multilevel yaitu Adaptive, ASBG, dan 2-Ary.
3) Peningkatan performansi dengan kombinasi metode pra proses Savitzky Golay Filter dengan beberapa kuantisasi multilevel yaitu Adaptive, ASBG, serta 2-Ary. Pengujan dilakukan dengan membandingkan performansi dari kombinasi metode pra proses dengan beberapa kuantisasi multilevel yang digunakan.
4) Penyederhanaan tahapan skema SKG dengan mengusulkan metode Modified Kalman (MK). Pada tahap ini skema yang diusulkan mampu mendapatkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi.
5) Efisiensi skema SKG dengan hanya menggunakan 3 tahap untuk membangkitkan *secret key* yang identik antara kedua pengguna. Pada tahap ini skema yang

diusulkan mampu mendapatkan *secret key* yang identik tanpa melalui tahap pra proses dan rekonsiliasi informasi.



Gambar 1.2 *Roadmap* Penelitian

1.6 Susunan Penulisan Disertasi

Pembahasan disertasi ini dimulai dari mekanisme peningkatan performansi dengan menggunakan metode pra proses serta kombinasinya dengan kuantisasi multilevel. Metode pra proses digunakan dengan tujuan untuk meningkatkan *reciprocity* parameter kanal hasil pengukuran, dimana metode yang digunakan meliputi Kalman Filter, *Modified Polynomial Regression* (MPR) serta Savitzky Golay Filter. Metode Kalman Filter dikembangkan dengan mengolah parameter kanal RSS hasil pengukuran menjadi beberapa blok data. Sedangkan metode MPR dikembangkan dengan mengolah kembali data hasil regresi polinomial dengan moving average. Tujuan dari bab ini adalah untuk untuk mengetahui seberapa optimal kombinasi yang didapat sehingga dapat mengatasi *trade-off* antara parameter performansi KDR dan KGR dibandingkan dengan skema yang eksisting. Pada bab 4 akan dibahas tentang mekanisme

penyederhanaan skema SKG dengan tujuan untuk mengeksplorasi pengembangan metode pra proses dan menghilangkan tahap rekonsiliasi informasi. Selanjutnya bab 5 akan membahas tentang pengembangan metode kuantisasi multilevel untuk membangun skema SKG yang efisien. Penulisan disertasi ini terdiri dari 6 bab, dengan rincian tiap bab sebagai berikut:

Bab 1 : Pendahuluan

Pada bagian ini peneliti menyajikan ikhtisar topik utama yang dibahas dengan latar belakang, perumusan masalah, tujuan dan manfaat, kontribusi dan orisinalitas serta posisi dan *roadmap* penelitian.

Bab 2 : Tinjauan Pustaka

Bab ini menjelaskan tentang beberapa teori yang mendukung pembangunan skema SKG. Secara umum terdapat 8 bagian yang akan dibahas, dimana bagian tersebut meliputi keamanan jaringan *wireless*, pemodelan dan prinsip skema SKG, jenis-jenis parameter kanal, tahapan skema SKG, pengembangan skema SKG, Advanced Encryption Standard (AES), parameter penentu performansi, serta beberapa penelitian terkait skema SKG.

Bab 3 : Peningkatan Performansi Skema SKG dengan Kombinasi Metode Pra proses dengan Kuantisasi Multilevel

Bab ini terdiri dari 3 bagian utama yang meliputi skema kombinasi metode Kalman Filter dengan kuantisasi multilevel, skema kombinasi metode MPR dengan kuantisasi multilevel, serta skema kombinasi metode *Savitzky Golay Filter* dengan kuantisasi multilevel. Beberapa parameter performansi yang digunakan akan dijelaskan secara detil sehingga bisa diketahui parameter yang menentukan keberhasilan skema SKG yang dibangun. Simulasi Monte Carlo juga akan dilakukan untuk mengetahui keberhasilan secara simulasi dari setiap tahap yang dilakukan. Validasi secara eksperimental juga dijelaskan

pada bagian eksperimental *setup* serta analisa performansi dari skema SKG yang dibangun.

Bab 4 : Penyederhanaan Skema SKG dengan Menggunakan Metode *Modified Kalman* (MK) dan *Combined Multilevel Quantization* (CMQ)

Bab ini terdiri atas 5 bagian yang meliputi tahapan skema SKG yang diusulkan, parameter performansi yang digunakan, simulasi Monte Carlo untuk keberhasilan penyederhanaan skema SKG, experimental *setup*, serta analisa performansi dari skema SKG yang dibangun.

Bab 5 : Efisiensi Skema SKG pada *Internet of Things* (IoT) dengan Menggunakan *Synchronized Quantization* (SQ)

Bab ini terdiri atas 4 bagian yang meliputi skema SKG *Signal Strength Exchange* (SSE), parameter performansi yang digunakan, simulasi Monte Carlo untuk efisiensi skema SKG dengan menggunakan *Synchronized Quantization* (SQ), serta evaluasi performansi dari skema SKG SSE.

Bab 6 : Kesimpulan dan Saran

Bab ini adalah bab terakhir yang berisi kesimpulan dan saran. Kesimpulan berisi hasil pengujian skema SKG yang dibangun untuk mengatasi permasalahan *trade-off* parameter performansi KDR dan KGR, kompleksitas implementasi, serta ketidakefisienan skema SKG yang dibangun. Sedangkan saran berisi penelitian selanjutnya yang dapat dikembangkan dari berbagai metode yang telah diusulkan untuk pengembangan skema SKG.

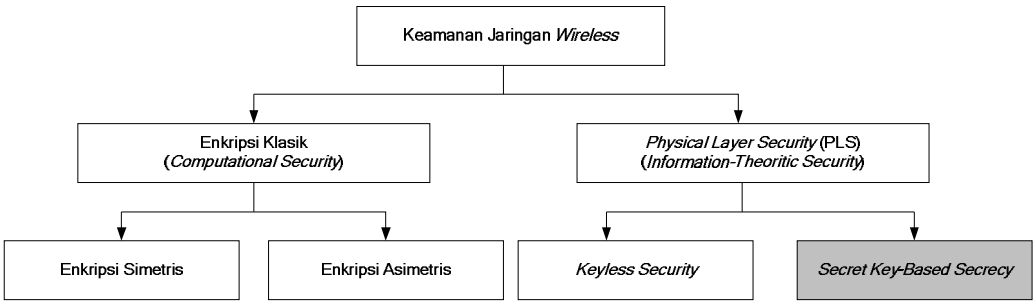
--Halaman ini sengaja dikosongkan--

BAB 2
KAJIAN PUSTAKA DAN DASAR TEORI

2.1 Keamanan Jaringan *Wireless*

Sifat *broadcast* dari komunikasi *wireless* memungkinkan informasi yang dikirim bisa diterima oleh pengguna manapun yang berada dalam jangkauan, sehingga memungkinkan berbagai serangan pasif seperti menyadap, atau serangan aktif seperti *jamming*, *spoofing*, serta *Denial-of-Service* (DoS) (Wu dkk, 2007). Hal inilah yang mendasari lahirnya beberapa penelitian untuk melindungi pengiriman informasi melalui komunikasi *wireless* (Chen dkk, 2013). Secara tradisional, informasi yang dikirimkan diamankan dengan menggunakan skema enkripsi klasik (Menezes dkk, 1996; Stallings, 2013). Dengan asumsi bahwa skema ini cukup kompleks maka waktu yang dibutuhkan untuk memecahkan skema tersebut jauh lebih lama dari validitas informasi itu sendiri. Gambar 2.1 menunjukkan bahwa skema enkripsi klasik terdiri dari skema enkripsi simetris dan asimetris tergantung dari jenis kunci yang digunakan. Skema enkripsi simetris menggunakan kunci yang sama dan biasanya digunakan untuk perlindungan informasi yang dikirim. Skema enkripsi asimetris, juga dikenal sebagai kriptografi kunci publik, menggunakan *public key* yang sama dan *private key* yang berbeda dan biasanya diterapkan untuk distribusi kunci.

Skema enkripsi klasik dihadapkan pada berbagai kerentanan dan permasalahan, salah satunya pada permasalahan kriptografi kunci publik. Permasalahan utama dari kriptografi ini adalah adanya ketergantungan terhadap kesulitan komputasi karena beberapa permasalahan matematika seperti logaritma diskrit. Hal inilah yang mengakibatkan kriptografi kunci publik sulit berkembang di masa yang akan datang karena pesatnya perkembangan dari teknologi *hardware*. Permasalahan lain dari kriptografi ini adalah dibutuhkannya infrastruktur manajemen kunci, sehingga kurang menarik bagi kebanyakan aplikasi *Internet of Thing* (IoT) dan jaringan *Ad hoc*, karena perangkat IoT memiliki kapasitas komputasi yang terbatas sedangan jaringan *Ad hoc* merupakan jaringan yang terpusat.



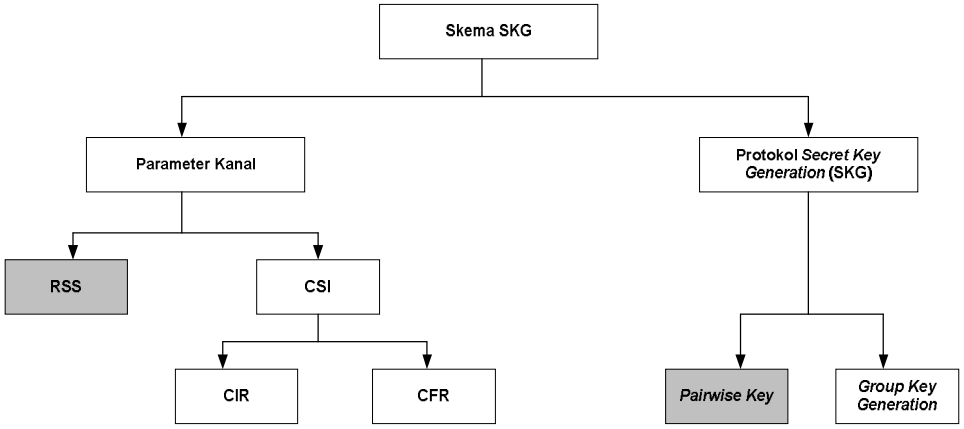
Gambar 2.1 Taksonomi keamanan jaringan *wireless* (Zhang dkk, 2016a).

Kelemahan dari skema enkripsi klasik mengakibatkan munculnya eksplorasi lapisan fisik untuk meningkatkan keamanan komunikasi *wireless*. Skema keamanan dengan lapisan fisik atau dikenal dengan *Physical Layer Security* (PLS) memanfaatkan karakteristik kanal *wireless* yang acak dan tidak terprediksi untuk mencapai informasi *theoretic-security* (shiu dkk, 2011; Mathur dkk, 2010). Secara garis besar terdapat 2 jenis dari PLS yaitu keamanan tanpa kunci (*keyless security*) dan keamanan dengan kunci berbasis *secrecy* (*secret key-based secrecy*) (Mukherjee dkk, 2014). Dipelopori oleh model kanal Wyner's *wiretap*, keamanan tanpa kunci tidak membutuhkan kunci untuk enkripsi namun menggunakan desain kode dan karakteristik saluran pengguna yang sah dan penyadap untuk mendapatkan *secrecy*. Keamanan kunci yang berbasis *secrecy* dimulai sejak tahun 1919, dengan adanya penggunaan *one time pad* yang juga dikenal dengan *cipher* Vernam yang digunakan untuk mengacak masing-masing bit pesan dengan bit kunci rahasia yang acak. Salah satu cara yang dapat digunakan untuk menghasilkan kunci adalah dengan memanfaatkan keacakan karakteristik kanal *wireless*, dimana skema pembangkitan kunci ini biasa disebut skema *Secret Key Generation* (SKG). Pada penelitian ini kami akan fokus pada skema SKG secara praktis. Tidak seperti kriptografi kunci publik yang aman secara komputasional, maka skema SKG adalah skema yang aman secara *information-theoritic* karena didasarkan pada keacakan karakteristik kanal *wireless*. Skema SKG secara teori diusulkan oleh (Ahlswede dkk, 1993) dan (Maurer dkk, 1993) pada tahun 1993, sedangkan skema

SKG secara praktis diusulkan pada tahun 1995 oleh (Hershey dkk, 1995) dan sejak saat itu memicu minat penelitian skema pembangkitan kunci di lingkungan *wireless*.

Gambar 2.2 menunjukkan klasifikasi dari skema berdasarkan parameter kanal yang digunakan dan mekanisme/protokol pembangkitan kunci. Terdapat 3 jenis parameter kanal yang bisa digunakan sebagai sumber pembangkitan kunci, dimana parameter tersebut meliputi *Received Signal Strength* (RSS), *Channel Impulse Response* (CIR), *Channel Frequency Response* (CFR). Beberapa penelitian menunjukkan bahwa CIR telah terbukti sebagai sumber yang ideal bagi pembangkitan kunci, karena memiliki fase dan amplitudo (Liu dkk, 2012). Pada sistem *Wideband*, pergeseran fase dapat diestimasi dan digunakan sebagai sumber untuk pembangkitan kunci (Shehadeh dkk, 2011). Pada sistem *Ultra Wideband* (UWB), amplitudo dapat diestimasi dengan mengirim sinyal pulsa (Marino dkk, 2014). Sistem CFR kebanyakan diimplementasikan di sistem OFDM IEEE 802.11(Zhang dkk, 2014; Zhang dkk, 2015), namun tidak semua *WiFi Network Interface Cards* (NICs) mendukung sistem ini. Salah satu NICs yang mendukung adalah Intel WiFi Link 5300 wireless, sedangkan *hardware* lain yang mendukung sistem ini adalah *Universal Software Radio Peripheral* (USRP) dan *Wireless Open-Access Research Platform* (WARP). RSS adalah parameter kanal yang paling popular digunakan untuk sistem pembangkitan kunci dan kebanyakan diimplementasikan pada IEEE 802.11 (Jana dkk, 2009; Premnath dkk, 2013; Guillaume dkk, 2015) dan IEEE 802.15.4 (Patwari dkk, 2010; Ali dkk, 2014).

Beberapa penelitian fokus pada skema pembangkitan kunci antara 2 pengguna yang sah (Premnath dkk, 2013; Mathur dkk, 2008), dimana pada skema ini hanya salah satu pengguna yang dipilih untuk melakukan *probe* pada kanal (*pairwise key*). Skema pembangkitan kunci untuk beberapa perangkat *wireless* (*Group Key Generation*) telah dilakukan secara teori (Ye dkk, 2007) dan praktis (Liu dkk, 2014). Pada skema ini hasil pengukuran yang didapat dibagi antar grup dan digunakan untuk membangkitkan kunci. Pada penelitian ini kami akan fokus pada desain skema *pairwise key* yang efisien dan aman dengan parameter kanal RSS.



Gambar 2.2 Klasifikasi Skema SKG.

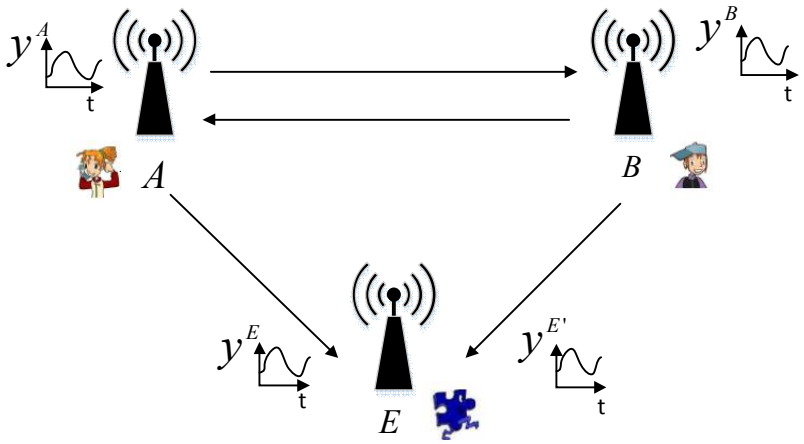
2.2 Pemodelan Skema SKG

Terdapat 3 pengguna yang terlibat pada penelitian ini yaitu Alice(A), Bob(B) dan Eve(E) seperti yang terlihat pada Gambar 2.3. Pengguna yang sah adalah A dan B, sedangkan pengguna yang tidak sah adalah E. Pada skema SKG, untuk membangkitkan *secret key* yang sama, Alice dan Bob mengukur variasi kanal *wireless* diantara mereka dengan mengirimkan *probe* satu sama lain dalam satu waktu tertentu dan mengukur nilai parameter kanal RSS dari *probe* tersebut. Di akhir proses pengukuran, diasumsikan Alice dan Bob akan membuat n pasangan dari parameter kanal RSS, seperti yang ditunjukkan oleh Persamaan (2.1) dan (2.2).

$$y^A = \{y^A(t_1), y^A(t_2), ..., y^A(t_n) \quad (2.1)$$

$$y^B = \{y^B(t_1^{'}), y^B(t_2^{'}), ..., y^B(t_n^{'}) \quad (2.2)$$

y^A adalah parameter kanal RSS yang diukur oleh Alice dan y^B adalah parameter kanal RSS yang diukur oleh Bob. Dalam implementasinya, meskipun y^A tidak sama persis y^B dengan karena kesalahan pengukuran ataupun variasi RSS yang didapat, namun mereka akan memiliki korelasi yang tinggi jika *bidirectional probing* (misal, $t_1^{'} - t_1$) lebih kecil dari *coherence time*.



Gambar 2.3 Pemodelan skema SKG.

Pada penelitian ini, terdapat 3 asumsi yang akan kami gunakan untuk penyadap E. Asumsi pertama yang digunakan adalah E sebagai node yang tidak legal mendengarkan semua proses probing sehingga akan mendapatkan parameter kanal dari A dan B yaitu y^E dan $y^{E'}$. Selain itu E juga berjarak lebih dari ½ panjang gelombang dari pengguna yang sah sehingga parameter kanal yang diterima tidak akan berkorelasi dengan parameter kanal yang dihasilkan node yang legal $(y^E \neq y^A, y^{E'} \neq y^B)$. Asumsi kedua yang kami gunakan adalah E merupakan penyadap yang sifatnya pasif sehingga tidak akan menyerang komunikasi yang dilakukan pengguna yang sah. Asumsi terakhir yang kami gunakan adalah E mengetahui semua algoritma yang digunakan oleh pengguna yang sah.

2.3 Prinsip Skema SKG

Skema SKG terdiri dari 3 prinsip yaitu *temporal variation*, *channel reciprocity*, dan *spatial decorrelation*. Penjelasan dari masing-masing prinsip bisa dilihat pada masing-masing sub bab berikut.

2.3.1 *Temporal Variation*

Temporal Variation diakibatkan oleh pergerakan pemancar, penerima, dan berbagai objek di suatu lingkungan, yang akan mengakibatkan refleksi, refraksi, dan *scattering* dari lintasan kanal. Keacakan yang disebabkan oleh pergerakan yang tidak terprediksi dapat digunakan sebagai sumber keacakan untuk skema pembangkitan kunci. Terdapat beberapa penelitian yang mengeksploitasi keacakan di domain frekuensi serta domain spasial. Namun pada lingkungan yang statis, dimana terdapat sedikit variasi dari parameter kanal maka keacakan akan sulit didapat. Sehingga bisa dikatakan bahwa *temporal variation* bisa digunakan sebagai sumber keacakan. *Temporal variation* dapat dihitung dengan *Autocorrelation Function (ACF)* dari sinyal yang dapat dihitung dengan Persamaan (2.3).

$$R_{y^u}(t,\Delta) = \frac{E\left\{\left(y^u(t)-\mu_{y^u}\right)\left(y^u(t+\Delta t)-\mu_{y^u}\right)\right\}}{\sigma^2_{y^u}} \tag{2.3}$$

Dimana $E\{.\}$ menunjukkan operator ekspektasi, dan μ_{y^u} serta σ_{y^u} menunjukkan nilai rata-rata dan varian dari variable acak hasil pengukuran pengguna yang sah $y^u(t)$, dimana u bisa diganti A untuk Alice dan B untuk Bob.

2.3.2 *Channel reciprocity*

Channel Reciprocity menunjukkan bahwa sinyal pada pengirim dan penerima yang memiliki kanal yang sama akan mendapatkan fitur statistik seperti *channel gain*, dan pergerakan fase yang identik. Hal inilah yang menjadi dasar bagi skema SKG untuk membangkitkan kunci yang simetris. Meskipun beberapa penelitian berupaya untuk mengadopsi perangkat yang *full duplex* (Vogt dkk, 2016), namun kebanyakan perangkat *wireless* yang ada saat ini bekerja pada mode *half duplex*. SKG biasanya bekerja pada sistem *Time-Division Duplexing* (TDD) dan *slow fading channel*. Sinyal yang diterima biasanya asimetris mengacu pada ketidaksimultanan pengukuran dan adanya pengaruh *noise* pada perangkat yang berbeda, sehingga mengakibatkan

berkurangnya kecepatan pembangkitan kunci dan meningkatnya ketidak cocokan kunci antara 2 pengguna. Kemiripan/keidentikan sinyal dapat dihitung dengan menggunakan *cross correlation* atau dikenal dengan koefisien korelasi Pearson antara 2 hasil pengukuran yang ditunjukkan dengan Persamaan (2.4).

$$\rho_{y^A y^B} = \frac{E\left\{y^A y^B\right\} - E\left\{y^A\right\} E\{y^B\}}{\sigma_{y^A} \sigma_{y^B}} \tag{2.4}$$

2.3.3 *Spatial Decorrelation*

Spatial Decorrelation menunjukkan bahwa penyadap yang berjarak lebih dari setengah panjang gelombang akan mengalami *multipath fading* yang tidak berkorelasi. Sifat ini sangat dipengaruhi oleh kondisi kanal. Pada lingkungan yang kaya akan *multipath* dengan *uniform scattering*, berdasarkan Jake model, jika jumlah *scatter* meningkat tidak terbatas, maka sinyal akan berdekorelasi pada jarak setengah panjang gelombang. Beberapa penelitian baik simulasi (He dkk, 2014) maupun praktis (Edman dkk, 2011) menunjukkan sebuah kondisi dimana sifat ini tidak terpenuhi, sehingga mengakibatkan skema SKG yang dihasilkan rentan dan membutuhkan beberapa pertimbangan khusus untuk mengatasi penyadap.

2.4 Parameter Kanal

PLS dapat diterapkan dan sangat memungkinkan untuk digunakan sebagai pendekatan mekanisme keamanan yang baru, sejak mekanisme pengukuran kanal selalu diimplementasikan pada beberapa perangkat *wireless*. Parameter kanal menyediakan akses ke sumber keacakan yang yang dihasilkan dari karakteristik kanal yang tidak bisa diprediksi, sehingga bisa dikatakan bahwa parameter kanal merupakan salah satu bagian yang paling penting dalam mekanisme SKG.

2.4.1 RSS (*Received Signal Strength*)

Hampir semua perangkat *wireless* menyediakan nilai RSSI **(***Received Signal Strength Indicator*), termasuk sistem yang dimodulasi oleh *Direct Sequence Spread Spectrum* (DSSS) atau *Frequency Hopping Spread Spectrum* (FHSS). RSSI saat ini banyak digunakan untuk ekstraksi kunci, terutama untuk penelitian berorientasi praktek dan implementasi. Rata-rata tingkat daya sinyal yang diterima yang diidentifikasi sebagai paket (atau bagian dari paket) disebut sebagai RSS, dan RSSI adalah indikator dari RSS. Biasanya, satu nilai RSSI diperoleh dari setiap paket yang diterima. Banyak sistem SKG berbasis RSSI yang telah diperkenalkan oleh beberapa penelitian, dimana sebagian besar didasarkan pada standarisasi IEEE 802.11 dan IEEE 802.15.4.

2.4.2 CSI (*Channel State Information*)

CSI adalah parameter kanal yang menyediakan informasi kanal secara detil, dan terdiri dari *Channel Impulse Responses* (CIR) dan *Channel Frequency Responses* (CFR). Sistem berbasis CSI bisa menghasilkan bit dengan kecepatan yang tinggi (Liu dkk, 2012) dan telah terbukti tahan terhadap *predictable channel attack* (Liu dkk, 2013). Kebanyakan WiFi *Network Interface Cards* (NICs) tidak menyediakan informasi CSI kecuali Intel WiFi Link 5300 wireless NIC. Beberapa perangkat lain yang juga menyediakan CSI adalah *Universal Software Radio Peripheral* (USRP) dan *Wireless Open-Access Research Platform* (WARP).

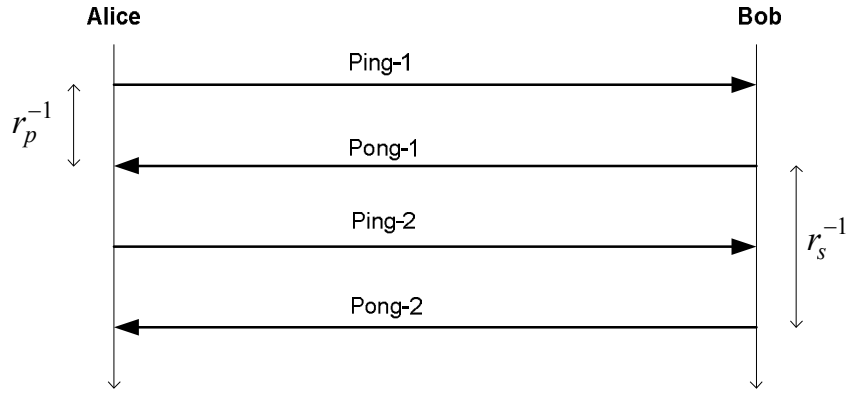
2.5 Tahapan Skema SKG

Terdapat 2 jenis jumlah tahapan skema SKG yang paling umum digunakan yaitu 4 tahap dan 5 tahap. Skema SKG yang memiliki 4 tahap lebih dikenal dengan nama skema *direct* quantization. Tahapan yang harus dilalui meliputi *channel probing*, kuantisasi, rekonsiliasi informasi, serta *privacy amplification*. Skema SKG yang memiliki 5 tahap menambahkan tahap pra proses sebelum kuantisasi. Tahap *channel probing* berguna untuk mendapatkan parameter kanal RSS dari sejumlah pengukuran

yang dilakukan. Jika digunakan 4 tahap dalam pembangkitan *secret key* maka parameter kanal RSS hasil pengukuran akan langsung dikuantisasi kedalam bentuk bit untuk mendapatkan *preliminary key*. Sedangkan jika digunakan 5 tahap maka parameter kanal RSS hasil pengukuran tersebut akan diolah terlebih dahulu dengan menggunakan beberapa metode pra proses. Parameter kanal RSS hasil pra proses akan dikuantisasi kedalam bentuk bit untuk mendapatkan *preliminary key*. Hasil pengukuran yang non simultan dan *noise* menyebabkan perbedaan bit dari *preliminary key* masing-masing pengguna yang sah. Kesalahan ini terdeteksi dan dikoreksi pada tahap rekonsiliasi informasi dengan teknik *error correcting* sehingga mendapatkan *synchronized key*. Terdapat 2 tahap yang dilakukan pada privacy amplification, dimana tahap tersebut meliputi peningkatan keacakan untuk memastikan kecukupan entropi, serta verifikasi bit kunci yang dihasilkan sehingga bisa didapatkan *secret key*.

2.5.1 *Channel Probing*

Karakteristik simetris dari *kanal wireless* bisa digunakan untuk pembangkitan kunci. *Channel probing* merupakan proses pengukuran untuk mengumpulkan parameter kanal RSS di sisi 2 pengguna yang sah. Parameter kanal yang diterima dari hasil pengukuran banyak dipengaruhi oleh variasi fenomena yang mencirikan kanal. Dua parameter penting yang biasanya digunakan pada pengukuran parameter kanal adalah *probing rate* r_p dan maksimum *sampling rate* r_s, seperti yang terlihat pada Gambar 2.4. Aturan komunikasi teknik praktis yang telah diaplikasikan pada beberapa penelitian sebelumnya (Jana dkk, 2009; Ambekar dkk, 2012) menyatakan bahwa pengukuran kanal antara 2 pengguna yang sah harus dilakukan dalam *coherence time* T_c dimana kanal diasumsikan tetap. Lebih jauh, pengukuran kanal lanjutan diasumsikan *independent* dari pengukuran kanal sebelumnya jika $r_s^{-1} > T_c$.



Gambar 2.4 Pengukuran parameter kanal RSS.

2.5.2 Pra proses Data Pengukuran

Kebanyakan parameter kanal RSS dikuantisasi langsung untuk mendapatkan *secret key*. Namun pengukuran kanal tidak selalu identik secara sempurna karena sifat pengukuran yang *half-duplex* (pengukuran yang tidak simultan) serta adanya *noise*. Beberapa penelitian mempertimbangkan mekanisme pra-proses parameter kanal dibandingkan langsung dikuantisasi, dimana beberapa pendekatan yang bisa digunakan meliputi interpolasi (Patwari dkk, 2010), dan filtering (Ali dkk, 2014). Kalman filter yang juga dikenal dengan *linear quadratic estimation* digunakan oleh beberapa penelitian sebagai algoritma pra-proses parameter kanal dan meningkatkan *reciprocity* hasil pengukuran. Kalman Filter secara rekursif mengestimasi *state* dari proses dengan menggunakan estimasi apriori dan aposteriori, sehingga *mean square error* bisa diminimalisir (Welch dkk, 2006).

2.5.2.1 Moving Average

Moving Average bekerja dengan merubah parameter kanal hasil pengukuran kedua pengguna $y(t_k)$ menjadi $z(t_k)$ dengan mengurangi $y(t_k)$ dengan rata-rata hasil pengukuran dalam *window* berukuran w seperti yang ditunjukkan oleh Persamaan (2.5).

$$z(t_k) = y(t_k) - \frac{\sum_{i=k-\left\lfloor \frac{w-1}{2} \right\rfloor}^{k+\left\lfloor \frac{w}{2} \right\rfloor} y(t_i)}{w} \tag{2.5}$$

2.5.2.2 Kalman Filter

Pada fase ini, parameter kanal hasil pengukuran akan diestimasi dengan menggunakan estimasi apriori dan posteriori. Prediksi awal dari parameter kanal dilakukan di persamaan *time update* dan hasil prediksi akan dikoreksi di persamaan *measurement update* (Welch dkk, 2006). Hasil estimasi parameter kanal yang dilakukan berulang-ulang seperti terlihat pada Gambar 2.5 menunjukkan mekanisme pra-proses sinyal yang akan menghasilkan peningkatan *reciprocity* dari estimasi parameter kanal. Estimasi dari parameter kanal hasil pengukuran x_k ditunjukkan oleh Persamaan (2.6), dimana A adalah matriks *nxn* yang menunjukkan state dari waktu $k-1$. B adalah matriks nxl yang menunjukkan opsional kontrol input u dan w_k adalah *noise* proses.

$$x_k = Ax_{k-1} + Bu_{k-1} + w_{k-1} \tag{2.6}$$

y_k adalah parameter kanal hasil pengukuran dari kedua pengguna pada waktu k seperti yang ditunjukkan oleh Persamaan (2.7). H adalah matrik *mxn* yang menunjukkan state pengukuran pada waktu k dan v_k adalah *noise* pengukuran.

$$y_k = Hx_k + v_k \tag{2.7}$$

Probabilitas distribusi normal dari *noise* proses dan *noise* pengukuran diberikan oleh Persamaan (2.8) dan (2.9), dengan Q dan R adalah kovarian dari *noise* proses dan pengukuran.

$$p(w) \sim N(0, Q) \tag{2.8}$$

$$p(v) \sim N(0, R) \tag{2.9}$$

Persamaan *time update* yang digunakan untuk memprediksi parameter kanal hasil pengukuran pada penelitian ini adalah Persamaan (2.10) dan (2.11), dimana $\hat{x}_k^-$ adalah estimasi apriori dan P_k^- adalah *error* kovarian apriori.

$$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1} \tag{2.10}$$

$$P_k^- = AP_{k-1}A^T + Q \tag{2.11}$$

Sedangkan persamaan *measurement update* untuk melakukan koreksi terhadap estimasi apriori dari parameter kanal hasil pengukuran bisa dilihat pada Persamaan (2.12), (2.13) dan (2.14). $\hat{x}_k$ adalah estimasi aposteriori dari parameter kanal, P_k adalah *error* kovarian aposteriori, sedangkan K_k mengacu pada Kalman Gain.

$$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1} \tag{2.12}$$

$$\hat{x}_k = \hat{x}_k^- + K_k(y_k - H\hat{x}_k^-) \tag{2.13}$$

$$P_k = (I - K_k H)P_k^- \tag{2.14}$$

Gambar 2.5 Mekanisme pra-proses.

2.5.2.3 Regresi Polinomial

Regresi Polinomial termasuk kelas dari algoritma regresi, dimana tujuan utamanya adalah untuk menggambarkan fungsi polinomial yang paling sesuai dengan data yang

diketahui. Fungsi pendekatan yang digunakan ditunjukkan oleh Persamaan (2.15), dimana y_i menunjukkan parameter kanal sejumlah n data pada waktu x_i dengan $i = (1,2,...,n)$. Koefisien polinomial yang menunjukkan tingkat perubahan dari parameter kanal ditunjukkan oleh $a_0, a_1, a_2, ..., a_m$, dengan m adalah orde polinomial.

$$y_i = a_0 + a_1 x_i + a_2 x_i^2 + ... + a_m x_i^m \tag{2.15}$$

2.5.2.4 Discrete Cosine Transform (DCT)

Beberapa penelitian mengaplikasikan Discrete cosine Transform (DCT) sebagai metode pra proses dari parameter kanal hasil pengukuran. DCT merubah sejumlah data parameter kanal hasil pengukuran menjadi sejumlah fungsi cosinus pada frekuensi yang berbeda dan dinyatakan dengan Persamaan (2.16).

$$z(k) = a(k)\sum_{n=1}^{N} y(n)\cos\left(\frac{(2n-1)(k-1)\pi}{N}\right), k = 1,2,...,N \tag{2.16}$$

Dimana N menunjukkan jumlah koefisien, $y(n)$ menunjukkan parameter kanal hasil pengukuran, $z(k)$ menunjukkan parameter kanal hasil pra proses sedangkan $a(k)$ dinyatakan dengan Persamaan (2.17).

$$a(k) = \begin{cases} 1/\sqrt{N}, k = 1 \\ \sqrt{2/N}, 2 \le k \le N \end{cases} \tag{2.17}$$

2.5.2.5 *Savitzky Golay Fillter*

Filter *low pass* tidak sesuai jika diimplementasikan pada skema SKG yang praktis karena adanya keacakan dari RSS yang dihasilkan. ,-*Golay filter* bertindak sebagai filter *low pass* yang mampu mengikuti pola RSS dan melakukan *smoothing* data RSS dalam domain waktu sehinggga mampu mengurangi ketidakcocokan RSS antara dua pengguna yang sah (Ali dkk, 2014). Parameter n_L adalah jumlah poin yang digunakan

di sebelah kiri data *point*, sedangkan n_R adalah jumlah poin yang digunakan di sebelah kanan data *point*. Nilai g_i sebagai rata-rata data point dari f_{i-n_L} hingga f_{i+n_R} yang dinyatakan dengan Persamaan (2.18).

$$g_i = \sum_{n=-n_L}^{n_R} c_n f_{i+n} \tag{2.18}$$

didapat dengan koefisien filter $c_n = 1/(n_L + n_R + 1)$ dan $n_L = n_R$. Jika fungsi yang didapat merupakan fungsi yang konstan atau berubah secara linear terhadap waktu baik menaik maupun menurun maka hasil yang didapat tidak akan bias. Koefisien filter c_n yang diharapkan adalah koefisien yang memiliki momen tertinggi. Untuk mendapatkan koefisien tersebut maka g_0 bisa didapatkan dari persamaan polinomial $a_0 + a_1 i + ... + a_m i$. Jika kita melakukan fit pada Polinomial dengan orde m pada i terhadap nilai $f_{-n_L}, ..., f_{n_R}$ maka g_0 akan menjadi nilai polinomial pada $i = 0$ yaitu a_0 . Disain matrix yang digunakan untuk persamaan ini $A_{ij} = i^j$ dengan $i = -n_L, ..., n_R$ dan $j = 0, ..., m$.

2.5.3 Kuantisasi Multilevel

Pada tahap ini, parameter kanal RSS diubah kedalam bentuk bit untuk mendapatkan *preliminary key*. Terdapat 2 skema kuantisasi yaitu skema kuantisasi yang *lossy* dan *lossless*. Kuantisasi *lossless* memetakan setiap sampel ke simbol yang terdiri dari sejumlah bit, sedangkan skema kuantisasi *lossy* membuang sampel tertentu untuk mendapatkan bit yang memiliki entropi yang tinggi. Pemilihan parameter skema kuantisasi akan mempengaruhi banyaknya bit yang dihasilkan dalam satu waktu tertentu, serta besarnya prosentase perbedaan bit antara 2 pengguna yang sah. Pada penelitian ini, kami akan fokus pada mekanisme SKG yang yang berorientasi pada praktis dengan mempertimbangkan implementasi dan kebutuhan dunia nyata dibandingkan skema SKG yang berorientasi pada teori.

2.5.3.1 2-Ary

Untuk meningkatkan kecocokan bit, metode kuantisasi 2-Ary bekerja dengan memasukkan *guard band* g_i antara dua level kuantisasi yang berurutan yaitu q_{i-1} dan q_i. Pada metode kuantisasi ini, diasumsikan parameter kanal RSS y mengikuti distribusi probabilitas f_y dimana semua hasil memiliki probabilitas yang sama. Parameter α digunakan sebagai parameter penentu parameter kanal hasil pra proses yang akan dibuang. Jika kita memiliki jumlah level kuantisasi sebanyak L maka interval kuantisasi yang didapatkan dinyatakan dengan Persamaan (2.19).

$$I_0 = (q_0, q_1 - g_1), I_1 = (q_1, q_2 - g_2), \ldots, I_{L-1} = (q_{L-1}, q_L) \tag{2.19}$$

dengan q_0 adalah nilai minimum dan q_L adalah nilai maksimum dari data parameter kanal hasil pra proses. Jumlah parameter kanal hasil pra proses yang akan diolah dinyatakan dengan persamaan (2.20) sedangkan data yang akan dibuang dinyatakan dengan Persamaan (2.21).

$$\int_{q_{i-1}}^{q_i - g_i} f_y dy = \frac{1-\alpha}{L} \tag{2.20}$$

$$\int_{q_i - g_i}^{q_i} f_y dy = \frac{\alpha}{L-1} \tag{2.21}$$

dengan nilai *i* antara 1 hingga *L-1*. Jika level kuantisasi L yang digunakan, maka masing-masing level akan disajikan dengan C bit ($C = \log_2 L$). *Gray coding* digunakan untuk mengisi C bit di masing-masing level.

2.5.3.2 *Adaptive*

Metode kuantisasi *Adaptive* bekerja dengan membagi parameter kanal RSS menjadi beberapa blok dan melakukan kuantisasi di tiap tiap blok tersebut. Level dari masing-masing kuantisasi dinyatakan dengan Persamaan (2.22).

$$Q(y) = \begin{cases} level1 & , \ [-\infty, \mu - \sigma^2 / 2] \\ level2 & , \ [\mu - \sigma^2 / 2, \mu] \\ level3 & , \ [\mu, \mu + \sigma^2 / 2] \\ level4 & , \ [\mu + \sigma^2 / 2, \infty] \end{cases} \quad (2.22)$$

Dimana μ adalah rata-rata, sedangkan σ^2 adalah varians dari masing-masing blok. *Gray coding* digunakan untuk mengisi C bit di masing-masing level (level 1(00), level 2(01), level 3(11), level 4(10)).

2.5.3.3 *Adaptive Secret Bit Generation* (ASBG)

Peneliti (Jana dkk, 2009) juga mengusulkan skema kuantisasi multilevel yang menawarkan ekstraksi C bit dari parameter kanal RSS y, dimana $C \leq \lfloor \log_2 range \rfloor$, dengan $range = y_{\max} - y_{\min}$ dihitung pada tiap-tiap blok dan dibagi ke dalam $L = 2^C$ interval yang sama. Masing-masing y akan dipetakan dalam C bit dengan penggunaan *Gray coding*. Hasil pengujian yang dilakukan menunjukkan semakin tinggi nilai C maka ketidakcocokan bit antara dua pengguna juga semakin tinggi.

2.5.3.4 *Modified Multibit* (MMB)

Peneliti (Yuliana dkk, 2017b) mengusulkan skema kuantisasi multilevel yaitu *modified multibit* (MMB) yang merupakan pengembangan dari metode kuantisasi adaptive. Parameter yang digunakan untuk menentukan level adalah rata-rata μ, standar deviasi σ, dan parameter α yang bernilai antara 0.01 hingga 0.06. Level dari masing-masing kuantisasi dinyatakan dengan Persamaan (2.23).

$$Q(y) = \begin{cases} level1 & , \ [-\infty, \mu - \alpha * \sigma] \\ level2 & , \ [\mu - \alpha * \sigma, \mu] \\ level3 & , \ [\mu, \mu + \alpha * \sigma] \\ level4 & , \ [\mu + \alpha * \sigma, \infty] \end{cases} \quad (2.23)$$

Gray coding digunakan untuk mengisi C bit di masing-masing level (level 1(01), level 2(00), level 3(10), level 4(11)).

2.5.3.5 *Cumulative Distribution Function* (CDF)

Peneliti (Zhang dkk, 2017) mengusulkan skema kuantisasi yang dikenal dengan sebutan *Cumulative Distribution Function* (CDF). Pada skema CDF, pertama kali akan dilakukan kuantisasi parameter kanal RSS y dengan jumlah level kuantisasi sebanyak L. CDF dari parameter kanal RSS dinyatakan dengan Persamaan (2.24).

$$F(y) = P(Y \leq y) \tag{2.24}$$

Level dari masing-masing kuantisasi didapatkan dari *inverse* CDF seperti yang terlihat pada Persamaan (2.25).

$$L_k = F^{-1}\left(\frac{k}{2^C}\right), k = 1,..,2^C - 1 \tag{2.25}$$

Gray coding digunakan untuk mengisi n bit di level $[L_{k-1}, L_k]$ dengan $\eta_0 = -\infty$ dan $L_k = 2^C$.

2.5.3.6 SKYGlow

Metode kuantisasi ini bekerja dengan menggunakan dua parameter yaitu rata-rata μ dan standar deviasi σ. Level dari masing-masing kuantisasi dinyatakan dengan Persamaan (2.26).

$$Q(y) = \begin{cases} level1 & , \quad [-\infty, \mu - \sigma] \\ level2 & , \quad [\mu - \sigma, \mu] \\ level3 & , \quad [\mu, \mu + \sigma] \\ level4 & , \quad [\mu + \sigma, \infty] \end{cases} \tag{2.26}$$

Gray coding digunakan untuk mengisi n bit di masing-masing level (level 1(00), level 2(01), level 3(10), level 4(11)).

2.5.4 Rekonsiliasi Informasi

Rekonsiliasi informasi bertanggung jawab untuk mendeteksi dan mengoreksi kesalahan *preliminary key* yang dihasilkan dari komunikasi dua pengguna. Kesalahan ini biasanya disebabkan oleh perbedaan saat proses pengukuran. Perbedaan ini disebabkan oleh *noise* karena ketidaksempurnaan *hardware*. Pada penelitian ini, kami menggunakan kode BCH. Untuk semua integer m ($m \geq 3$) dan t ($t \leq 2^{m-1}$) terdapat kode BCH dengan beberapa parameter yang meliputi panjang blok $n = 2^{m-1}$, jumlah digit *parity check* $n-k \leq mt$, dan jarak minimum $n-k \leq 2t+1$. Secara umum kode ini dapat mengoreksi t atau lebih sedikit kesalahan pada sebuah blok data, dengan α adalah elemen primitif dari $GF(2^m)$. Generator polinomial $g(x)$ dari kode BCH dengan panjang 2^{m-1} adalah polinomial derajat terendah dari $GF(2)$ yang memiliki akar seperti yang ditunjukkan pada Persamaaan (2.27).

$$\alpha, \alpha^2, \alpha^3, ..., \alpha^{2t} \tag{2.27}$$

Dengan $g(\alpha^i) = 0$ untuk $1 \leq i \leq 2t$, dan $\phi_i(X)$ adalah polinomial minimal dari α^i. $g(x)$ harus *Least Common Multiple* (LCM) dari $\phi_1(x), \phi_2(x), ..., \phi_{2t}(x)$ seperti yang ditunjukkan pada Persamaan (2.28).

$$g(x) = LCM\{\phi_1(x), \phi_2(x), ..., \phi_{2t}(x)\} \tag{2.28}$$

Generator Polinomial $g(X)$ yang diberikan oleh persamaan (2.24) dapat dikurangi sehingga menjadi Persamaan (2.29).

$$g(x) = LCM\{\phi_1(x), \phi_3(x), ..., \phi_{2t-1}(x)\} \tag{2.29}$$

Langkah pertama dari proses decoding adalah menyimpan *codeword* yang diterima di *buffer* dan menghitung *sindrom*. *Codeword* $r(x)$ yang diterima dapat dikorupsi dengan *error pattern* seperti yang ditunjukkan oleh Persamaan (2.30).

$$r(x) = c(x) + e(x) \tag{2.30}$$

Codeword yang diterima ditunjukkan oleh Persamaan (2.31)

$$r(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1} x^{n-1} \tag{2.31}$$

Codeword yang dikirimkan ditunjukkan oleh Persamaan (2.32)

$$c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1} \tag{2.32}$$

Error pattern ditunjukkan oleh Persamaan (2.33)

$$e(x) = e_0 + e_1 x + e_2 x^2 + \ldots + e_{n-1} x^{n-1} \tag{2.33}$$

Sindrom S_i dapat dihitung dengan Persamaan (2.34)

$$S_i = r(a^i) = r_0 + r_1 a^i + r_2 a^{2i} + \ldots + r_{n-1} a^{(n-1)i} \tag{2.34}$$

Dengan $1 \le i \le 2t - 1$. Jika tidak ada kesalahan pada *codeword* yang diterima, maka sindrom yang dihasilkan adalah nol. Jika terdapat kesalahan maka langkah selanjutnya adalah mencari koefisien dari lokasi *error* yang ditunjukkan oleh Persamaan (2.35)

$$\lambda(a^i) = \lambda_0 + \lambda_1 a^j + \lambda_2 a^{2j} \tag{2.35}$$

Koefisien $\lambda_0, \lambda_1, \lambda_2$ dicari dengan algoritma Inversion-less Berlekamp Massey dengan $1 \le j \le n$. Langkah terakhir yang dilakukan adalah melakukan koreksi *error* dengan membalik bit pada posisi yang salah.

2.5.5 *Privacy Amplification*

Selama fase rekonsiliasi informasi para penyadap juga akan memiliki akses untuk mengoreksi kesalahan. Untuk menghindari kemungkinan prediksi kunci dan mendapatkan entropi dari kunci yang dihasilkan, maka perlu dilakukan *privacy amplification*. *Privacy amplification* dapat diimplementasikan dengan ekstraktor (Wang dkk, 2011), atau *universal hash function* seperti leftover hash lemma (Jana dkk, 2009), sedangkan *cryptographic hash function* seperti SHA-1(Yuliana dkk, 2017b) digunakan untuk verifikasi. Pada penelitian ini, kami menggunakan *universal hash function* dengan membangkitkan sebuah matrik acak T berukuran nxm, sehingga fungsi *hash* yang didapat $h(o) = To$, dimana O adalah kunci dengan $o \in \{0,1\}^n$.

Verifikasi digunakan untuk memastikan bahwa kunci yang dihasilkan kedua pengguna yang sah adalah sama. Pada penelitian ini, kami menggunakan SHA-1 dan SHA-256 yang dapat digunakan untuk melakukan *hash* pada pesan M yang memiliki panjang l bit ($0 \le l \le 2^{64}$). SHA-1 menggunakan : 1) jadwal pesan dari 80 *word* (masing-masing 32 bit), 2) 5 variabel (masing-masing 32 bit), 3) nilai *hash* dari 5 *word* (masing-masing 32 bit). Hasil akhir dari SHA-1 adalah 160 bit *message digest*. *Word* dari masing-masing jadwal pesan diberi label $W_0, W_1, ..., W_{79}$. Lima variabel yang digunakan diberi label a, b, c, d, e. Nilai *hash* dari *word* dilabelkan dengan $H_0^{(i)}, H_1^{(i)}, ..., H_4^{(i)}$, yang akan menahan nilai *hash* awal, $H^{(0)}$, untuk digantikan oleh setiap nilai *hash* (setelah masing-masing blok pesan diproses), $H^{(i)}$, dan diakhiri dengan nilai *hash*, $H^{(N)}$. SHA-1 juga menggunakan *word* temporer, T .

SHA-256 menggunakan : 1) jadwal pesan dari 64 *word* (masing-masing 32 bit), 2) 8 variabel (masing-masing 32 bit), 3) nilai *hash* dari 8 *word* (masing-masing 32 bit). Hasil akhir dari SHA-256 adalah 256 bit *message digest*. *Word* dari masing-masing jadwal pesan diberi label $W_0, W_1, ..., W_{63}$. Delapan variabel yang digunakan diberi label a, b, c, d, e, f, g, h . Nilai *hash* dari *word* dilabelkan dengan $H_0^{(i)}, H_1^{(i)}, ..., H_7^{(i)}$, yang akan menahan nilai *hash* awal, $H^{(0)}$, untuk digantikan oleh setiap nilai *hash* (setelah

masing-masing blok pesan diproses), $H^{(i)}$, dan diakhiri dengan nilai *hash*, $H^{(N)}$. SHA-1 juga menggunakan 2 *word* temporer, T_1 dan T_2 .

2.6 Pengembangan Skema SKG

Beberapa penelitian mengusulkan pengembangan kuantisasi multilevel sebagai upaya untuk peningkatan performansi. Ikhtisar dari penelitian yang mengembangkan skema kuantisasi multilevel ditunjukkan oleh Tabel 2.1. Penelitian yang menggunakan CDF (Patwari dkk, 2010; Zhang dkk, 2017) untuk melakukan ekstraksi bit kunci menghasilkan waktu komputasi yang lebih lama jika semakin banyak level kuantisasi yang digunakan. Selain itu KDR juga akan mengalami peningkatan karena semakin banyaknya perbedaan parameter kanal antara kedua pengguna. Metode kuantisasi yang diusulkan oleh (Liu dkk, 2014) juga meningkatkan waktu komputasi karena ada beberapa tahap yang harus dilakukan untuk melakukan konversi bit. Terdapat penurunan KGR yang dihasilkan karena adanya kombinasi dari konversi kuantisasi *single bit* dan multi bit. Secara umum terdapat 2 jenis kuantisasi yang dikembangkan oleh peneliti, dimana kuantisasi tersebut meliputi kuantisasi *lossy* (Ambekar dkk, 2015; Yuliana dkk, 2017b; Zeng dkk, 2010) dan *lossless* (Patwari dkk, 2010; Jana dkk, 2009; Margelis dkk, 2018; Zhang dkk, 2017). Pada kuantisasi *lossy* terdapat bagian dari parameter kanal yang dibuang karena berada di *threshold*. Kelebihan dari kuantisasi ini adalah KDR yang dihasilkan lebih rendah meskipun KGR yang dihasilkan juga mengalami penurunan. Sedangkan pada kuantisasi *lossless* tidak ada bagian dari parameter kanal yang dibuang , sehingga KGR yang dihasilkan juga lebih tinggi namun KDR yang dihasilkan juga mengalami peningkatan.

Tabel 2.1 Ikhtisar penelitian pengembangan kuantisasi multilevel.

No	Hasil Penelitian
1	Mengusulkan metode baru yaitu *Multi bit adaptive quantization* (MAQ) yang menggunakan *cumulative distribution function* (CDF) dari parameter kanal hasil pengukuran. Penentuan jumlah level kuantisasi didasarkan pada jumlah bit kuantisasi yang diinginkan (Patwari dkk, 2010).
2	Mengusulkan gabungan estimasi *fading trend* dengan *extended RSS fading trend and quantization* (RTQ). Estimasi *fading trend* bekerja dengan mengubah parameter kanal RSS yang monoton menjadi bit 1 atau 0. Sisa dari estimasi *fading trend* akan diekstrak menjadi bit dengan menggunakan metode RTQ. Metode ini bekerja dengan menggunakan *cumulative distribution function* (CDF) (Liu dkk, 2014).
3	Mengusulkan metode kuantisasi *Adaptive Secret Bit Generation* (ASBG) multi bit. Metode tersebut melakukan ekstraksi multi bit dengan melakukan pengurutan RSS hasil pengukuran dan membaginya kedalam interval. Mengubah masing-masing RSS yang terletak pada interval untuk menjadi bit dengan menggunakan *Gray Coding* (Jana dkk, 2009).
4	Mengusulkan metode kuantisasi *Adaptive*. Metode tersebut melakukan kuantisasi multi bit dengan membagi parameter kanal hasil pengukuran kedalam beberapa level . Parameter penentu level yang digunakan adalah rata-rata dan varian (Ambekar dkk, 2015).
5	Mengusulkan metode *Modified Multibit* (MMB). Metode tersebut melakukan kuantisasi multi bit dengan membagi parameter kanal hasil pengukuran kedalam beberapa level. Parameter penentu level yang digunakan adalah rata-rata, standar deviasi, serta parameter α (Yuliana dkk, 2017b).
6	Mengusulkan metode 2-ary *quantization*. Metode ini bekerja dengan memasukkan guard band pada level kuantisasi yang berurutan (Zeng dkk, 2010).
7	Mengusulkan metode kuantisasi SKYGlow. Skema tersebut menggunakan mean dan standar deviasi sebagai parameter penentu level kuantisasi (Margelis dkk, 2018).
8	Mengusulkan metode kuantisasi Cumulative Distribution Function (CDF). Skema tersebut bekerja dengan menggunakan cumulative distribution function (CDF) dari parameter kanal hasil pengukuran. Penentuan jumlah level kuantisasi didasarkan pada jumlah bit kuantisasi yang diinginkan (

Beberapa penelitian melakukan *direct* kuantisasi dengan melakukan konversi bit langsung dari parameter kanal RSS hasil pengukuran (Zenger dkk, 2015; Zhang dkk, 2017). Salah satu pengembangan dari proses konversi dilakukan dengan pembagian

parameter kanal RSS hasil pengukuran kedalam blok dimana masing-masing blok berisi 128 data. Masing-masing blok tersebut akan dikonversi menjadi multibit (Zenger dkk, 2015). Sedangkan peneliti (Zhang dkk, 2017) melakukan konversi multibit langsung dari parameter kanal RSS hasil pengukuran tanpa melakukan pembagian per blok. *Direct* kuantisasi umumnya lebih efisien karena semakin sedikitnya tahapan yang harus dilalui. Waktu komputasi yang dibutuhkan juga cenderung lebih rendah jika dibandingkan dengan skema SKG yang menambahkan tahap lain misalnya tahap pra proses. Namun mekanisme ini umumnya memiliki KDR yang tinggi karena adanya perbedaan parameter kanal RSS hasil pengukuran antara kedua pengguna. Tingginya KDR ini terutama diperoleh pada koefisien korelasi parameter kanal RSS hasil pengukuran yang rendah. Semakin tinggi KDR akan berpengaruh pada KGR yang dihasilkan. Hal ini terjadi karena semakin sulitnya tahap rekonsiliasi informasi untuk melakukan koreksi dari perbedaan bit yang dihasilkan. Jika tahap rekonsiliasi informasi tidak mampu melakukan koreksi, maka blok data tersebut akan dibuang sehingga mengurangi KGR yang diperoleh.

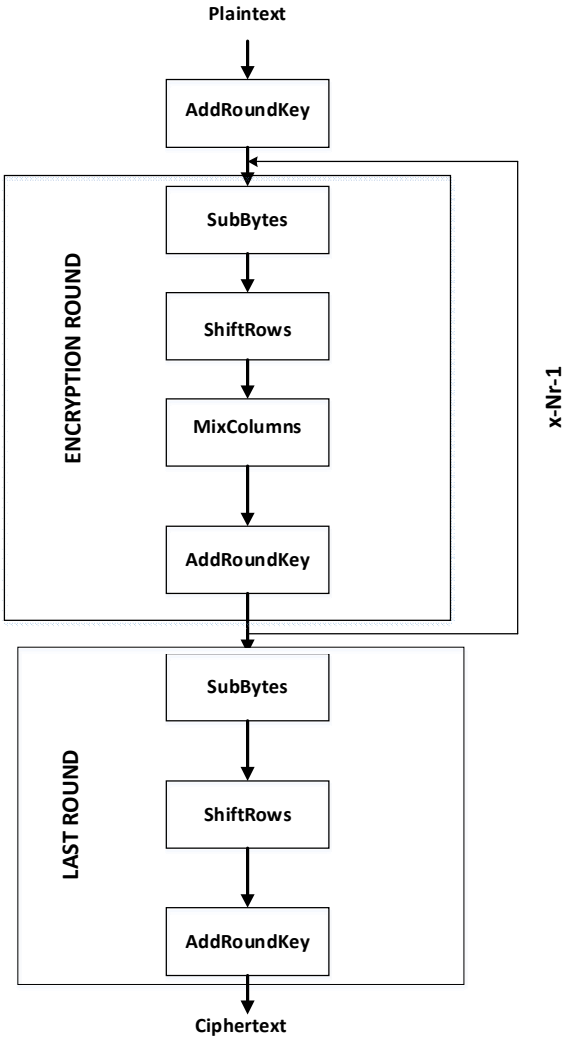
Salah satu upaya yang dapat dilakukan untuk meningkatkan performansi dari skema SKG yang dibangun adalah dengan menambahkan metode pra proses dan melakukan kombinasi dengan kuantisasi multilevel seperti yang terlihat pada Tabel 2.2. Peneliti (Patwari dkk, 2010; Liu dkk, 2014) melakukan kombinasi antara metode pra proses Interpolasi dan kuantisasi multilevel. Namun kedua penelitian tersebut memiliki kompleksitas yang tinggi karena banyaknya tahapan yang harus dilalui. Beberapa peneliti melakukan kombinasi antara metode pra proses dengan kuantisasi yang berisi *single bit* (Jana dkk, 2009; Ali dkk, 2010; Jiang dkk, 2018). Kondisi ini mengakibatkan lebih rendahnya KGR yang dihasilkan meskipun tetap ada penurunan KDR karena pemanfaatan metode pra proses. Hasil penelitian yang dilakukan menunjukkan bahwa kebanyakan metode pra proses dikombinasikan dengan metode kuantisasi *lossy* (Ambekar dkk, 2015; Guillaume dkk, 2015; Ambekar dkk, 2012; Zeng dkk, 2010). Hal ini dilakukan untuk mendapatkan KDR yang rendah sehingga mengurangi blok data yang dibuang di tahap rekonsiliasi informasi.

Tabel 2.2 Ikhtisar penelitian kombinasi metode pra proses dengan kuantisasi multilevel.

No	Hasil Penelitian
1	Metode pra proses yang digunakan Fractional Interpolation Filter serta Karhunen Loeve Transform sedangkan metode kuantisasi yang digunakan adalah MAQ (Patwari dkk, 2010).
2	Metode pra proses yang digunakan Interpolasi sedangkan metode kuantisasi yang digunakan adalah gabungan estimasi *fading trend* dengan extended RSS fading trend and quantization (RTQ) (Liu dkk, 2014).
3	Metode pra proses yang digunakan moving average sedangkan metode kuantisasi yang digunakan multibit ASBG dan ASBG (Jana dkk, 2009).
4	Metode pra proses yang digunakan Kalman Filter serta metode kuantisasi *Adaptive* (Ambekar dkk, 2015).
5	Metode pra proses yang digunakan Savitzky Golay Filter serta metode kuantisasi Mathur (Ali dkk, 2010).
6	Metode pra proses yang digunakan Polinomial Orde 3 serta metode kuantisasi *Adaptive* (Guillaume dkk, 2015).
7	Metode pra proses yang digunakan adalah *curve fitting* dengan regresi polinomial serta metode kuantisasi *Adaptive* (Ambekar dkk, 2012).
8	Metode pra proses yang digunakan adalah *moving average* serta kuantisasi 2-Ary (Zeng dkk, 2010)
9	Metode pra proses yang digunakan adalah DCT dan kuantisasi SKYGlow (Margelis dkk, 2018).
10	Metode pra proses yang digunakan adalah *data interleaving, smoothing* dan normalisasi. Sedangkan metode kuantisasi yang digunakan adalah Mathur (Jiang dkk, 2018).

2.7 *Advanced Encryption Standard* (AES)

AES merupakan *block cipher* yang simetris dengan panjang masing-masing blok 128 bit dan mendukung panjang kunci 128,192 dan 256 bit. Struktur enkripsi dari AES bisa dilihat pada Gambar 2.6. Terdapat 4 tahapan yang digunakan, dimana tahapan tersebut meliputi *SubByte, ShiftRows*, *MixColumns*, serta *AddRoundKey*. Proses didalam AES merupakan transformasi terhadap *state*, dimana *state* yang menjadi keluaran ronde ke k menjadi masukan untuk ronde ke k+1. Berdasarkan ukuran blok tetap, AES bekerja pada matrik berukuran 4x4 dimana tiap-tiap sel matrik terdiri atas 1 *byte*.

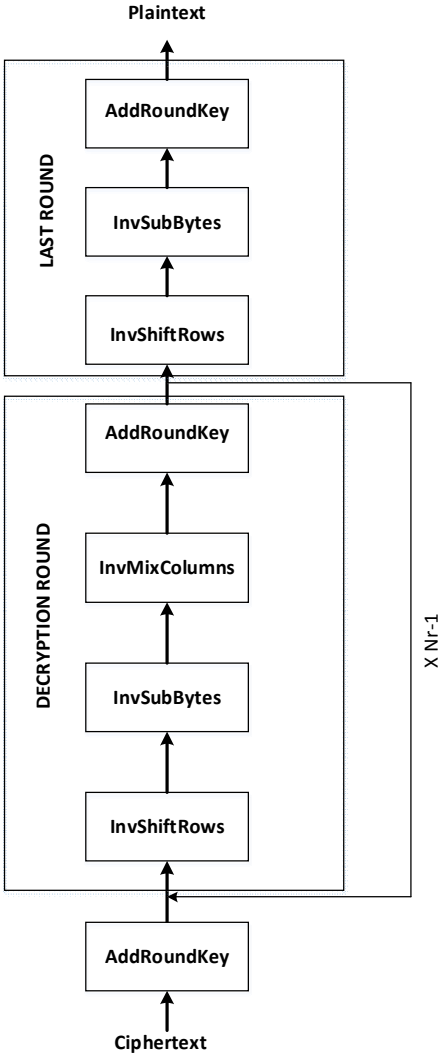


Gambar 2.6 Proses Enkripsi AES.

Transformasi pertama yaitu A*ddRoundKey* mencampur sebuah *state* masukan dengan kunci ronde menggunakan operasi ekslusif OR ($\oplus$). Setiap elemen pada *state* masukan yang merupakan sebuah *byte* dikenakan operasi ekslusif OR dengan byte pada posisi yang sama dikunci ronde (kunci ronde direpresentasikan sebagai *state*). Transformasi kedua adalah S*ubByte* yang menggunakan substitusi non linear pada ukuran byte yang disebut dengan *SubByte*. Setiap elemen pada *state* dari elemen $s_{0,0}$

sampai $s_{3,3}$ dikenakan transformasi *SubByte*. Transformasi *SubByte* dapat menggunakan tabel substitusi yaitu dengan cara menginterpretasikan byte masukan $s_{i,j}$ sebagai 2 bilangan heksadesimal. Digit kiri menunjukkan indeks baris dan indeks kanan menunjukan index kolom di tabel substitusi. Nilai *byte* pada tabel substitusi yang dirujuk oleh indeks baris dan kolom menjadi nilai yang mensubstitusi $s_{i,j}$. Selain menggunakan substitusi untuk mengganti nilai pada elemen *state*, AES menggunakan permutasi pada *state* yang dikenal dengan tranformasi *ShiftRows*. Transformasi ini dilakukan dengan menjalankan operasi pergeseran *shift left* sebanyak I pada baris ke-i dari *state*. Pada transformasi *MixColumns* dilakukan perkalian tiap elemen dari blok cipher dengan matriks yang sudah ditentukan. Operasi perkalian matrik yang digunakan adalah operasi perkalian matrik dengan operasi perkalian dan penjumlahan menggunakan operator pada GF (2^8) dengan irreducible polynomial ($x^8+x^4+x^3+x+1$). Semua transformasi tersebut akan diulang hingga *round* yang sudah ditentukan. Hasil akhir yang didapat dari proses enkripsi ini adalah *ciphertext*.

Struktur dekripsi dari AES bisa dilihat pada Gambar 2.7. Secara ringkas algoritma dekripsi merupakan kebalikan algoritma enkripsi AES. Algoritma dekripsi AES menggunakan transformasi invers semua transformasi dasar yang digunakan pada algoritma enkripsi AES. Setiap transformasi dasar AES memiliki transformasi invers yaitu *InvSubBytes*, *InvShiftRows*, dan *InvMixColumns*. *AddRoundKey* merupakan transformasi yang bersifat *self-Invers* dengan syarat menggunakan kunci yang sama dan dieksekusi sebagai inisial *round*. Perubahan pada *InvSubBytes* hanya terjadi pada tabel S-Box. Pada transformasi ini tabel S-Box yang digunakan adalah invers dari tabel S-Box yaitu S-Box^{-1}. *InvShiftRows* bekerja dengan menggeser siklik kearah berlawanan. Baris kedua digeser siklik kekanan sekali, baris ketiga dua kali dan baris keempat sebanyak tiga kali. *InvMixColumns* bekerja sebagai kebalikan dari *MixColumns*. Hasil akhir yang didapat dari proses dekripsi ini adalah *plaintext*.



Gambar 2.7 Proses Dekripsi AES

2.8 Parameter Performansi

Kami menggunakan koefisien korelasi Pearson, *Key Generation Rate* (KGR), *Key Disagreement Rate* (KDR), dan Keacakan (*Randomness*). Penjelasan parameter performansi yang digunakan bisa dilihat pada ringkasan dibawah ini.

2.8.1 Koefisien Korelasi

Parameter ini dilakukan untuk melakukan estimasi dari linear dependence RSS hasil pengukuran antara Alice dan Bob dengan memberikan nilai antara +1 hingga -1.

Nilai +1 menunjukkan korelasi yang positif, nilai -1 menunjukkan korelasi yang negatif, sedangkan nilai 0 menunjukkan tidak ada korelasi. Koefisien korelasi $\rho_{A,B}$ antara 2 data hasil pengukuran Alice dan Bob ditunjukkan oleh persamaan (2.4).

2.8.2 KGR (*Key Generation Rate*)

KGR mengacu pada jumlah bit yang bisa dibangkitkan dalam durasi waktu pembangkitan *secret key*. Parameter ini sering digunakan untuk menentukan kualitas dari protokol pembangkitan kunci. Secara spesifik terdapat 3 jenis KGR yaitu KGR setelah kuantisasi, rekonsiliasi serta *privacy amplification* seperti yang terlihat pada Persamaan (2.36) hingga (2.38). KGR_{ik} menunjukkan banyaknya bit yang dihasilkan dalam durasi waktu tahapan pembangkitan *secret key* hingga tahap kuantisasi T_{ik} , KGR_r didapat dari banyaknya bit yang mampu dikoreksi dalam durasi waktu tahapan pembangkitan *secret key* hingga tahap rekonsiliasi informasi T_r, KGR_{pa} menunjukkan banyaknya bit yang diperoleh dalam durasi waktu tahapan pembangkitan *secret key* hingga tahap *privacy amplification* T_{pa} , sedangkan n menunjukkan panjang dari bit yang dihasilkan .

$$KGR_{ik} = \frac{\sum_{i=0}^{n} K_i}{T_{ik}} \tag{2.36}$$

$$KGR_r = \frac{\sum_{i=0}^{n} S_i}{T_r} \tag{2.37}$$

$$KGR_{pa} = \frac{\sum_{i=0}^{n} \varepsilon_i}{T_{pa}} \tag{2.38}$$

Dimana K_i adalah hasil konversi bit dari parameter kanal RSS ke-i pada tahap kuantisasi, S_i adalah hasil konversi bit dari parameter kanal RSS ke-i pada tahap rekonsiliasi, dan ε_i adalah hasil konversi bit dari parameter kanal RSS ke-i pada tahap *privacy amplification*.

2.8.3 KDR (*Key Diasagreement Rate*)

Kami mendefinisikan KDR sebagai rasio dari jumlah bit yang tidak sesuai antara Alice dan Bob dengan total bit yang dihasilkan dari proses kuantisasi. Jika k_b adalah jumlah bit yang tidak sesuai dan n adalah total bit yang dihasilkan dari proses kuantisasi, maka KDR bisa didapatkan dengan menggunakan Persamaan (2.39).

$$KDR = \frac{k_b}{n} \tag{2.39}$$

Kami menggunakan KDR untuk menentukan error dari *preliminary key* yang didapat setelah proses kuantisasi. Dengan penurunan KDR maka upaya yang diperlukan untuk mendeteksi dan memperbaiki kesalahan juga menurun.

2.8.4 Keacakan (*Randomness*)

Komponen yang paling penting dari perangkat kriptografi adalah pembangkit bilangan acak. Untuk melakukan validasi keacakan dari *Pseudo-Random Number Generator* (PRNG) dilakukan uji statistik dengan menggunakan *National Institute of Standards and Technology* (NIST), dimana terdapat 15 tes yang disediakan. Masing-masing tes akan menghasilkan nilai p yang digunakan untuk menilai kualitas kunci yang dihasilkan. Tingkat signifikan yang dinotasikan dengan α mendefinisikan batas antara acak dan tidak acak. Nilai p yang lebih atau sama dengan batasan $p \geq \alpha$ dikatakan sebagai acak, jika tidak maka nilai p dikatakan tidak acak. NIST merekomendasikan nilai α antara 0,001 hingga 0,1 ($(0,001 \leq \alpha \leq 0,01)$ yang

menunjukkan bahwa keacakan rangkaian adalah benar dengan probabilitas 99%. Untuk aplikasi kriptografi nilai p yang dipilih adalah 0,01(Rukhin dkk, 2010).

Beberapa tes yang disediakan oleh NIST membutuhkan *input* yang panjang, misal panjang *input* yang direkomendasikan untuk tes *linear complexity*, dan *random excursions* adalah 10^6 dan nilai tersebut dianggap terlalu panjang untuk skema SKG. Hal inilah yang menjadi alasan mengapa kebanyakan skema SKG hanya mengadopsi sebagian dari tes keacakan (Rukhin dkk, 2010; Zhang dkk, 2016a). Pada penelitian ini hanya digunakan 6 tes keacakan dengan menggunakan NIST. Ringkasan dari 6 tes tersebut bisa dilihat pada penjelasan dibawah ini.

2.8.4.1 *Frequency (Monobit) Test*

Tujuan dari tes ini adalah untuk menentukan apakah jumlah 1 dan 0 pada kunci yang dihasilkan hampir sama seperti yang diharapkan untuk rangkaian kunci yang benar-benar acak. Bit kunci yang dihasilkan adalah acak jika $p \leq 0,01$. Panjang bit kunci adalah n, Bit kunci yang dihasilkan adalah ε dengan $\varepsilon = \varepsilon_1, \varepsilon_2, ..., \varepsilon_n$, S_n adalah $X_1 + X_2 + ... + X_n$ dimana $X_i = 2\varepsilon_i - 1$, sedangkan $s_{obs} = \frac{|S_n|}{\sqrt{n}}$. Jika nilai p terlalu kecil, maka nilai $|S_n|$ atau $|s_{obs}|$ terlalu besar. Nilai positif S_n yang terlalu besar berarti terlalu banyak bit 1, dan nilai negatif S_n yang terlalu besar berarti terlalu banyak bit 0. Panjang bit yang direkomendasikan pada tes ini adalah minimum 100 bit.

2.8.4.2 *Block Frequency Test*

Tujuan dari tes ini adalah untuk menentukan apakah frekuensi bit 1 dalam sebuah blok dengan sejumlah M bit adalah $M/2$ agar bisa memenuhi persyaratan keacakan. Jika nilai p yang dihasilkan lebih kecil dari 0,01 maka terjadi simpangan (deviasi) yang besar dari proporsi 1 dan 0 pada masing-masing blok. Bit kunci ε akan dibagi sejumlah N blok dimana $N = \left\lfloor \frac{n}{M} \right\rfloor$. Panjang bit n yang direkomendasikan adalah

minimum 100 bit dengan nilai $n \geq MN$ dan M yang dipilih harus $M \geq 20$ atau $M \geq 0,01n$ dan $N \leq 100$.

2.8.4.3 *Runs Test*

Tujuan dari tes ini adalah untuk menentukan apakah osilasi dari 0 dan 1 terlalu cepat atau terlalu lambat. Variasi osilasi disebut sebagai *run*. Jumlah bit 0 dan bit 1 sepanjang bit kunci dinotasikan sebagai $v_n(obs)$. Jika $v_n(obs)$ memiliki nilai terlalu besar maka bisa dikatakan bahwa osilasi terlalu cepat. Osilasi diasumsikan sebagai perubahan dari 1 ke 0 dan sebaliknya. Osilasi yang cepat terjadi saat terjadi terlalu banyak perubahan, misalnya 010101010. Osilasi yang rendah terjadi saat lambatnya perubahan, misalnya sebuah kunci yang terdiri dari bit 1 sepanjang 100 bit, diikuti oleh bit 0 sepanjang 73 bit, dan bit 1 sepanjang 127 bit (hanya ada 3 *run*), padahal yang diharapkan agar bit kunci yang dihasilkan adalah acak adalah adanya 150 *run.* Panjang bit n yang direkomendasikan adalah minimum 100 bit.

2.8.4.4 *Longest Run of Ones in a Block Test*

Tujuan dari tes ini adalah untuk menentukan apakah banyaknya bit 1 pada rangkaian kunci adalah konsisten dengan panjang bit 1 pada bilangan acak. Ketidakteraturan panjang bit 1 juga akan berakibat pada ketidakteraturan bit 0. Nilai yang menyatakan seberapa banyak panjang bit 1 pada sebuah blok sama dengan panjang bit 1 yang diharapkan pada sebuah blok dinotasikan dengan $\chi^2(obs)$.

2.8.4.5 *Approximate Entropy Test*

Tujuan dari tes ini adalah untuk membandingkan frekuensi dari blok yang *overlapping* dengan panjang yang berurutan. Panjang dari masing-masing blok adalah m dimana m adalah blok pertama dan $m+1$ adalah blok kedua. Nilai dari blok *overlapping* yang pertama adalah $\varphi^{(m)}$ dan blok yang kedua adalah $\varphi^{(m+1)}$, sedangkan nilai *approximate entropy* adalah $APEn(m) = \varphi^{(m)} - \varphi^{(m+1)}$. Nilai $ApEn(m)$ yang terlalu kecil

menunjukkan keteraturan yang kuat, sedangkan nilai $ApEn(m)$ yang terlalu besar menunjukkan ketidakteraturan.

2.8.4.6 *Cumulative Sums (Cusum) Test*

Tujuan dari tes ini adalah untuk menentukan apakah jumlah kumulatif dari bit kunci yang dihasilkan relatif terlalu besar atau terlalu kecil terhadap jumlah kumulatif yang diharapkan dari sebuah bit kunci yang acak. Jumlah kumulatif ini dapat dianggap sebagai jalan yang acak, dimana untuk bit kunci yang acak nilai yang didapat semakin mendekati 0. Terdapat 2 mode yang digunakan yaitu mode 0 (*forward*) dan mode 1 (*backward*). Jika yang digunakan adalah mode 0, maka nilai yang terlalu besar menunjukkan terlalu banyaknya nilai 1 atau nilai 0 di awal bit kunci. Sedangkan nilai yang terlalu besar pada mode 1 menunjukkan terlalu banyaknya nilai 1 atau 0 di akhir bit kunci.

2.8.5 Waktu Komputasi

Lamanya waktu yang dibutuhkan untuk menyelesaikan masing-masing tahapan skema SKG. Waktu komputasi sangat dipengaruhi oleh tingginya kompleksitas algoritma yang digunakan serta banyaknya data yang diolah. Semakin rendah waktu komputasi yang dibutuhkan, maka semakin sesuai algoritma tersebut diimplementasikan di perangkat dengan keterbatasan sumber daya.

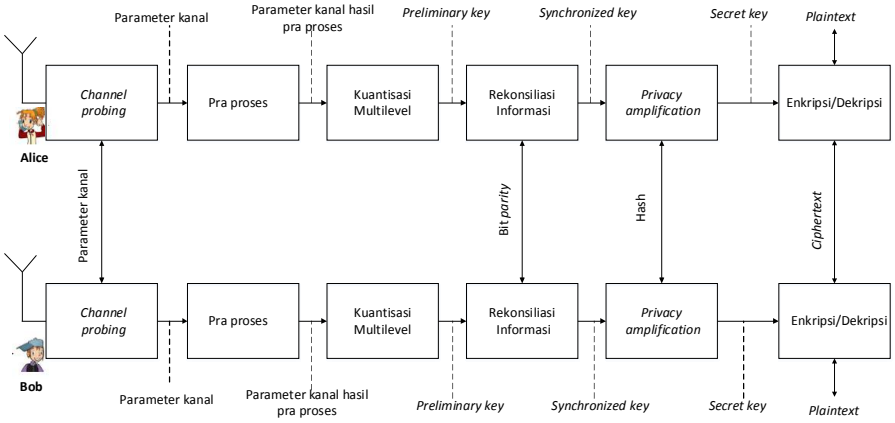
2.8.6 Komunikasi *Overhead*

Jumlah *byte* komunikasi yang dikirimkan antara kedua pengguna. Pada skema SKG komunikasi *overhead* sangat dipengaruhi oleh banyaknya *byte* informasi yang digunakan untuk sinkronisasi diantaranya saat tahap rekonsiliasi informasi serta *privacy amplification*. Semakin banyak ukuran komunikasi *overhead* maka waktu komputasi yang dibutuhkan juga semakin tinggi.

BAB 3
PENINGKATAN PERFORMANSI SKEMA SKG DENGAN KOMBINASI METODE PRA PROSES DAN KUANTISASI MULTILEVEL

3.1 Skema SKG dengan Kombinasi Metode Pra Proses dengan Kuantisasi Multilevel

Skema SKG yang kami usulkan terdiri dari 5 tahap yaitu *channel probing*, pra proses, kuantisasi multilevel, rekonsiliasi informasi, serta *privacy amplification* seperti yang terlihat pada Gambar 3.1. Dibandingkan dengan pemanfaatan 4 tahap dalam pembangkitan kunci, kami memilih untuk menggunakan 5 tahap dengan menambahkan metode pra proses sebelum kuantisasi. Beberapa penelitian (Ambekar dkk, 2012; Ali dkk, 2010) menunjukkan bahwa pemanfaatan metode pra proses dapat meningkatkan *reciprocity* parameter kanal sehingga mengurangi ketidakcocokan bit yang dihasilkan. Kuantisasi multilevel akan meningkatkan kecepatan pembangkitan *secret key* namun ketidak cocokan bit yang dihasilkan juga akan meningkat. Kombinasi metode pra proses dengan kuantisasi multilevel yang kami usulkan diharapkan dapat mengatasi *trade-off* antara kecepatan pembangkitan *secret key* dengan ketidakcocokan bit yang dihasilkan.



Gambar 3.1 Skema SKG dengan Kombinasi Metode Pra proses dengan Kuantisasi Multilevel.

Pada penelitian ini, terdapat 2 pengguna yang saling berkomunikasi untuk mendapatkan *secret key* yaitu Alice dan Bob. *Alice* ditunjuk sebagai inisiator sedangkan Bob sebagai responder. Secara garis besar terdapat lima tahap yang digunakan untuk membangkitkan *secret key*, dimana tahap tersebut meliputi *channel probing,* pra proses, kuantisasi multilevel, rekonsiliasi informasi, serta *privacy amplification*. *Channel probing* bertujuan untuk mengumpulkan parameter kanal dalam durasi waktu tertentu. Kami menggunakan *received signal strength* (RSS) sebagai parameter kanal karena banyak digunakan sebagai sumber ekstraksi untuk membangkitkan *secret key* dalam berbagai implementasi dan eksperimen (Guillaume dkk, 2015). Pra proses bertujuan untuk meningkatkan *reciprocity* (kemiripan) parameter kanal antara dua pengguna, sehingga mampu menurunkan KDR. Kuantisasi multilevel bertujuan untuk mengubah parameter kanal hasil pra proses menjadi multi bit sehingga didapatkan *preliminary key*. Rekonsiliasi informasi bertujuan untuk melakukan koreksi kesalahan bit pada *preliminary key* sehingga bisa didapatkan *synchronized key*. Tahap terakhir yaitu *privacy amplification* bertujuan untuk memastikan bahwa kualitas *secret key* yang dihasilkan memenuhi persyaratan persyaratan keacakan sedangkan verifikasi sebagai bagian dari *privacy amplification* bertujuan untuk memastikan bahwa *secret key* yang dihasilkan dua pengguna adalah sama.

Terdapat 3 metode pra proses yang digunakan yaitu Kalman Filter, Modified Polynomial Regression (MPR) serta Savitzky Golay Filter dengan beberapa alasan sebagai berikut.

1. Kalman Filter
    a. Metode Kalman Filter mampu meningkatkan *reciprocity* (kemiripan) parameter kanal RSS yang lebih optimal jika dibandingkan dengan metode pra proses yang lain karena banyaknya parameter yang dapat diubah/dimodifikasi. Peningkatan kemiripan ini berpengaruh pada menurunnya KDR yang dihasilkan.

b. Kombinasi metode Kalman Filter dan kuantisasi multilevel juga akan meningkatkan KGR yang dihasilkan. Peningkatan ini terjadi karena rendahnya KDR yang diperoleh sehingga mengurangi jumlah blok data yang dibuang karena tidak mampu dikoreksi di tahap rekonsiliasi informasi serta rendahnya waktu komputasi yang dibutuhkan dibandingkan dengan metode MPR.

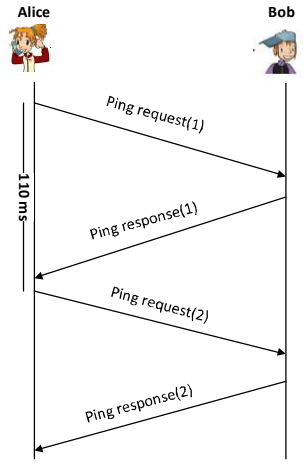
2. *Modified Polynomial Regression* (MPR)
   a. Pemanfaatan metode Regresi Polinomial sebagai metode pra proses terbukti mampu meningkatkan *reciprocity* parameter kanal RSS. Namun metode ini tidak bekerja dengan baik pada parameter kanal RSS hasil pengukuran dengan koefisien korelasi yang cukup tinggi. Hal inilah yang mendasari upaya untuk mengolah kembali parameter kanal RSS hasil pra proses tersebut dengan Moving Average sehingga bisa didapatkan peningkatan *reciprocity* parameter kanal RSS secara lebih signifikan yang ditunjukkan dengan peningkatan koefisien korelasi. Kombinasi dari kedua metode tersebut dinamakan dengan metode *Modified Polynomial Regression* (MPR). Meningkatnya koefisien korelasi juga akan berpengaruh pada penurunan KDR yang diperoleh.
   b. Kombinasi metode MPR dan kuantisasi multilevel juga akan meningkatkan KGR yang dihasilkan karena penurunan KDR yang diperoleh. Namun jika dibandingkan dengan mekanisme peningkatan performansi yang lain maka kombinasi ini menghasilkan KGR yang paling rendah karena meningkatnya waktu komputasi yang dibutuhkan. Peningkatan waktu ini terjadi karena adanya kombinasi 2 metode pra proses.

3. Savitzky Golay Filter
   a. Pemilihan metode ini didasarkan dari hasil yang diperoleh (Ali dkk, 2014) dimana metode ini mampu meningkatkan *reciprocity* parameter kanal RSS hasil pra proses secara signifikan sehingga menurunkan KDR yang diperoleh.
   b. Penelitian (Ali dkk, 2014) melakukan kombinasi metode Savitzky Golay Filter dengan kuantisasi single level sehingga KGR yang dihasilkan menjadi

rendah. Untuk mengatasi permasalahan tersebut kami menggunakan kuantisasi multilevel sehingga bisa didapatkan peningkatan KGR dari skema kombinasi yang digunakan.

3.1.1 Mekanisme *Channel Probing*

Pada tahap ini, Alice dan Bob mengumpulkan parameter kanal dengan saling mengirimkan *frame probing* dan menyimpan parameter kanal hasil pengukuran yang didapat seperti yang terlihat pada Gambar 3.2. *Frame probing* dikirim dengan menggunakan perintah ping dari protokol ICMP. Alice sebagai inisiator melakukan ping *request* dan Eve sebagai responder memberikan *response.* Nilai dari *sampling rate* r_s^{-1} yang digunakan pada *channel probing* ini adalah sebesar 110 ms, dimana *sampling rate* ini harus melebihi *coherence time* sehingga persyaratan keacakan dapat terpenuhi. *Coherence time* T_c didapat dengan mempertimbangkan kecepatan pengguna v serta frekuensi carrier f_c yang digunakan (Zenger dkk, 2015). Pada penelitian ini, kami menggunakan f_c sebesar 2,4 GHz sehingga didapatkan panjang gelombang $\lambda = c / f = 3.10^8 / 2,4.10^9 = 0,125$ m. Jika kecepatan pengguna diasumsikan 1,2 m/s maka nilai frekuensi Doppler yang didapat adalah $f_D = 1,2 / 0,125 \approx 9,6$ Hz. Sehingga nilai *coherence time* yang didapat adalah $T_c = 1 / 9,6 = 104,16$ ms.



Gambar 3.2 Mekanisme *channel probing*.

Sistem komunikasi *wireless* dilakukan oleh dua pengguna yang sah yaitu Alice dan Bob serta satu penyadap yang dikenal sebagai pihak ketiga yaitu Eve. Jika parameter kanal yang diukur oleh Alice adalah y^A dan Bob adalah y^B, maka berdasarkan prinsip channel *reciprocity* akan didapatkan kemiripan karakteristik kanal jika pengukuran dilakukan pada *coherence time*, sehingga $y^A \approx y^B$. Sejumlah n hasil pengukuran yang didapat oleh Alice dan Bob ditunjukkan oleh Persamaan (3.1) dan (3.2).

$$y^A = [y^A(1) + y^A(2) + y^A(3) + ... + y^A(n)] \quad (3.1)$$

$$y^B = [y^B(1) + y^B(2) + y^B(3) + ... + y^B(n)] \quad (3.2)$$

Diasumsikan bahwa Eve berjarak lebih dari setengah panjang gelombang dari dua pengguna yang sah sehingga y^E dan $y^{E'}$ tidak berkorelasi dengan y^A dan y^B, dimana y^E adalah karakteristik kanal yang diukur oleh Eve dari Alice dan $y^{E'}$adalah karakteristik kanal yang diukur Eve dari Bob. Sejumlah n hasil pengukuran yang didapat oleh Eve dari Alice dan Bob ditunjukkan oleh Persamaan (3.3) dan (3.4).

$$y^E = [y^E(1) + y^E(2) + y^E(3) + ... + y^E(n)] \quad (3.3)$$

$$y^{E'} = [y^{E'}(1) + y^{E'}(2) + y^{E'}(3) + ... + y^{E'}(n)] \quad (3.4)$$

3.1.2 Mekanisme Pra Proses

Tahap ini digunakan untuk meningkatkan *reciprocity* (kemiripan) parameter kanal yang dihasilkan dari tahap *channel* probing. Terdapat 3 metode pra proses yang kami gunakan yaitu Kalman Filter, *Modified Polynomial Regression* (MPR), serta Savitzky Golay Filter.

3.1.2.1 Mekanisme Kalman Filter

Parameter kanal hasil pengukuran y akan dipecah menjadi beberapa blok data N sejumlah N_B seperti yang terlihat pada Persamaan (3.5) dengan panjang masing-

masing blok adalah l dengan $l = 1,2,...,10$. Masing-masing blok akan diolah dengan menggunakan Metode Kalman Filter sehingga akan didapatkan peningkatan *reciprocity* yang lebih signifikan. Metode Kalman Filter bekerja dengan persamaan matematis yang secara rekursif memperkirakan *state* dari proses dengan menggunakan estimasi apriori dan aposteriori sehingga dapat meminimalisir nilai *mean square error* (MSE). Prediksi awal dari parameter kanal dilakukan di persamaan *time update* sedangkan proses koreksi dilakukan di persamaan *measurement update*. Persamaan *time update* dinyatakan dengan Persamaan (3.6) sedangkan *measurement update* dinyatakan dengan Persamaan (3.7).

$$\mathbf{Y} = [\mathbf{y}_1^T, ..., \mathbf{y}_N^T, ..., \mathbf{y}_{N_B}^T] \tag{3.5}$$

Dimana $\mathbf{y}_N = [y_{1,N}, ..., y_{\frac{n}{N_B},N}]$ dan $\mathbf{Y}$ merupakan matrik parameter kanal RSS sejumlah n yang dibagi-bagi kedalam N_B blok, masing-masing berisi $\frac{n}{N_B}$ data. *super script* u bisa digantikan dengan A untuk Alice dan B untuk Bob.

$$\hat{x}_k^- = A\hat{x}_{k-1} \tag{3.6}$$

$$P_k^- = AP_{k-1}A^T + Q$$

$$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1} \tag{3.7}$$

$$\hat{x}_k = \hat{x}_k^- + K_k(y_{l,N}^u - H\hat{x}_k^-)$$

$$P_k = (1 - K_k H)P_k^-$$

Detil dari mekanisme peningkatan *reciprocity* untuk tiap tiap blok data parameter kanal hasil pengukuran dengan menggunakan Kalman Filter dapat dilihat pada Algoritma 1 dan Gambar 3.3. *Input* dari algoritma ini meliputi y^u dimana *superscript* u digantikan A untuk Alice dan B untuk Bob, $\hat{x}_k^-$, P_k^- , $\hat{x}_k$, P_k , serta K_k . Kami melakukan inisialisasi untuk parameter $A, H, Q, R, \hat{x}_0, P_0$ serta panjang masing-masing

blok S_B. Pemilihan parameter tersebut dilakukan karena parameter tersebut mampu memberikan performansi yang paling optimal. Mekanisme *time update* ditunjukkan pada baris 5-6 serta baris 11-12 (Persamaan 3.6) sedangkan mekanisme *measurement update* ditunjukkan pada baris 7-9 serta 13-15 (Persamaan 3.7). Masing-masing mekanisme dilakukan berulang-ulang sebanyak paameter kanal RSS hasil pengukuran.

Algoritma 1: Kalman Filter

Input : Parameter kanal hasil pengukuran y^u

Input : Estimasi apriori $\hat{x}_k^-$, *error* kovarian apriori P_k^-

Input : Estimasi aposteriori $\hat{x}_k$, *error* kovarian aposteriori P_k, serta Kalman *Gain* K_k

Input : Jumlah blok data N_B

Output : Parameter kanal hasil pra proses z^u

1 : $A=1$, $H=1$, $Q=0.12$, $R=0.4$

2 : $\hat{x}_0=-30$, $P_0=1$

3 : $S_B=10$

4 : **for** $i \leftarrow 1$ **to** N_B **do**

5 : $\hat{x}_{k_{1,i}}^- = A.\hat{x}_0$

6 : $P_{k_{1,i}}^- = A.A.P_0 + Q$

7 : $K_{k_{1,i}} = P_{k_{1,i}}^- H / (HP_0H + R)$

8 : $P_{k_{1,i}} = P_{k_{1,i}}^- (1 - K_{k_{1,i}} H)$

9 : $\hat{x}_{k_{1,i}} = \hat{x}_{k_{1,i}}^- + K_{k_{1,i}} (y_{l,i}^u - H.\hat{x}_{k_{1,i}}^-)$

10 : **for** $j \leftarrow 2$ **to** S_B **do**

11 : $\hat{x}_{k_{j,i}}^- = A.\hat{x}_{j-1,i}$

12 : $P_{k_{j,i}}^- = A.A.P_{j-1,i} + Q$

13 : $K_{k_{j,i}} = P_{k_{j,i}}^- H / (HP_{j,i}H + R)$

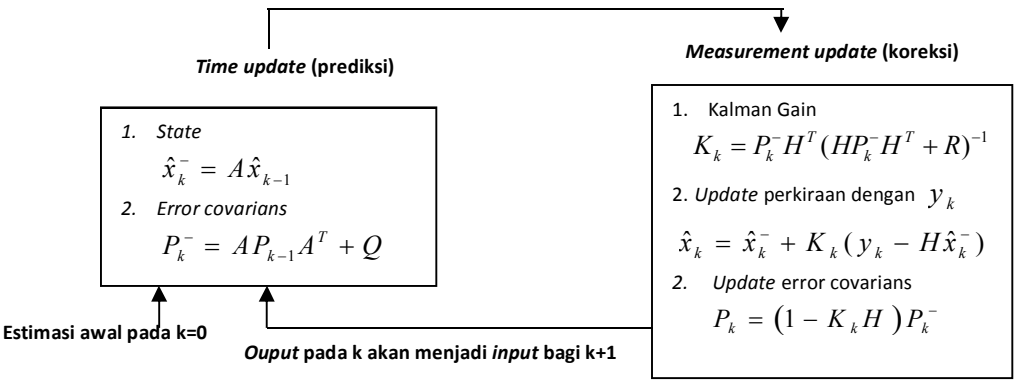
14 : $P_{k_{j,i}} = P_{k_{j,i}}^- (1 - K_{k_{j,i}} H)$

15 : $\hat{x}_{k_{j,i}} = \hat{x}_{k_{j,i}}^- + K_{k_{j,i}} (y_{j,i}^u - H.\hat{x}_{k_{j,i}}^-)$

16 : **end for**

17 : **end for**

18 : $z^u = \hat{x}_k$



Gambar 3.3 Mekanisme peningkatan *reciprocity* dengan menggunakan metode Kalman Filter.

3.1.2.2 Mekanisme *Modified Polynomial Regression* (MPR)

Peneliti (Ambekar dkk, 2012) menggunakan metode Regresi Polinomial untuk meningkatkan *channel reciprocity* dari parameter kanal. Persamaan Polinomial yang digunakan untuk menyatakan perubahan dari parameter kanal hasil pengukuran ditunjukkan dengan $h_i = a_0 + a_1 x_i + a_2 x_i^2 + ... + a_m x_i^m$, dimana $i = (1,2,3,..,n)$, h_i adalah parameter kanal hasil pra proses dari metode Regresi Polinomial sedangkan $a_0, a_1, ..., a_m$ adalah koefisien polinomial yang digunakan. Kami mengusulkan metode *Modified Polynomial Regression* (MPR) yang merupakan pengembangan dari metode Regresi Polinomial dengan mengolah kembali data hasil pra proses menggunakan Moving Average.

Parameter kanal hasil pengukuran juga akan dipecah menjadi beberapa blok data sejumlah N_B. Masing-masing blok akan diolah dengan menggunakan metode MPR sehingga akan didapatkan peningkatan *reciprocity* yang lebih signifikan. Detil mekanisme peningkatan *reciprocity* dengan menggunakan metode MPR dapat dilihat pada Algoritma 2. Input dari metode ini meliputi y^u, h^u, m, serta N_B. Inisialisasi jumlah data per blok S_B ditunjukkan pada baris 1. Penentuan koefisien polinomial dilakukan dengan menggunakan metode Eliminasi Gauss Jordan. Sedangkan mekanisme *fitting* dengan regresi polinomial ditunjukkan pada baris 3-11 sehingga bisa didapatkan parameter kanal hasil pra proses h^u. Hasil yang diperoleh akan diolah

kembali dengan menggunakan metode Moving Average seperti yang ditunjukkan pada baris 12-18.

Algoritma 2: *Modified Polynomial Regression* (MPR)

Input : Parameter kanal hasil pengukuran y^u
Input : Parameter kanal hasil pra proses dengan Regresi Polinomial h^u
Input : Orde polinomial m
Input : Jumlah blok data N_B, jumlah parameter kanal n
Output : Parameter kanal hasil pra proses z^u

1 : $S_B = 50$
2 : Penentuan koefisien polinomial dari nilai y^u per blok dengan eliminasi gauss jordan
3 : **for** $i \leftarrow 1$ **to** N_B
4 : **for** $j \leftarrow 1$ **to** S_B
5 : $sum = 0$
6 : **for** $m \leftarrow 1$ **to** m
7 : $sum = sum + a_m x_j^m$
8 : **end for**
9 : $h_{j,i} = a_0 + sum$
10 : **end for**
11 : **end for**
12 : **for** $i \leftarrow 2$ **to** n
13 : $sum = 0$
14 : **for** $k \leftarrow i-1$ **to** $k \leftarrow i+1$
15 : $sum = sum + h_k$
16 : **end for**
17 : $z_i = h_i - sum / w$
18 : **end for**
19 : $z^u = z$

3.1.2.3 Mekanisme *Savitzky Golay Filter*

Savitzky Golay Filter digunakan sebagai metode pra proses yang bertindak sebagai filter *low pass* dan melakukan *smoothing* data RSS dalam domain waktu sehinggga mampu mengurangi ketidakcocokan RSS antara dua pengguna yang sah (Ali dkk, 2014). Detil mekanisme peningkatan *reciprocity* dengan menggunakan metode Savitzky Golay Filter dapat dilihat pada Algoritma 3. *Input* dari metode ini meliputi parameter kanal hasil pengukuran y^u, Orde polinomial m, serta sampel *frame*.

Langkah pertama yang dilakukan adalah menentukan nilai dari matriks polinomial sesuai dengan banyaknya *frame* yang ditentukan. Matriks polinomial yang diperoleh dapat digunakan untuk menentukan koefisien filter c_n. Hasil terakhir yang diperoleh adalah parameter kanal hasil pra proses z^u yang diperoleh dengan mengalikan c_n dengan masing-masing parameter kanal hasil pengukuran y^u.

Algoritma 3: Savitzky Golay Filter

Input	:	Parameter kanal hasil pengukuran y^u
Input	:	Jumlah poin sebelah kiri n_L, jumlah poin sebelah kanan n_R
Input	:	Orde polinomial m, sampel frame
Output	:	Parameter kanal hasil pra proses z^u
1	:	Penentuan nilai dari matriks Polinomial sesuai dengan banyaknya sample frame
2	:	Penentuan nilai koefisien filter c_n dari persamaan Polinomial $a_0+a_1i+\ldots+a_mi$
3	:	Perkalian koefisien filter yang diperoleh dengan parameter kanal hasil pengukuran y^u sehingga diperoleh parameter kanal hasil pra proses z^u

3.1.3 Mekanisme Kuantisasi Multilevel

Kuantisasi dilakukan dengan tujuan untuk mengubah parameter kanal hasil pra proses menjadi *preliminary key*. Pada penelitian ini digunakan kuantisasi multilevel dengan tujuan untuk meningkatkan KGR dari skema SKG yang dihasilkan. Kuantisasi tersebut meliputi *Adaptive, Adaptive secret bit generation* (ASBG), *Modified* multibit (MMB), serta 2-Ary. Tiga kuantisasi selain ASBG menggunakan beberapa parameter untuk menentukan bagian parameter kanal yang akan dibuang. Sedangkan pada metode kuantisasi ASBG tidak ada parameter kanal yang dibuang.

3.1.3.1 Mekanisme Kuantisasi *Adaptive*

Kuantisasi ini bekerja dengan membagi parameter kanal hasil pra proses menjadi *preliminary key* dengan menggunakan beberapa parameter yaitu μ dan σ^2. Detil mekanisme konversi multibit dengan menggunakan metode kuantisasi mutilevel *adaptive* dapat dilihat pada Algoritma 4. *Input* dari metode ini adalah z^u dan N_B. Langkah pertama yang dilakukan adalah penentuan jumlah blok data S_B serta level kuantisasi sesuai dengan Persamaan (2.22) seperti yang terlihat pada baris 1-2. Konversi level kuantisasi kedalam bentuk bit dengan menggunakan *Gray coding* dapat dilihat pada baris 3-6, dimana mekanisme konversi tersebut dilakukan di masing-masing blok data.

3.1.3.2 Mekanisme Kuantisasi *Adaptive secret bit generation* (ASBG)

Algoritma 5 menunjukkan mekanisme kuantisasi dengan menggunakan metode ASBG. Pada mekanisme kuantisasi ini tidak ada pembagian blok data dari parameter kanal hasil pra proses. Langkah pertama yang dilakukan adalah mengurutkan nilai RSS hasil pra proses dan menentukan *range* dari data tersebut seperti yang terlihat pada baris 1. Mekanisme penentuan jumlah bit yang akan diekstrak, pembagian *range*, serta konversi level kuantisasi kedalam bentuk bit ditunjukkan pada baris 2-4. Jumlah maksimal bit C yang dapat diekstrak dari tiap-tiap nilai RSS harus kurang dari sama dengan $\lfloor \log_2 range \rfloor$. Setelah menentukan nilai C, maka *range* tersebut akan dibagi kedalam ukuran interval L yang sama. Hasil akhir dari mekanisme ini adalah *preliminary key* yang didapatkan dari ekstraksi masing-masing nilai RSS hasil pra proses kedalam bentuk bit dengan menggunakan *Gray Coding*. Berbeda dengan kuantisasi multilevel adaptive, tidak ada parameter kanal pra proses yang dibuang pada mekanisme konversi bit yang dilakukan pada kuantisasi ini. Kondisi ini mengakibatkan lebih banyaknya jumlah bit *preliminary key* yang dihasilkan.

Algoritma 4: Kuantisasi multilevel Adaptive

Input : Parameter kanal hasil pra proses z^u

Input : Jumlah blok data N_B

Output : *Preliminary key* K^u

1 : Penentuan jumlah data dalam blok data S_B

2 : Penentuan level kuantisasi sesuai dengan persamaan (2.22)

3 : **REPEAT**

4 : Untuk masing-masing blok data sepanjang S_B dilakukan konversi level kuantisasi ke dalam bentuk bit dengan menggunakan Gray Coding $Q(z^u)$, dimana level kuantisasi 1(00), 2(01), 3(11), dan 4(10).

5 : Membuang parameter kanal hasil pra proses diluar level

6 : **UNTIL** jumlah blok data N_B

7 : $K^u = Q(z^u)$

Algoritma 5: Kuantisasi Multibit ASBG

Input : Parameter kanal hasil pra proses z^u

Output : *Preliminary key* K^u

1 : Mengurutkan nilai RSS hasil pra proses z^u, dan menentukan *range* dari nilai minimum dan maksimum data tersebut.

2 : Menentukan nilai C yang merupakan jumlah bit yang dapat diekstrak dari tiap RSS, dimana $C \le \lfloor \log_2 range \rfloor$

3 : Membagi range kedalam $L = 2^C$ ukuran interval yang sama

4 : Mengubah z^u dimasing-masing interval kedalam C bit dengan menggunakan Gray Coding $Q(z^u)$, dimana level kuantisasi 1(00), 2(01), 3(11), dan 4(10).

5 : $K^u = Q(z^u)$

3.1.3.3 Mekanisme Kuantisasi *Modified Multibit* (MMB)

Mekanisme kuantisasi dengan menggunakan metode MMB ditunjukkan pada Algoritma 6. Kuantisasi ini bekerja dengan membagi parameter kanal hasil pra proses menjadi *preliminary key* dengan menggunakan beberapa parameter yaitu μ, α dan σ. Parameter α bernilai antara 0 hingga 1. *Input* dari metode ini adalah z^u dan N_B. Langkah pertama yang dilakukan adalah penentuan jumlah blok data S_B serta level kuantisasi sesuai dengan Persamaan (2.23) seperti yang terlihat pada baris 1-2.

Konversi level kuantisasi kedalam bentuk bit dengan menggunakan *Gray coding* dapat dilihat pada baris 3-6, dimana mekanisme konversi tersebut dilakukan di masing-masing blok data.

3.1.3.4 Mekanisme Kuantisasi 2-Ary

Algoritma 7 menunjukkan mekanisme kuantisasi dengan menggunakan metode 2-Ary. Tidak ada pembagian blok dari parameter kanal pra proses yang akan dikonversi menjadi bit. Baris 1-2 menunjukkan penentuan interval kuantisasi, dimana interval ini tergantung dari jumlah level kuantisasi L yang dipilih. Terdapat beberapa parameter kanal hasil pra proses yang akan dibuang dengan tujuan untuk mengurangi ketidacocokan bit yang dihasilkan kedua pengguna. Penentuan banyaknya parameter kanal hasil pra proses yang akan dibuang dan diolah ditunjukkan pada baris 3, sedangkan konversi kedalam bentuk bit ditunjukkan pada baris 4. Parameter kanal RSS yang berada diluar level kuantisasi akan dibuang.

Algoritma 6: Kuantisasi multilevel Modified Multibit (MMB)		
Input	:	Parameter kanal hasil pra proses z^u
Input	:	Jumlah blok data N_B
Output	:	*Preliminary key* K^u
1	:	Penentuan jumlah data dalam blok data S_B
2	:	Penentuan level kuantisasi sesuai dengan persamaan (2.23)
3	:	**REPEAT**
4	:	Untuk masing-masing blok data sepanjang S_B dilakukan konversi level kuantisasi ke dalam bentuk bit dengan menggunakan Gray Coding $Q(z^u)$, dimana level kuantisasi 1(01), 2(00), 3(10), dan 4(11).
5	:	Membuang parameter kanal hasil pra proses yang berada diluar level kuantisasi
6	:	**UNTIL** jumlah blok data N_B
7	:	$K^u = Q(z^u)$

Algoritma 7: Kuantisasi 2-Ary

Input : Parameter kanal hasil pra proses z^u

Output : *Preliminary key* K^u

1 : Penentuan jumlah level kuantisasi L.

2 : Penentuan interval kuantisasi sesuai jumlah L yang ditentukan $I_0 = (q_0, q_1 - g_1), I_1 = (q_1, q_2 - g_2), ..., I_{L-1} = (q_{L-1}, q_L)$.

3 : Penentuan parameter kanal hasil pra proses yang akan diolah dengan menggunakan $\int_{q_{i-1}}^{q_i - g_i} f_z dz = \frac{1-\alpha}{L}$, serta parameter kanal yang akan dibuang dengan $\int_{q_i - g_i}^{q_i} f_z dz = \frac{\alpha}{L-1}$ dengan $i = 1, ..., L-1$.

4 : Konversi level kuantisasi ke dalam bentuk bit dengan menggunakan Gray Coding $Q(z^u)$, dimana level kuantisasi 1(01), 2(00), 3(10), dan 4(11).

5 : Membuang parameter kanal hasil pra proses yang berada diluar level kuantisasi

6 : $K^u = Q(z^u)$

3.1.4 Mekanisme Rekonsiliasi Informasi

Tidak simultannya pengukuran yang dilakukan serta faktor *noise* memicu didapatkannya ketidakcocokan bit dari *preliminary key* K^u hasil kuantisasi. Hal ini diatasi dengan pemanfaatan metode rekonsiliasi informasi yang bertujuan untuk melakukan koreksi terhadap ketidakcocokan bit antara dua pengguna. Pada penelitian ini kami menggunakan kode BCH (255,k) sebagai metode untuk rekonsiliasi informasi dengan kemampuan koreksi hingga 25% (Zhang dkk, 2016a) sehingga diharapkan tidak banyak bit data yang terbuang karena tidak mampu dikoreksi. Sisa dari *preliminary key* yang tidak terbuang disebut sebagai *synchronized key* S^u.

3.1.5 Mekanisme *Privacy Amplification*

Pada tahap ini terdapat mekanisme peningkatan keacakan untuk memastikan kecukupan entropy dari *secret key* ε^u yang dihasilkan serta verifikasi untuk menjamin bahwa *secret key* yang dihasilkan kedua pengguna adalah sama. Mekanisme peningkatan keacakan menggunakan Universal Hash function (Carter dkk, 1979),

sedangkan verifikasi dilakukan dengan menggunakan SHA-256. *Secret key* yang diperoleh sepanjang 256 bit akan digunakan untuk mengacak pesan yang dikirim serta mengembalikan pesan yang teracak kedalam bentuk pesan semula.

3.2 Parameter Performansi dari Skema SKG dengan Kombinasi Metode Pra Proses dan Kuantisasi Multilevel

Terdapat 4 parameter performansi yang digunakan untuk melakukan evaluasi terhadap skema SKG yang dibangun, dimana parameter tersebut meliputi :

1. Koefisien korelasi : Parameter ini digunakan untuk menunjukkan ketergantungan antara parameter kanal hasil pengukuran Alice dan Bob seperti yang ditunjukkan pada persamaaan (2.4). Nilai yang dihasilkan berkisar antara 1 hingga -1, dimana nilai 1 menunjukkan ketergantungan yang mutlak sedangkan nilai -1 menunjukkan ketergantungan yang berlawananan. Penghitungan koefisien korelasi dilakukan pada parameter kanal hasil pengukuran serta parameter kanal hasil pra proses sehingga bisa diketahui keberhasilan peningkatan *reciprocity* dari pengembangan metode pra proses yang dilakukan. Semakin mendekati 1 maka semakin tinggi *reciprocity* parameter kanal yang didapat kedua pengguna.
2. *Key Generation Rate* (KGR) : Parameter ini digunakan untuk menentukan kecepatan pembangkitan *secret key.* Terdapat 3 jenis KGR yang akan dianalisa pada bagian ini yaitu KGR_{ik}, KGR_r serta KGR_{pa}. KGR_{ik} menunjukkan kecepatan pembangkitan *preliminary key*, KGR_r menunjukkan kecepatan pembangkitan *synchronized key*, sedangkan KGR_{pa} menunjukkan kecepatan pembangkitan *secret key*. Tujuan dari disain skema SKG ini adalah melakukan *refresh secret key* setiap 1 jam sesuai dengan standarisasi IEEE 802.1x (Moore, 2001).
3. *Key Disagreement Rate* (KDR) : Parameter ini digunakan untuk mengetahui ketidakcocokan bit yang dihasilkan setelah tahap kuantisasi. Nilai KDR yang diperoleh merupakan jumlah nilai bit yang berbeda terhadap total bit yang dihasilkan setelah tahap kuantisasi. Semakin tinggi nilai KDR yang dihasilkan akan mengurangi nilai KGR_r dan KGR_{pa} yang dihasilkan.

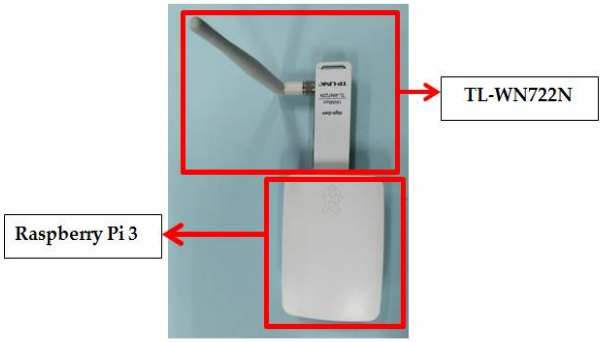
4. *Randomness* (keacakan) : Terdapat 6 jenis tes keacakan dari National Institute of Standards and Technology (NIST) yang akan digunakan untuk melakukan validasi terhadap secret key yang dihasilkan. Tes tersebut meliputi *Approximate Entropy*, *Frequency (monobit), block frequency, runs, Longest Run of Ones in a Block* (LROB), serta *Cumulative Sums (Cusum)* untuk masing-masing pengujian. Nilai p digunakan untuk menentukan kualitas dari kunci yang dihasilkan, sedangkan *significance level* α digunakan untuk menentukan batas antara acak dan tidak acak. Jika nilai $p \geq \alpha$, maka kunci dinyatakan memenuhi persyaratan keacakan. NIST merekomendasikan nilai $0,001 \leq \alpha \leq 0,01$.

3.3 Skenario Pengujian Eksperimental

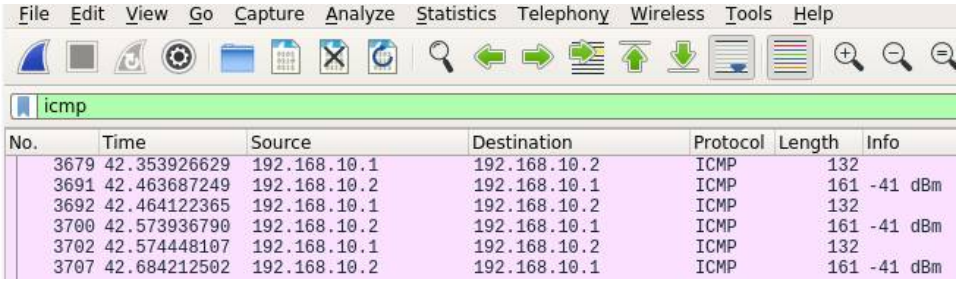
Pada bagian ini dijelaskan tentang skenario pengujian yang meliputi jenis perangkat/*software* yang digunakan serta skenario pengukuran. Bagian perangkat/*software* berisi tipe perangkat/*software* serta jumlah perangkat yang digunakan, sedangkan skenario pengukuran berisi mekanisme pengukuran serta lingkungan pengujian.

3.3.1 Perangkat/*Software* yang Digunakan

Kami mengimplementasikan skema SKG yang dibangun dengan menggunakan 3 perangkat Raspberry Pi 3 yang bertindak sebagai Alice, Bob dan Eve. Alice bertindak sebagai inisiator, Bob sebagai responder sedangkan Eve sebagai penyadap. Setiap perangkat dilengkapi dengan TP-Link TL-WN722N WiFi USB *adapter* dan beroperasi di mode 802.11b seperti yang terlihat pada Gambar 3.4. Frekuensi *carrier* yang digunakan adalah 2,4 GHz, sedangkan pada tahap *channel probing,* ping *request* dilakukan secara periodik dari Alice ke Bob setiap 110 ms. Masing-masing pengguna dilengkapi dengan *software Wireshark* yang berada di mode monitor untuk menyimpan parameter kanal RSS hasil pengukuran di tahap *channel probing* seperti yang terlihat pada Gambar 3.5. Eve juga berada di mode monitor untuk menyimpan parameter kanal RSS dari Alice dan Bob. Jumlah parameter kanal RSS yang tersimpan pada skenario 1 hingga 4 adalah 10.000.



Gambar 3.4 Raspberry Pi 3 dan TP-Link TL-WN722N WiFi USB *adapter*.



Gambar 3.5 Mekanisme penyimpanan parameter kanal RSS dengan *Wireshark*.

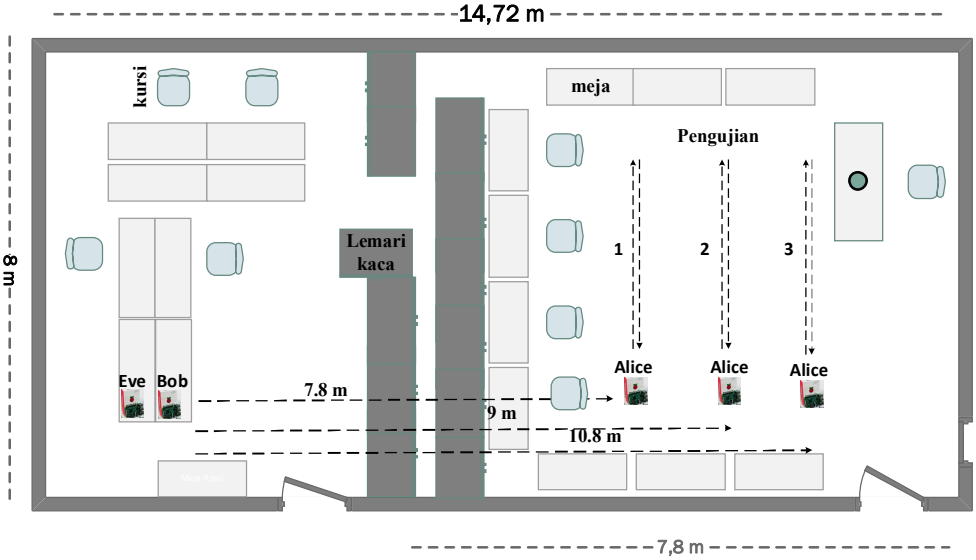
3.3.2 Skenario Pengukuran

Terdapat 4 skenario pengukuran yang digunakan pada bagian ini yaitu skenario 1 hingga 4. Perbedaan masing-masing skenario terletak pada mekanisme pengukuran yang dilakukan serta kondisi lingkungan pengujian.

3.3.2.1 Skenario 1 hingga 3

Pada skenario ini, pengujian dilakukan pada siang hari di sebuah ruangan dengan panjang 14,72 meter dan lebar 8 meter. Alice berjalan sesuai dengan lintasan yang ditunjukkan pada Gambar. 3.6 dengan kecepatan sekitar 1,2 m/s, sedangkan Bob dan Eve diam dengan jarak yang sangat dekat (10 cm). Ruangan terdiri dari meja, kursi, dan lemari kaca serta memiliki dua pintu. Alice dan Bob terhalang lemari berbahan kaca dan alumunium. Tidak ada orang yang berlalu lalang pada saat pengukuran. Terdapat 3 skenario yang akan dijelaskan pada bagian ini, dimana perbedaan masing-

masing skenario terletak pada jarak pengukuran yang dilakukan. Alice memulai c*hannel probing* pada jarak 7,8 m (skenario 1), 9 m (skenario 2), serta 10,8 m (skenario 3) dari Bob. Pada masing-masing skenario, Alice berjalan lurus bolak balik dengan variasi jarak antara 7,8 m hingga 8,8 m (skenario 1), 9 m hingga 9,8 m (skenario 2), 10,8 m hingga 11,5 m (skenario 3). Detil kondisi lingkungan ruang pengukuran terlihat pada Gambar 3.7.

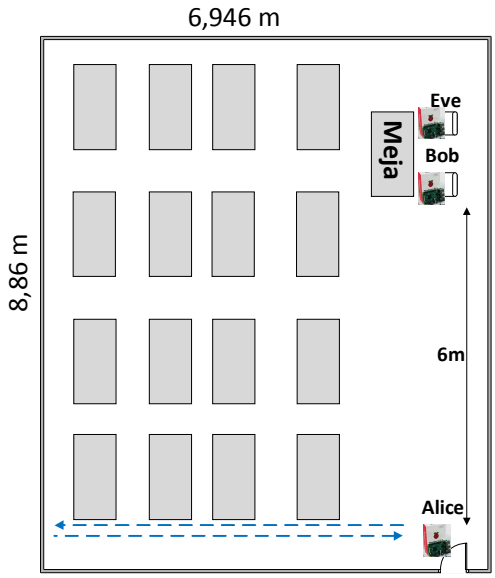


Gambar 3.6 *Lay out* skenario 1 hingga 3.

Gambar 3.7 Lingkungan ruang pengukuran skenario 1 hingga 3.

3.3.2.2 Skenario 4

Pada skenario ini, pengujian dilakukan pada siang hari di ruangan dengan panjang 6,946 meter dan lebar 8,86 meter. Alice berjalan lurus dengan kecepatan 1,2 m/s mengikuti jalur biru seperti yang ditunjukkan oleh Gambar 3.8 sedangkan Bob dan Eve diam dengan jarak 10 cm. Jarak dari Alice ke Bob adalah 6 hingga 9,05 m. Pengujian dilakukan saat siang hari dan tidak ada orang yang berlalu lalang saat pengujian. Detil lingkungan ruang pengukuran dapat dilihat pada Gambar 3.9.



Gambar 3.8 *Lay out* skenario 4.

Gambar 3.9 Lingkungan ruang pengukuran skenario 4.

3.4 Skema SKG dengan Kombinasi Metode Kalman Filter dan Kuantisasi Multilevel

Bagian ini bertujuan untuk menguji performansi skema SKG dengan kombinasi metode Kalman Filter dan kuantisasi multilevel. Pengujian dilakukan secara simulasi dan divalidasi dengan eksperimen di lingkungan riil.

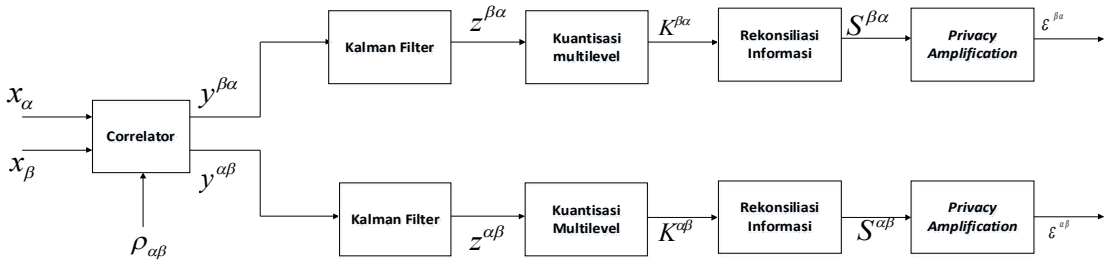
3.4.1 Simulasi Monte Carlo untuk Skema SKG dengan Kombinasi Metode Kalman Filter dan Kuantisasi Multilevel

Kami menggunakan simulasi Monte Carlo dengan menggunakan lingkungan simulasi yang ditunjukkan pada Gambar 3.10. Dua bilangan acak yang *independent* dengan panjang data $n = 10.000$, $x_\alpha = [x_\alpha(1), x_\alpha(2), \ldots, x_\alpha(n)]^T$ dan $x_\beta = [x_\beta(1), x_\beta(2), \ldots, x_\beta(n)]^T$ saling berkorelasi dengan distribusi Rayleigh. Kami menggunakan koefisien korelasi Pearson $\rho_{\alpha\beta}$ yang bernilai 0,6 dan 0,8 sebagai tingkat *reciprocity* antara estimasi parameter kanal $y^{\beta\alpha}$ dan $y^{\alpha\beta}$ dari pengguna α dan β (dengan $\alpha, \beta \in \{A, B, E\}$ dan $\alpha \neq \beta$. Pemilihan nilai koefisien korelasi tersebut disesuaikan dengan nilai parameter kanal hasil pengukuran di bagian eksperimental. $\rho_{\alpha\beta}$ digunakan sebagai korelator yang mengkorelasikan variabel acak x_α dan x_β untuk menciptakan estimasi *reciprocity* yang tidak sempurna antara $y^{\beta\alpha}$ dan $y^{\alpha\beta}$. Seperti yang telah ditunjukkan oleh (Gene dkk, 2012), estimasi tersebut dapat ditunjukkan dengan menggunakan *Cholesky Decomposition* dari kovarian matriks C yang tergantung pada $\rho_{\alpha\beta}$. Jika $y^{\beta\alpha} = x_\alpha$ maka

$$y^{\alpha\beta} = \rho_{\alpha\beta} y^{\beta\alpha} + x_\beta \sqrt{1 - \rho_{\alpha\beta}^2} \tag{3.8}$$

Estimasi parameter kanal $y^{\beta\alpha}$ dan $y^{\alpha\beta}$ akan diolah dengan metode Kalman Filter untuk mendapatkan parameter kanal hasil pra proses $z^{\beta\alpha}$ dan $z^{\alpha\beta}$. Pemanfaatan metode tersebut dilakukan untuk meningkatkan *reciprocity* dari estimasi parameter kanal. Kuantisasi dilakukan dengan menggunakan beberapa kuantisasi multilevel yaitu

Adaptive, MMB, dan 2-Ary untuk mendapatkan *preliminary key* $K^{\beta\alpha}$ dan $K^{\alpha\beta}$. Perbedaan bit yang terjadi akan dikoreksi di tahap rekonsiliasi informasi dengan menggunakan BCH (255,87). Blok bit dari *preliminary key* yang tidak mampu dikoreksi akan dibuang dan sisa dari blok bit tersebut akan menjadi *synchronized key* $S^{\beta\alpha}$ dan $S^{\alpha\beta}$. Bit dari *synchronized key* akan masuk di tahap *privacy amplification* sehingga bisa didapatkan *secret key* $\varepsilon^{\beta\alpha}$ dan $\varepsilon^{\alpha\beta}$.



Gambar 3.10 Model simulasi skema SKG dengan metode pra proses Kalman Filter.

Evaluasi terhadap performansi skema SKG dengan kombinasi metode Kalman Filter dan kuantisasi multilevel dilakukan dengan mengimplementasikan skema SKG di Matlab dengan nilai koefisien korelasi 0,6 dan 0,8. Terdapat 2 evaluasi yang akan dilakukan yaitu peningkatan *reciprocity* dengan menggunakan metode Kalman, serta pengujian parameter KDR dan KGR dari masing-masing tahap. Detil Parameter yang digunakan dalam simulasi ditunjukkan pada Tabel 3.1. Perbedaan dari Kalman Filter eksisting dan Kalman Filter yang diusulkan terletak pada mekanisme pengolahan estimasi parameter kanal yang dihasilkan. Pada Kalman Filter yang diusulkan, estimasi parameter kanal akan dibagi menjadi beberapa blok data. Masing-masing blok data akan diolah dengan menggunakan metode Kalman Filter. Sedangkan pada Kalman Filter yang eksisting tidak ada pembagian estimasi parameter kanal menjadi blok.

Tabel 3.1 Parameter simulasi skema SKG dengan kombinasi metode Kalman Filter dan kuantisasi multilevel.

No	Parameter	Keterangan
1	Jumlah data	10.000
2	Distribusi data x_α dan x_β	Rayleigh dengan varian=4
3	Kalman Filter yang eksisting	$A=1, H=1, Q=0,12, R=0,4, S_B=10.000$
4	Kalman Filter yang diusulkan	$A=1, H=1, Q=0,12, R=0,4, S_B=10$
5	Kuantisasi *adaptive*	$S_B = 50$
6	Kuantisasi MMB	$\alpha = 0,002$
7	Kuantisasi 2-Ary	$\alpha = 0,1$
8	Metode rekonsiliasi informasi	BCH(255,87)
9	Metode *privacy amplification*	Universal hash untuk 256 bit serta SHA-256

Tabel 3.2 menunjukkan peningkatan koefisien korelasi dari estimasi parameter kanal $y^{\alpha\beta}, y^{\beta\alpha}$ dengan menggunakan metode pra proses Kalman Filter yang eksisting dan Kalman Filter yang diusulkan. Hasil pengujian yang dilakukan menunjukkan adanya peningkatan koefisien korelasi $z^{\alpha\beta}, z^{\beta\alpha}$ yang signifikan dari hasil pra proses menggunakan Kalman Filter yang diusulkan (Algoritma 1). Pembagian estimasi parameter kanal kedalam bentuk blok menyebabkan semakin banyak blok data yang mengalami peningkatan koefisien korelasi sehingga meningkatkan koefisien korelasi secara keseluruhan. Peningkatan koefisien korelasi tertinggi diperoleh saat jumlah data dalam blok sebanyak 10. Tabel 3.3 menunjukkan perbandingan KDR yang dihasilkan dari tiap-tiap skema yang digunakan. Skema 1 hingga 3 menggunakan sistem *direct* kuantisasi dengan kuantisasi multilevel yang digunakan adalah *Adaptive* (skema 1), MMB (skema 2), serta 2-Ary (skema 3). Skema 4 menggunakan gabungan Kalman Filter yang eksisting dengan kuantisasi *Adaptive*. Skema usulan 1 menggunakan mekanisme yang telah dijelaskan pada Algoritma 1 dan 4. Untuk pengujian keamanan, dengan cara yang sama kami membangkitkan dua bilangan acak dengan panjang

$n = 10.000$, $x_e = [x_e(1), x_e(2), ..., x_e(n)]^T$ yang berkorelasi dengan x_α berdistribusi Rayleigh dan $x_{e'} = [x_{e'}(1), x_{e'}(2), ..., x_{e'}(n)]^T$ yang berkorelasi dengan x_β berdistribusi Rician. Estimasi parameter kanal yang diperoleh adalah $y^{\alpha e}$ dan $y^{\beta e'}$. Diasumsikan $y^{\alpha\beta}$ dan $y^{\beta\alpha}$ adalah data dari pengguna yang sah yang memiliki koefisien korelasi tinggi, sedangkan $y^{\alpha e}$ dan $y^{\beta e'}$ adalah data dari penyadap yang memiliki koefisien korelasi sangat rendah.

Tabel 3.2 Peningkatan koefisien korelasi hasil simulasi dengan menggunakan Kalman Filter.

Koefisien korelasi $y^{\alpha\beta}, y^{\beta\alpha}$	**Kalman Filter eksisting**	**Peningkatan koefisien korelasi per**			
		10	**20**	**40**	**50**
0,81	0,8124	0,9859	0,9798	0,9677	0,9617
0,69	0,7019	0,9774	0,9679	0,9478	0,9401
0,65	0,6517	0,9738	0,9628	0,9401	0,9283

Tabel 3.3 Perbandingan KDR hasil simulasi antara skema 1-4 serta usulan 1.

Estimasi parameter kanal	**Koefisien korelasi**	**KDR**				
		Skema 1	**Skema 2**	**Skema 3**	**Skema 4**	**Skema usulan 1**
$y^{\alpha\beta}$ dan $y^{\beta\alpha}$	0,81	0,2647	0,2548	0,2601	0,2282	0,0217
$y^{\beta\alpha}$ dan $y^{\alpha e}$	0,007	0,4900	0,5550	0,4903	0,4118	0,6348
$y^{\alpha\beta}$ dan $y^{\beta e'}$	0,014	0,4950	0,5646	0,4987	0,3930	0,6414
$y^{\alpha\beta}$ dan $y^{\beta\alpha}$	0,69	0,3171	0,2616	0,3176	0,2611	0,0286
$y^{\beta\alpha}$ dan $y^{\alpha e}$	0,014	0,4938	0,5548	0,5001	0,4104	0,6303
$y^{\alpha\beta}$ dan $y^{\beta e'}$	0,014	0,4950	0,5652	0,5016	0,3995	0,6422
$y^{\alpha\beta}$ dan $y^{\beta\alpha}$	0,65	0,3371	0,2624	0,3391	0,2841	0,0296
$y^{\beta\alpha}$ dan $y^{\alpha e}$	0,007	0,4918	0,5565	0,4918	0,3994	0,6312
$y^{\alpha\beta}$ dan $y^{\beta e'}$	0,010	0,4940	0,5683	0,5042	0,3887	0,6415

Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 1 menunjukkan nilai KDR $K^{\alpha\beta}$ dan $K^{\beta\alpha}$ yang lebih rendah dibandingkan dengan skema yang lain pada semua data dengan variasi nilai koefisien korelasi. Hal ini tejadi karena skema usulan 1 menggunakan data hasil pra proses yang memiliki koefisien korelasi yang tinggi sehingga kemungkinan untuk mendapatkan bit yang sama juga tinggi. Kondisi ini mengakibatkan lebih rendahnya nilai KDR yang diperoleh. Pada pengujian keamanan, diasumsikan penyadap mengetahui algoritma pra proses dan kuantisasi yang digunakan namun tidak mengetahui parameter dari masing-masing algoritma tersebut. Analisa keamanan dilakukan dengan melakukan rekonsiliasi informasi terhadap bit hasil kuantisasi yang diperoleh. Secara keseluruhan terlihat bahwa skema SKG hasil simulasi yang dibangun dapat memenuhi persyaratan keamanan karena KDR dari $K^{\beta\alpha}$, $K^{\alpha e}$ serta $K^{\alpha\beta}$, $K^{\beta e'}$ skema usulan 1 telah melebihi 0,4 sehingga sulit bagi penyadap untuk mendapatkan *preliminary key* yang sama pada saat tahap rekonsiliasi informasi.

Tabel 3.4 menunjukkan KGR yang dihasilkan dari semua skema. KGR_{ik} yang diperoleh setelah kuantisasi cenderung stabil untuk semua data dengan variasi nilai koefisien korelasi. Hal ini terjadi karena pada tahap ini faktor penentu KGR yang utama adalah metode kuantisasi yang digunakan serta waktu komputasi dari masing-masing proses. Perbedaan terlihat saat KGR_r karena saat tahap ini blok data yang tidak mampu dikoreksi akan dibuang. Semakin tinggi nilai KDR maka KGR_r yang dihasilkan juga akan semakin rendah. Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 1 memiliki KGR_r yang lebih tinggi jika dibandingkan dengan skema yang lain pada data dengan variasi nilai koefisien korelasi. Hal ini terjadi karena skema yang diusulkan memiliki KDR yang lebih rendah sehingga tidak banyak blok data yang terbuang. Hasil dari KGR_{pa} tidak terlalu berbeda dengan KGR_r karena pada tahap ini nilai yang dihasilkan hanya tergantung dari waktu komputasi dari *privacy amplification*

.

Tabel 3.4 Perbandingan KGR hasil simulasi antara skema 1-4 serta usulan 1.

Koefisien korelasi	KGR	Skema 1	Skema 2	Skema 3	Skema 4	Skema usulan 1
0,81	KGR_{ik} (bps)	3642,99	3606,91	3214,29	669,12	670,24
	KGR_{r} (bps)	51,57	58,77	48,80	56,60	60,93
	KGR_{pa} (bps)	48,67	55,58	46,23	53,71	57,86
0,69	KGR_{ik} (bps)	3683,24	3604,36	3185,84	668,90	671,37
	KGR_{r} (bps)	28,71	54,06	23,59	46,68	60,89
	KGR_{pa} (bps)	27,19	51,11	22,22	44,44	57,83
0,65	KGR_{ik} (bps)	3686,64	3585,53	3396,23	670,69	670,47
	KGR_{r} (bps)	19,53	5,47	15,79	40,30	60,87
	KGR_{pa} (bps)	18,49	51,77	14,95	38,55	57,88

3.4.2 Hasil Eksperimen Skema SKG dengan Kombinasi Metode Kalman Filter dan Kuantisasi Multilevel

Pada bagian ini akan dibahas evaluasi performansi dari hasil eksperimen yang dilakukan pada skenario 1 hingga 3. Evaluasi yang dilakukan meliputi evaluasi peningkatan *reciprocity* dengan menggunakan metode kalman Filter serta evaluasi parameter performansi KDR, KGR serta *randomness* (keacakan).

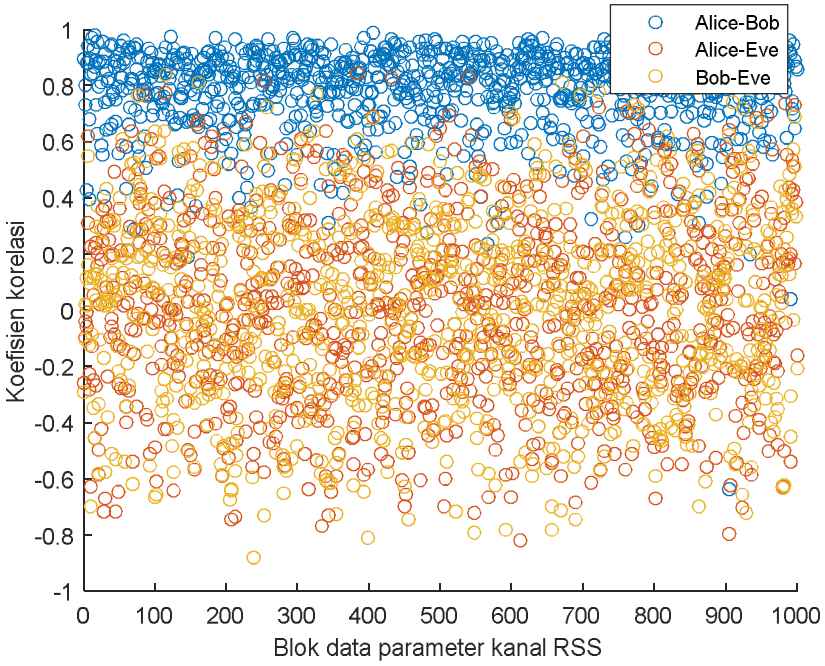
3.4.2.1 Evaluasi Peningkatan *Reciprocity* dengan Menggunakan Metode Kalman Filter

Range nilai parameter kanal RSS hasil pengukuran dari 2 pengguna yang sah pada 3 skenario adalah -77 dBm hingga -48 dBm, dengan korelasi awal untuk masing-masing skenario bisa dilihat pada Tabel 3.5. Pada penelitian ini, nilai korelasi yang dihasilkan antara Alice dan Bob pada semua skenario lebih dari 0,5, sedangkan nilai korelasi antara pengguna yang sah dengan penyadap sangat kecil yaitu dibawah 0,5.

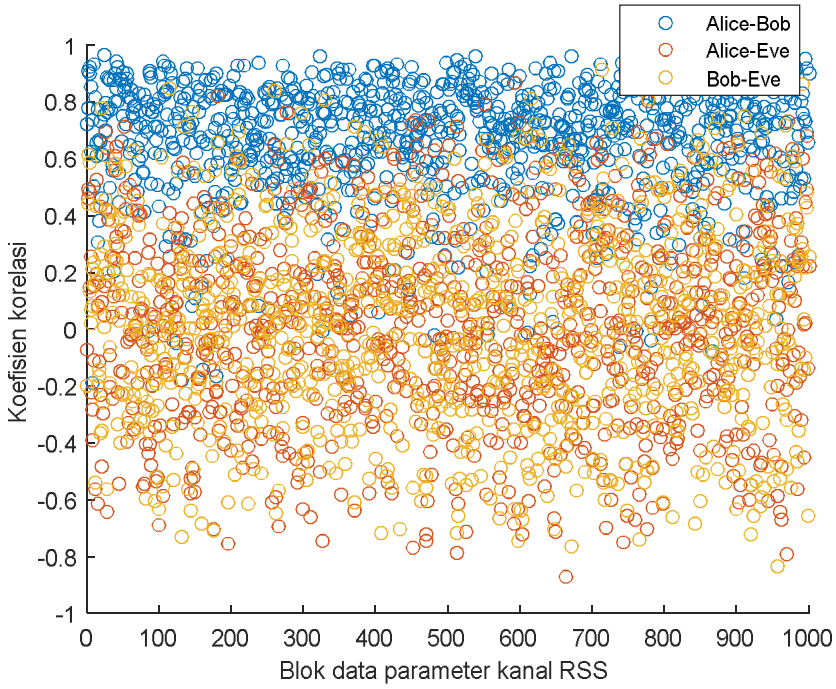
Hal ini mengakibatkan sulitnya penyadap untuk mendapatkan kunci yang sama dengan Eve. Hasil pengukuran juga menunjukkan bahwa semakin jauh jarak pengukuran maka semakin banyak data parameter kanal RSS yang berbeda antara Alice dan Bob sehingga korelasi yang didapatkan juga semakin rendah. Detil nilai korelasi dari parameter kanal RSS akan ditunjukkan pada Gambar 3.11 hingga Gambar 3.13. Nilai tersebut didapatkan dari blok data RSS, dengan masing-masing blok berisi 10 data RSS. Hasil pengujian yang dilakukan menunjukkan bahwa rata-rata nilai korelasi blok data RSS antara pengguna yang sah kebanyakan melebihi 0,5, sedangkan korelasi dengan penyadap kebanyakan berada dibawah 0,1.

Tabel 3.5 Koefisien korelasi hasil pengukuran dari skenario 1 hingga 3

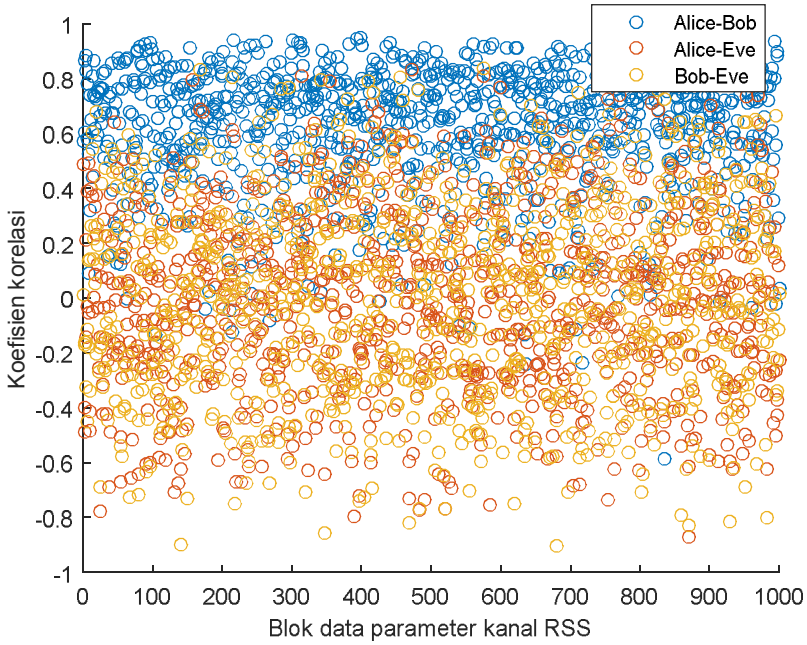
Pengguna	**Koefisien korelasi dari skenario**		
	1	**2**	**3**
Alice-Bob	0,8056	0,6961	0,6549
Alice-Eve	0,0073	0,0153	0,0079
Bob-Eve	0.0140	0,0112	0,0059



Gambar 3.11 Koefisien korelasi dari blok data parameter kanal RSS pada skenario 1.



Gambar 3.12 Koefisien korelasi dari blok data parameter kanal RSS pada skenario 2.

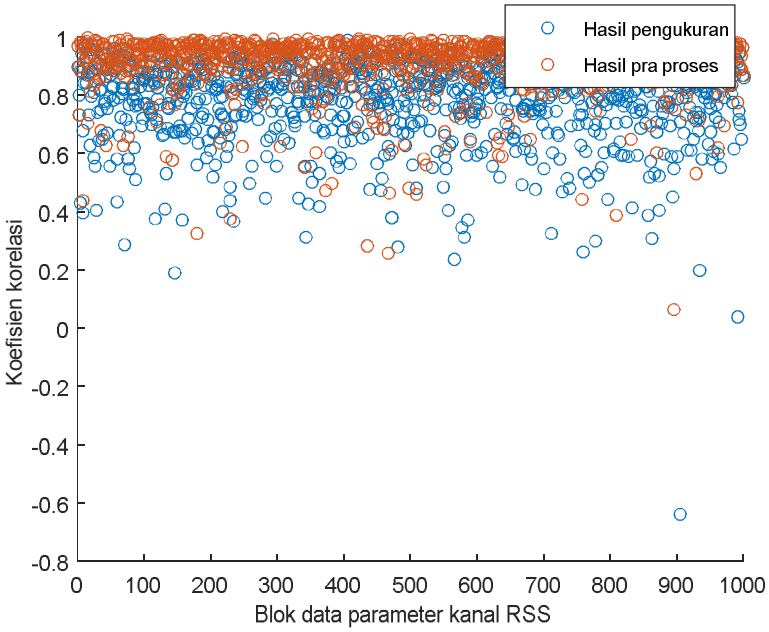


Gambar 3.13 Koefisien korelasi dari blok data parameter kanal RSS pada skenario 3.

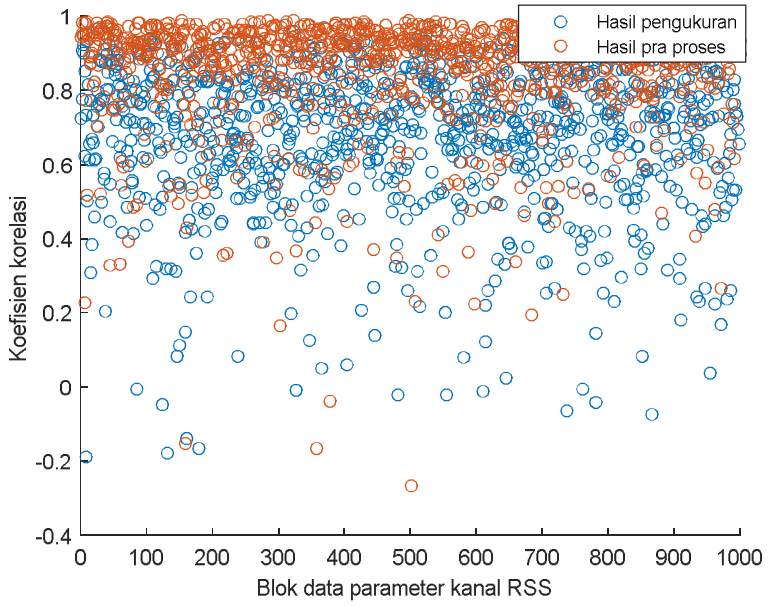
Kami menggunakan metode Kalman Filter untuk meningkatkan *reciprocity* parameter kanal RSS antara dua pengguna yang sah. Peningkatan *reciprocity* ditunjukkan dengan peningkatan koefisien korelasi. Tabel 3.6 menunjukkan peningkatan koefisien korelasi yang didapatkan saat menggunakan metode Kalman Filter yang eksisting dan Kalman Filter yang diusulkan. Hasil pengujian yang dilakukan menunjukkan adanya peningkatan koefisien korelasi yang signifikan dari hasil pra proses menggunakan Kalman Filter yang diusulkan (Algoritma 1). Pembagian parameter kanal RSS hasil pengukuran kedalam bentuk blok menyebabkan semakin banyak blok data yang mengalami peningkatan koefisien korelasi. Kondisi ini mengakibatkan peningkatan koefisien korelasi secara keseluruhan. Pengujian pada Tabel 3.6 menunjukkan bahwa peningkatan koefisien korelasi tertinggi diperoleh saat jumlah data dalam blok sebanyak 10. Gambar 3.14 hingga 3.16 menunjukkan detil perbandingan koefisien korelasi per blok data yang diperoleh saat hasil pengukuran dengan hasil pra proses pada skenario 1 hingga 3. Masing-masing blok data berisi 10 parameter kanal RSS. Hasil pengujian pada skenario 2 dan 3 menunjukkan peningkatan koefisien korelasi yang lebih rendah dari skenario 1. Hal tersebut terjadi karena lebih banyak blok data yang memiliki koefisien korelasi dibawah 0,8 jika dibandingkan dengan skenario 1 sehingga secara keseluruhan koefisien korelasi parameter kanal hasil pra proses mengalami penurunan.

Tabel 3.6 Peningkatan koefisien korelasi dengan menggunakan metode Kalman Filter

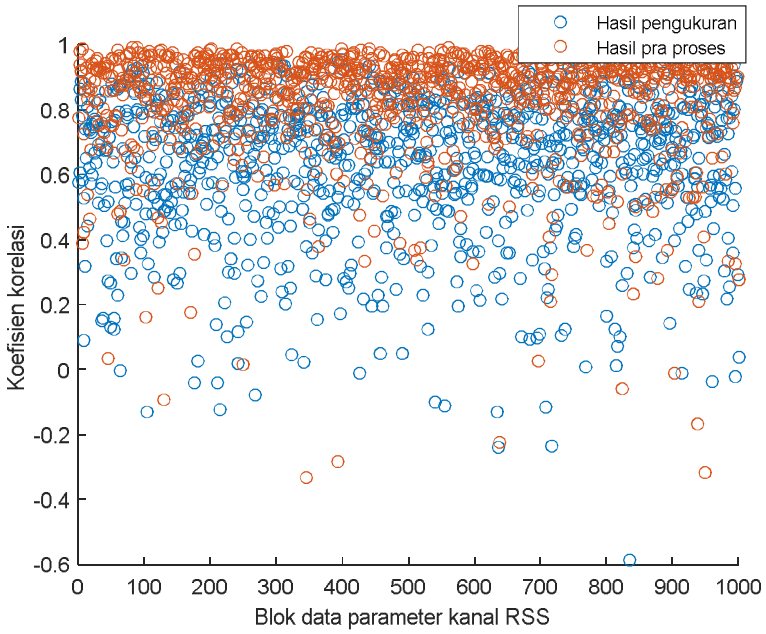
Skenario	**Pengguna**	**Koefisien korelasi hasil pengukuran**	**Peningkatan koefisien korelasi**				
			Kalman Filter Eksisting	**Jumlah blok skema usulan 1**			
				10	**20**	**40**	**50**
1	Alice-Bob	0,8056	0,8043	0,9061	0,8899	0,8636	0,8522
2	Alice-Bob	0,6961	0,6968	0,8459	0,8218	0,7836	0,7671
3	Alice-Bob	0,6549	0,6655	0,8258	0,7900	0,7509	0,7431



Gambar 3.14 Peningkatan koefisien korelasi dari blok data parameter kanal RSS pada skenario 1.



Gambar 3.15 Peningkatan koefisien korelasi dari blok data parameter kanal RSS pada skenario 2.



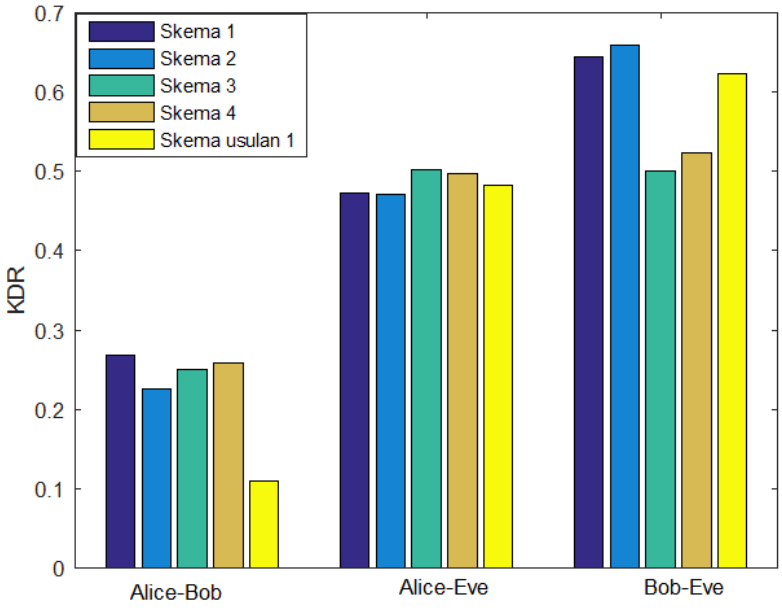
Gambar 3.16 Peningkatan koefisien korelasi dari blok data parameter kanal RSS pada skenario 3.

3.4.2.2 Evaluasi Performansi Kombinasi Metode Kalman dengan Kuantisasi Multilevel

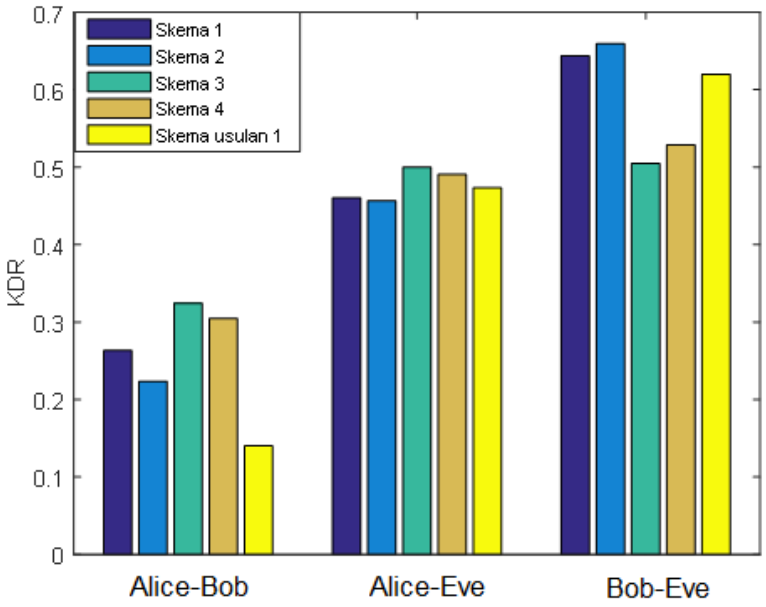
Pada bagian ini kami melakukan evaluasi performansi skema kombinasi metode Kalman dengan kuantisasi multilevel. Evaluasi dilakukan di masing-masing skenario dengan menggunakan parameter KDR, KGR, serta keacakan. Sama dengan sistem simulasi, pada validasi dengan eksperimental ini terdapat 5 skema yang akan kami bandingkan yaitu skema 1 hingga 4 serta skema usulan 1. Skema 1 hingga 3 menggunakan sistem *direct* kuantisasi dengan kuantisasi multilevel yang digunakan adalah Adaptive (skema 1), MMB (skema 2), serta 2-Ary (skema 3). Skema 4 menggunakan gabungan Kalman Filter yang eksisting dengan kuantisasi *Adaptive*. Skema usulan 1 menggunakan mekanisme yang telah dijelaskan pada Algoritma 1 dan 4. Parameter yang digunakan untuk menjalankan masing-masing skema sama dengan parameter yang digunakan di simulasi seperti yang terlihat pada Tabel 3.1.

Perbandingan KDR yang dihasilkan dari skema ditunjukkan pada Gambar 3.17 hingga 3.19. Parameter KDR yang akan dianalisa meliputi KDR pengguna yang sah

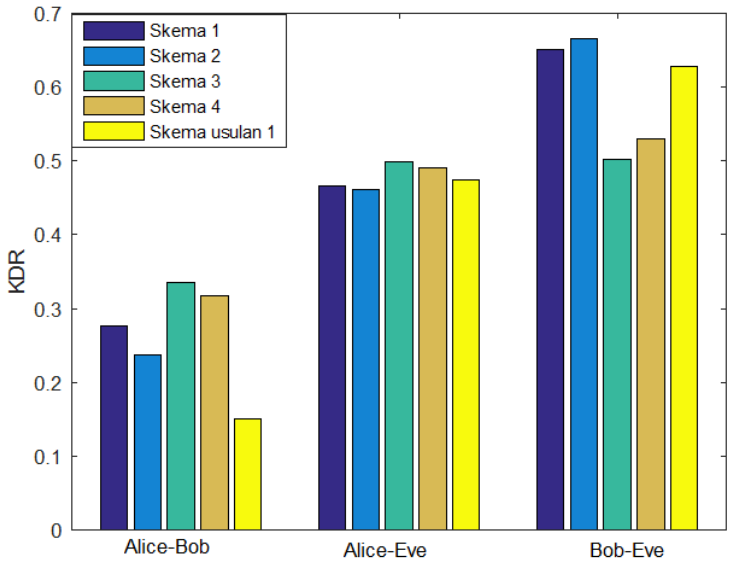
serta KDR penyadap. KDR pengguna yang sah didapatkan dengan membandingkan bit hasil kuantisasi dari masing-masing pengguna yang sah. KDR penyadap didapatkan dengan membandingkan bit hasil kuantisasi dari penyadap dengan pengguna yang sah. Diasumsikan penyadap mengetahui algoritma pra proses dan kuantisasi yang digunakan namun tidak mengetahui parameter dari masing-masing algoritma tersebut. Analisa keamanan dilakukan dengan melakukan rekonsiliasi informasi terhadap bit hasil kuantisasi yang diperoleh. Hasil pengujian KDR pengguna yang sah menunjukkan bahwa skema yang diusulkan memiliki KDR terendah di semua skenario. Penurunan KDR tertinggi terjadi di skenario 1 yaitu sebesar 58,9 %. Semakin rendah KDR yang diperoleh maka semakin tinggi KGR_r dan KGR_{pa} yang diperoleh. Hal ini terjadi karena semakin besar kemungkinan blok data tersebut mampu dikoreksi saat tahap rekonsiliasi informasi sehingga jumlah blok data yang terbuang menjadi berkurang. Hasil pengujian KDR penyadap menunjukkan nilai KDR diatas 40% untuk semua skenario sehingga sangat kecil kemungkinan penyadap mendapatkan kunci yang sama dengan pengguna yang sah.



Gambar 3.17 Perbandingan KDR hasil eksperimen antara skema 1-4 serta usulan 1 (skenario 1).



Gambar 3.18 Perbandingan KDR hasil eksperimen antara skema 1-4 serta usulan 1 (skenario 2).



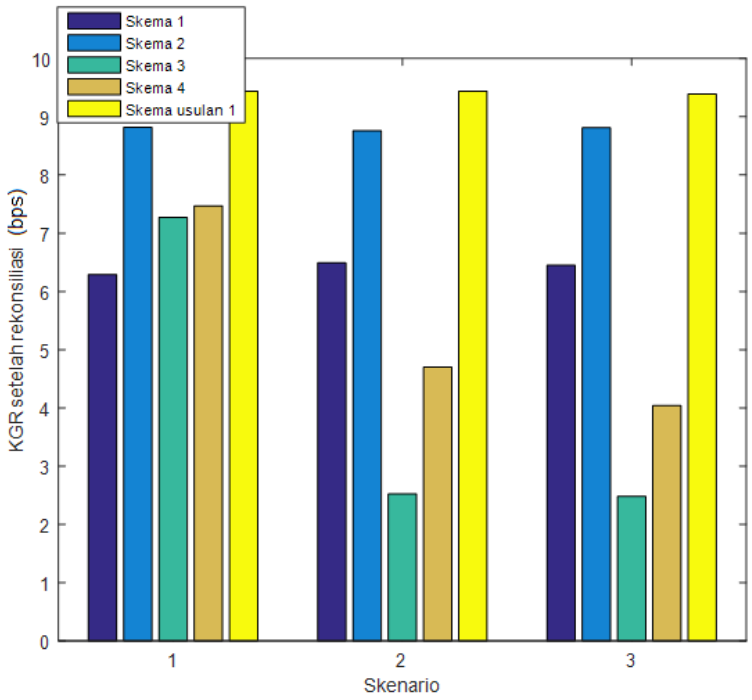
Gambar 3.19 Perbandingan KDR hasil eksperimen antara skema 1-4 serta usulan 1 (skenario 3).

Perbandingan KGR dari semua skenario dapat dilihat pada Tabel 3.7 serta Gambar 3.20 hingga 3.21. Hasil pengujian yang dilakukan menunjukkan bahwa KGR_{ik} yang

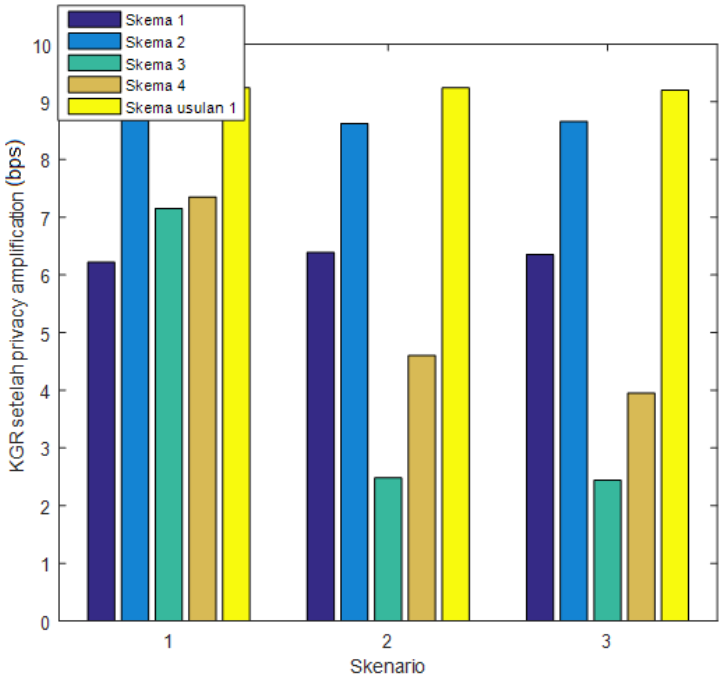
diperoleh setelah kuantisasi cenderung stabil untuk skema dan skenario. Hal ini terjadi karena pada tahap ini faktor penentu KGR yang utama adalah metode kuantisasi yang digunakan serta waktu komputasi dari masing-masing proses. Perbedaan terlihat saat KGR_r karena saat tahap ini blok data yang tidak mampu dikoreksi akan dibuang. Semakin tinggi nilai KDR maka KGR_r yang dihasilkan juga akan semakin rendah. Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 1 memiliki KGR_r yang lebih tinggi jika dibandingkan dengan skema yang lain di semua skenario dengan peningkatan KGR_r tertinggi terjadi di skenario 3 yaitu sebesar 2,79 kali lipat. Hal ini terjadi karena skema usulan 1 memiliki KDR yang lebih rendah dibandingkan dengan skema yang lain sehingga lebih sedikit jumlah blok data yang terbuang. Hasil dari KGR_{pa} tidak terlalu berbeda dengan KGR_r karena pada tahap ini nilai yang dihasilkan hanya tergantung dari penambahan waktu komputasi dari *privacy amplification*. Secara keseluruhan dapat dikatakan bahwa skema yang dibangun dapat memenuhi standarisasi dari (Moore, 2001). KGR_{pa} tertinggi dari skema usulan 1 didapatkan saat skenario 1 dan 2 yaitu sebesar 9,24 bps yang artinya dibutuhkan waktu sebanyak 27,71 detik untuk mendapatkan 256 bit *secret key*.

Tabel 3.7 Perbandingan KGR_{ik} hasil eksperimen antara skema 1-4 serta usulan 1.

Nama skema	KGR_{ik} **pada Skenario (bps)**		
	1	**2**	**3**
Skema 1	18,00	18,08	18,07
Skema 2	18,05	18,10	18,08
Skema 3	16,36	16,30	16,30
Skema 4	18,02	18,00	17,99
Skema usulan 1	17,96	17,94	17,95



Gambar 3.20 Perbandingan KGR_r hasil eksperimen antara skema 1-4 serta usulan 1.



Gambar 3.21 Perbandingan KGR_{pa} hasil eksperimen antara skema 1-4 serta usulan 1.

Hasil dari tahap *privacy amplification* adalah kandidat 256 bit *secret key* yang akan digunakan untuk mengacak pesan yang dikirim. *Input* dari tahap ini adalah *synchronized key* yang akan ditingkatkan keacakannya dengan menggunakan Universal hash. Proses selanjutnya adalah pengujian keacakan dengan menggunakan NIST sehingga bisa diketahui nilai p. Jika nilai yang dihasilkan melebihi 0,01 maka *synchronized key* akan menjadi kandidat *secret key*, dimana kandidat yang dipilih adalah kandidat yang memiliki nilai approximate entropy tertinggi. Tabel 3.8 menunjukkan hasil pengujian NIST untuk kandidat *secret key* yang memiliki *approximate entropy* tertinggi di masing-masing pengujian. Hasil pengujian yang dilakukan menunjukkan bahwa *secret key* yang dihasilkan di semua skenario telah memenuhi persayaratan keacakan yang diharapkan karena semua nilai p di masing-masing tes telah melebihi 0,01.

Tabel 3.8 Hasil pengujian NIST dari skema usulan 1

NIST Test	**Nilai** p		
	Skenario 1	**Skenario 2**	**Skenario 3**
Approximate entropy	0,9910	0,9548	0,9871
Frequency	0,8026	1,0000	0,9005
Block Frequency	0,4194	0,2750	0,5000
Runs	0,6142	0,7077	0,6164
Longest of runs	0,4936	0,5085	0,5666
Cusum (fwd)	0,6871	0,9064	0,9742
Cusum (rev)	0,9064	0,9064	0,9742

3.5 Skema SKG dengan Kombinasi Metode *Modified Polynomial Regression* (MPR) dengan Kuantisasi Multilevel

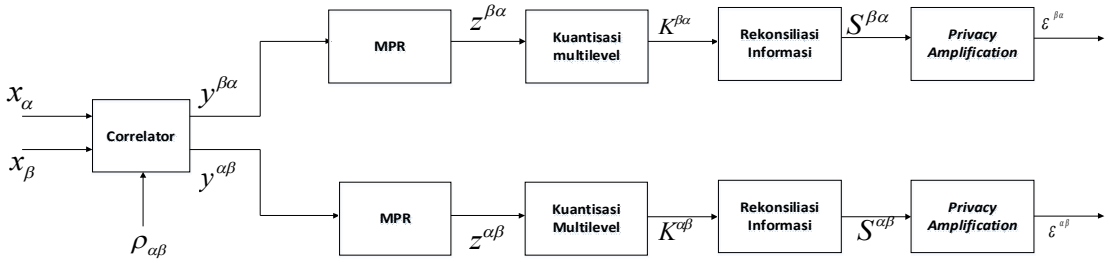
Bagian ini bertujuan untuk menguji performansi skema SKG dengan kombinasi metode MPR dan kuantisasi multilevel. Pengujian dilakukan secara simulasi dan divalidasi dengan eksperimen di lingkungan riil.

3.5.1 Simulasi Monte Carlo untuk Skema SKG dengan Kombinasi Metode MPR dengan Kuantisasi Multilevel

Detil mekanisme simulasi Monte Carlo telah dijelaskan pada sub bab 3.4.1. Pada skema ini kami menggunakan model simulasi yang ditunjukkan oleh Gambar 3.22. Dua bilangan acak yang *independent* dengan panjang data $n = 10.000$, $x_\alpha = [x_\alpha(1), x_\alpha(2), ..., x_\alpha(n)]^T$ dan $x_\beta = [x_\beta(1), x_\beta(2), ..., x_\beta(n)]^T$ saling berkorelasi dengan distribusi Rician. Estimasi parameter kanal $y^{\beta\alpha}$ dan $y^{\alpha\beta}$ akan diolah dengan metode MPR untuk mendapatkan parameter kanal hasil pra proses $z^{\beta\alpha}$ dan $z^{\alpha\beta}$. Kuantisasi dilakukan dengan menggunakan beberapa kuantisasi multilevel yaitu *Adaptive*, ASBG dan 2-Ary untuk mendapatkan *preliminary key* $K^{\beta\alpha}$ dan $K^{\alpha\beta}$. Perbedaan bit yang terjadi akan dikoreksi di tahap rekonsiliasi informasi dengan menggunakan BCH (255,87). Blok bit dari *preliminary key* yang tidak mampu dikoreksi akan dibuang dan sisa dari blok bit tersebut akan menjadi *synchronized key* $S^{\beta\alpha}$ dan $S^{\alpha\beta}$. Bit dari *synchronized key* akan masuk di tahap *privacy amplification* sehingga bisa didapatkan *secret key* $\varepsilon^{\beta\alpha}$ dan $\varepsilon^{\alpha\beta}$ sepanjang 256 bit.

Evaluasi terhadap performansi skema SKG dengan kombinasi metode MPR dan kuantisasi multilevel dilakukan dengan mengimplementasikan skema SKG di Matlab dengan nilai koefisien korelasi 0,7. Pemilihan nilai koefisien korelasi tersebut disesuaikan dengan nilai parameter kanal hasil pengukuran di bagian eksperimental. Terdapat 3 evaluasi yang akan dilakukan yaitu peningkatan *reciprocity* dengan menggunakan metode MPR, serta pengujian parameter KDR dan KGR dari masing-masing tahap. Detil Parameter yang digunakan dalam simulasi ditunjukkan pada Tabel 3.9. Perbedaan dari metode Regresi polinomial yang eksisting dengan metode MPR

terletak pada pengolahan kembali estimasi parameter kanal hasil pra proses dengan menggunakan Moving Average sehingga bisa didapatkan peningkatan *reciprocity* yang lebih signifikan. Tabel 3.10 menunjukkan peningkatan koefisien korelasi dari estimasi parameter kanal $y^{\alpha\beta}, y^{\beta\alpha}$ dengan menggunakan metode Regresi Polinomial dan MPR. Terlihat bahwa penambahan metode Moving Average mampu meningkatkan *reciprocity* lebih tinggi dari $z^{\alpha\beta}, z^{\beta\alpha}$ jika dibandingkan dengan Regresi Polinomial eksisting. Semakin tinggi peningkatan koefisien korelasi estimasi parameter kanal hasil pra proses yang diperoleh maka diharapkan semakin rendah KDR yang dihasilkan.



Gambar 3.22 Model simulasi skema SKG dengan metode pra proses MPR.

Tabel 3.9 Parameter Simulasi skema SKG dengan metode pra proses MPR.

No	Parameter	Keterangan
1	Jumlah data	10.000
1	Distribusi data	Rician dengan s=4
2	Regresi Polinomial	$m = 2$
3	MPR	$m = 2$, $w = 3$
4	Kuantisasi adaptive	$S_B = 50$
5	Kuantisasi ASBG	$C = 2$
6	Kuantisasi 2-Ary	$\alpha = 0{,}1$
7	Metode rekonsiliasi informasi	BCH(255,87)
8	Metode *privacy amplification*	Universal hash 256 bit serta SHA-256

Tabel 3.10 Peningkatan koefisien korelasi hasil simulasi dengan menggunakan metode MPR.

Koefisien korelasi $y^{\alpha\beta}, y^{\beta\alpha}$	**Peningkatan koefisien korelasi**	
	Regresi Polinomial eksisting	**MPR**
0,71	0,7139	0,7224

Tabel 3.11 menunjukkan perbandingan KDR yang dihasilkan dari tiap-tiap skema yang digunakan. Skema 3 dan 5 menggunakan sistem *direct* kuantisasi dengan kuantisasi multilevel yang digunakan adalah 2-Ary (skema 3), dan ASBG (skema 5). Skema 6 menggunakan gabungan Regresi Polinomial yang eksisting dengan kuantisasi *Adaptive*. Skema usulan 2 menggunakan mekanisme yang telah dijelaskan pada Algoritma 2 dan 4. Untuk pengujian keamanan, dengan cara yang sama kami membangkitkan dua bilangan acak dengan panjang $n = 10.000$, $x_e = [x_e(1), x_e(2), ..., x_e(n)]^T$ yang berkorelasi dengan x_α berdistribusi Rician dan $x_{e'} = [x_{e'}(1), x_{e'}(2), ..., x_{e'}(n)]^T$ yang berkorelasi dengan x_β berdistribusi Rician. Estimasi parameter kanal yang diperoleh adalah $y^{\alpha e}$ dan $y^{\beta e'}$. Diasumsikan $y^{\alpha\beta}$ dan $y^{\beta\alpha}$ adalah data dari pengguna yang sah yang memiliki koefisien korelasi tinggi, sedangkan $y^{\alpha e}$ dan $y^{\beta e'}$ adalah data dari penyadap yang memiliki koefisien korelasi sangat rendah.

Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 2 menghasilkan nilai KDR $K^{\alpha\beta}$ dan $K^{\beta\alpha}$ yang lebih rendah dibandingkan dengan skema yang lain pada semua data dengan variasi nilai koefisien korelasi. Hal ini tejadi karena skema usulan 2 menggunakan data hasil pra proses yang memiliki koefisien korelasi yang tinggi sehingga kemungkinan untuk mendapatkan bit yang sama juga tinggi. Kondisi ini mengakibatkan lebih rendahnya nilai KDR yang diperoleh. Pada pengujian keamanan, diasumsikan penyadap mengetahui algoritma pra proses dan kuantisasi yang digunakan namun tidak mengetahui parameter dari masing-masing algoritma tersebut. Analisa keamanan dilakukan dengan melakukan rekonsiliasi informasi

terhadap bit hasil kuantisasi yang diperoleh. Secara keseluruhan terlihat bahwa skema SKG hasil simulasi yang dibangun dapat memenuhi persyaratan keamanan karena KDR dari $K^{\beta\alpha}$, $K^{\alpha e}$ serta $K^{\alpha\beta}$, $K^{\beta e'}$ skema usulan 2 telah melebihi 0,4 sehingga sulit bagi penyadap untuk mendapatkan *preliminary key* yang sama pada saat tahap rekonsiliasi informasi.

Tabel 3.12 menunjukkan KGR yang dihasilkan dari semua skema. KGR_{ik} yang diperoleh setelah kuantisasi cenderung stabil untuk semua data dengan variasi nilai koefisien korelasi. Hal ini terjadi karena pada tahap ini faktor penentu KGR yang utama adalah metode kuantisasi yang digunakan serta waktu komputasi dari masing-masing proses. Perbedaan terlihat saat KGR_r karena saat tahap ini blok data yang tidak mampu dikoreksi akan dibuang. Semakin tinggi nilai KDR maka KGR_r yang dihasilkan juga akan semakin rendah. Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 2 memiliki KGR_r yang lebih tinggi jika dibandingkan dengan skema yang lain. Hal ini terjadi karena skema yang diusulkan memiliki KDR yang lebih rendah sehingga tidak banyak blok data yang terbuang. Hasil dari KGR_{pa} tidak terlalu berbeda dengan KGR_r karena pada tahap ini nilai yang dihasilkan hanya tergantung dari waktu komputasi dari *privacy amplification* .

Tabel 3.11 Perbandingan KDR hasil simulasi antara skema 3,5-6 serta usulan 2.

Estimasi parameter kanal	**Koefisien korelasi**	**KDR**			
		Skema 3	**Skema 5**	**Skema 6**	**Skema usulan 2**
$y^{\alpha\beta}$ dan $y^{\beta\alpha}$	0,71	0,3068	0,3059	0,2660	0,1369
$y^{\beta\alpha}$ dan $y^{\alpha e}$	0,01	0,4980	0,4998	0,4171	0,4598
$y^{\alpha\beta}$ dan $y^{\beta e'}$	0,007	0,4987	0,4994	0,4171	0,4808

Tabel 3.12 Perbandingan KGR hasil simulasi antara skema 3,5-6 serta usulan 2.

Koefisien korelasi $y^{\alpha\beta}$ dan $y^{\beta\alpha}$	**KGR**	**Skema 3**	**Skema 5**	**Skema 6**	**Skema usulan 2**
0,710	KGR_{ik} (bps)	3461,54	4008,02	588,24	470,59
	KGR_{r} (bps)	29,48	33,66	41,03	47,20
	KGR_{pa} (bps)	27,57	31,69	39,16	45,99

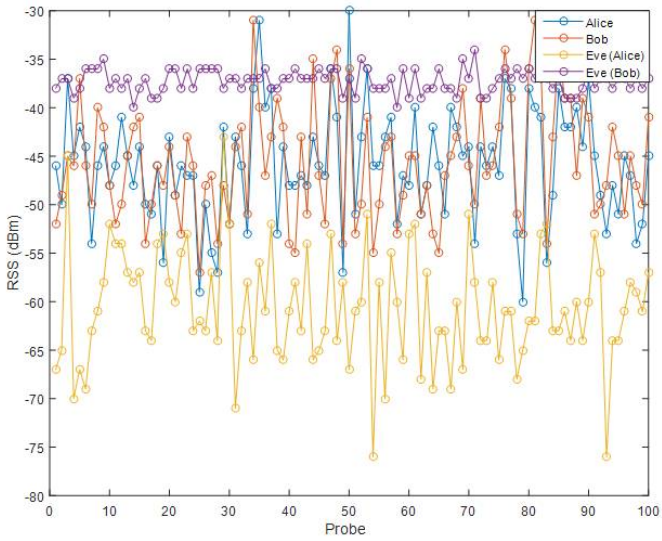
3.5.2 Hasil Eksperimen Skema SKG dengan Kombinasi Metode MPR dengan kuantisasi Multilevel

Pada bagian ini akan dibahas evaluasi performansi dari hasil eksperimen skema SKG dengan kombinasi metode MPR dan kuantisasi multilevel yang dilakukan pada skenario 4. Evaluasi yang dilakukan meliputi evaluasi peningkatan *reciprocity* dengan menggunakan metode MPR serta evaluasi parameter performansi KDR, KGR serta *randomness* (keacakan).

3.5.2.1 Evaluasi Peningkatan *Reciprocity* dengan Menggunakan Metode MPR

Gambar 3.23 menunjukkan hasil pengukuran parameter kanal RSS dari Alice, Bob dan Eve pada probe 1 hingga 100. Hasil pengujian yang dilakukan menunjukkan *reciprocity* yang cukup tinggi antara kedua pengguna yang sah, sedangkan parameter kanal yang didapat penyadap baik dari Alice maupun Bob menunjukkan *reciprocity* yang rendah. Karena Alice bergerak sedangkan Bob dalam posisi diam terlihat bahwa parameter kanal RSS yang didapat Eve lebih dinamis jika dibandingkan dengan Bob. Namun secara keseluruhan terlihat bahwa parameter kanal RSS yang didapat Eve benar-benar berbeda dari kedua pengguna yang sah. Kami menggunakan koefisien korelasi Pearson yang digunakan oleh (Ali dkk, 2014) untuk menentukan tingkat *reciprocity* dari parameter kanal RSS hasil pengukuran. Nilai koefisien korelasi yang

didapatkan berkisar antara -1 hingga 1. Nilai dari koefisien korelasi yang ditunjukkan pada Tabel 3.13 menunjukkan bahwa koefisien korelasi yang didapat dari Alice dan Bob telah melebihi 0,5 sedangkan nilai koefisien korelasi yang didapat Eve dengan pengguna yang sah dibawah 0,1. Sehingga bisa dikatakan bahwa Alice dan Bob memiliki tingkat *reciprocity* yang tinggi sedangkan Eve memiliki tingkat *reciprocity* yang rendah terhadap kedua pengguna yang sah. Kondisi ini mengakibatkan sulit bagi Eve untuk mendapatkan *secret key*.



Gambar 3.23 Hasil *channel probing* skenario 4 pada probe ke 1 hingga 100

Tabel 3.13 Koefisien korelasi parameter kanal hasil pengukuran dari skenario 4

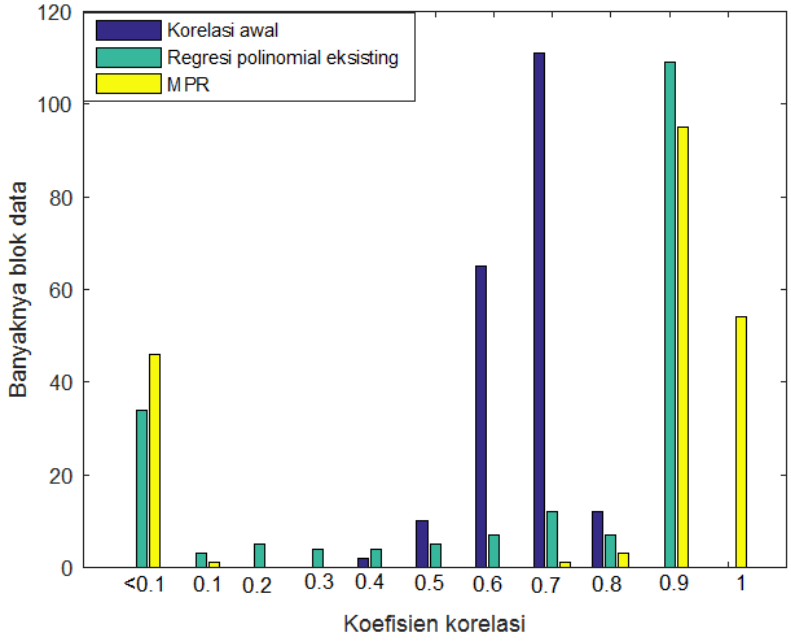
Skenario	**Pengguna**	**Koefisien Korelasi**
4	Alice-Bob	0,7133
	Alice-Eve	0,0121
	Bob-Eve	0,0084

Metode Regresi Polinomial eksisting yang digunakan memiliki orde m sebesar 2 dengan jumlah data n sebanyak 10.000. Metode ini digunakan untuk melakukan pra

proses terhadap beberapa blok data sejumlah N_B sehingga didapatkan peningkatan *reciprocity* yang lebih signifikan. Dengan jumlah m dan n yang sama, metode MPR (Algoritma 2) menambahkan parameter w dengan nilai sebesar 3. Tabel 3.14 menunjukkan peningkatan koefisien korelasi yang didapatkan oleh metode MPR. Hasil pengujian yang dilakukan menunjukkan bahwa pengolahan parameter kanal hasil pengukuran dengan menggunakan metode MPR memberikan peningkatan *reciprocity* yang lebih signifikan jika dibandingkan dengan pengolahan dengan menggunakan Regresi Polinomial yang eksisting yaitu dari 0,7133 menjadi 0,7844. Detil perbandingan jumlah koefisien korelasi per blok data dapat dilihat pada Gambar 3.24. Blok data hasil pengukuran memiliki rata-rata koefisien korelasi di 0,5 hingga 0,7 sedangkan blok data hasil Regresi Polinomial eksisting mengalami peningkatan koefisien korelasi di 0,9. Kondisi inilah yang memicu meningkatnya koefisien korelasi yang dihasilkan jika dibandingkan dengan koefisien korelasi awal. Pemanfaatan metode MPR juga mampu meningkatkan koefisien korelasi di 0,9 dari blok data parameter kanal RSS hasil pengukuran. Jika dibandingkan dengan metode Regresi Polinomial yang eksisting maka metode MPR menghasilkan peningkatan koefisien korelasi yang lebih signifikan. Hal ini terjadi karena jumlah blok data yang memiliki koefisien korelasi di 0,9 hingga 1 lebih banyak jika dibandingkan dengan metode Regresi polinomial sehingga secara keseluruhan koefisien korelasi parameter kanal RSS juga mengalami peningkatan.

Tabel 3.14 Peningkatan koefisien korelasi parameter kanal hasil pengukuran dari skenario 4

Skenario	**Koefisien korelasi hasil pengukuran**	**Peningkatan Koefisien korelasi**	
		Regresi Polinomial eksisting	**MPR**
4	0,7133	0,7446	0,7844



Gambar 3.24. Jumlah koefisien korelasi di masing-masing blok pada skenario 4

3.5.2.2 Evaluasi Performansi Kombinasi Metode MPR dan Kuantisasi Multilevel

Pada bagian ini kami melakukan evaluasi performansi skema kombinasi metode MPR dengan kuantisasi multilevel. Evaluasi dilakukan di masing-masing skenario dengan menggunakan parameter KDR, KGR, serta keacakan. Sama dengan sistem simulasi, pada validasi dengan eksperimental ini terdapat 4 skema yang akan kami bandingkan yaitu skema 3, 5 dan 6 serta skema usulan 2. Skema 3 dan 5 menggunakan sistem *direct* kuantisasi dengan kuantisasi multilevel yang digunakan adalah 2-Ary (skema 3), serta ASBG (skema 5). Skema 6 menggunakan gabungan Regresi Polinomial yang eksisting dengan kuantisasi Adaptive. Skema usulan 2 menggunakan mekanisme yang telah dijelaskan pada Algoritma 2 dan 4. Parameter yang digunakan untuk menjalankan masing-masing skema sama dengan parameter yang digunakan di simulasi seperti yang terlihat pada Tabel 3.9. Parameter performansi yang akan dianalisa adalah KGR, KDR serta keacakan. Nilai KDR didapatkan dari perbedaan bit yang dihasilkan kedua pengguna yang sah setelah tahap kuantisasi. Nilai KGR

didapatkan setelah tahap kuantisasi, rekonsiliasi informasi serta *privacy amplification*. Keacakan dari *secret key* diuji dengan menggunakan NIST *statistical suite*.

Parameter KDR yang akan dianalisa meliputi KDR pengguna yang sah serta KDR penyadap. KDR pengguna yang sah didapatkan dengan membandingkan bit hasil kuantisasi dari masing-masing pengguna yang sah. KDR penyadap didapatkan dengan membandingkan bit hasil kuantisasi dari penyadap dengan pengguna yang sah. Diasumsikan penyadap mengetahui algoritma pra proses dan kuantisasi yang digunakan namun tidak mengetahui parameter dari masing-masing algoritma tersebut. Analisa keamanan dilakukan dengan melakukan rekonsiliasi informasi terhadap bit hasil kuantisasi yang diperoleh. Hasil pengujian KDR pengguna yang sah di Tabel 3.15 menunjukkan bahwa skema usulan 2 memiliki KDR terendah di semua skenario. Penurunan KDR yang didapat mencapai 53,72 % dibandingkan dengan skema yang eksisting. Semakin rendah KDR yang diperoleh maka semakin tinggi KGR_r dan KGR_{pa} yang diperoleh. Hal ini terjadi karena semakin besar kemungkinan blok data tersebut mampu dikoreksi saat tahap rekonsiliasi informasi sehingga jumlah blok data yang terbuang menjadi berkurang. Hasil pengujian KDR penyadap menunjukkan nilai KDR diatas 40% untuk semua skenario sehingga sangat kecil kemungkinan penyadap mendapatkan kunci yang sama dengan pengguna yang sah.

Tabel 3.15 Perbandingan KDR hasil eksperimen antara skema 3,5-6 serta usulan 2.

Pengguna	**KDR**			
	Skema 3	**Skema 5**	**Skema 6**	**Skema usulan 2**
Alice-Bob	0,3116	0,3109	0,2425	0,1442
Alice-Eve	0,4974	0,4983	0,4380	0,4474
Bob-Eve	0,5023	0,5032	0,4072	0,4478

Tabel 3.16 menunjukkan pengujian parameter KGR hasil eksperimen. Pengujian KGR_{ik} yang diperoleh setelah tahap kuantisasi cenderung stabil untuk semua skenario. Hal ini terjadi karena pada tahap ini faktor penentu KGR yang utama adalah metode kuantisasi yang digunakan serta waktu komputasi dari masing-masing proses. Perbedaan terlihat saat KGR_r karena saat tahap ini blok data yang tidak mampu dikoreksi akan dibuang. Semakin tinggi nilai KDR maka KGR_r yang dihasilkan juga akan semakin rendah. Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 2 memiliki KGR_r yang lebih tinggi jika dibandingkan dengan skema yang eksisting. Peningkatan KGR_r yang didapat mencapai 81,95% dibandingkan dengan skema yang eksisting. Hal ini terjadi karena skema usulan 2 memiliki KDR yang lebih rendah dibandingkan dengan skema yang lain sehingga lebih sedikit jumlah blok data yang terbuang. Hasil dari KGR_{pa} tidak terlalu berbeda dengan KGR_r karena pada tahap ini nilai yang dihasilkan hanya tergantung dari penambahan waktu komputasi dari *privacy amplification*. Secara keseluruhan dapat dikatakan bahwa skema yang dibangun dapat memenuhi standarisasi dari (Moore, 2001) karena KGR_{pa} yang didapat sebesar 7,10 bps yang artinya dibutuhkan waktu sebanyak 36,06 detik untuk mendapatkan 256 bit *secret key*.

Hasil dari tahap *privacy amplification* adalah kandidat 256 bit *secret key* yang akan digunakan untuk mengacak pesan yang dikirim. *Input* dari tahap ini adalah *synchronized key* yang akan ditingkatkan keacakannya dengan menggunakan Universal hash. Proses selanjutnya adalah pengujian keacakan dengan menggunakan NIST sehingga bisa diketahui nilai p. Jika nilai yang dihasilkan melebihi 0,01 maka *synchronized key* akan menjadi kandidat *secret key*, dimana kandidat yang dipilih adalah kandidat yang memiliki nilai approximate entropy tertinggi. Tabel 3.17 menunjukkan hasil pengujian NIST untuk kandidat *secret key* yang memiliki *approximate entropy* tertinggi di masing-masing pengujian. Hasil pengujian yang dilakukan menunjukkan bahwa *secret key* yang dihasilkan di semua skenario telah

memenuhi persayaratan keacakan yang diharapkan karena semua nilai p di masing-masing tes telah melebihi 0,01.

Tabel 3.16 Perbandingan KGR antara skema 3,5-6 serta usulan 2

Nama	**KGR (bps)**		
	KGR_{ik}	KGR_{r}	KGR_{pa}
Skema 3	16,2970	3,9673	3,9028
Skema 5	18,1159	4,3483	4,2791
Skema 6	17,5654	6,4834	6,3805
Skema usulan 2	17,3943	7,2186	7,1037

Tabel 3.17 Hasil pengujian NIST dari skema usulan 2

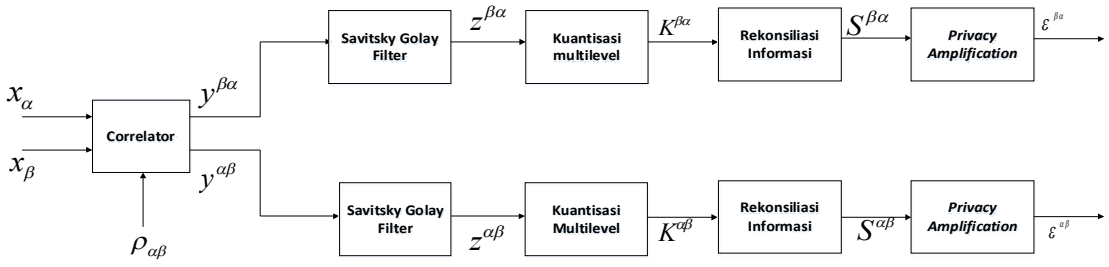
NIST Test	**Skema usulan 2**
Approximate entropy	0,9949
Frequency	0,9005
Block Frequency	0,3491
Runs	0,5313
Longest of runs	0,9306
Cusum (fwd)	0,9064
Cusum (rev)	0,9742

3.6 Skema SKG dengan Kombinasi Metode *Savitzky Golay Filter* dan Kuantisasi Multilevel

Bagian ini bertujuan untuk menguji performansi skema SKG dengan kombinasi metode *Savitzky Golay Filter* dan kuantisasi multilevel. Pengujian dilakukan secara simulasi dan divalidasi dengan eksperimen di lingkungan riil.

3.6.1 Simulasi Monte Carlo untuk Skema SKG dengan Kombinasi Metode *Savitzky Golay Filter* dan Kuantisasi Multilevel

Detil mekanisme simulasi Monte Carlo telah dijelaskan pada sub bab 3.3.1. Pada skema ini kami menggunakan model simulasi yang ditunjukkan oleh Gambar 3.25. Dua bilangan acak yang *independent* dengan panjang data $n = 10.000$, $x_\alpha = [x_\alpha(1), x_\alpha(2), ..., x_\alpha(n)]^T$ dan $x_\beta = [x_\beta(1), x_\beta(2), ..., x_\beta(n)]^T$ saling berkorelasi dengan distribusi Rayleigh. Estimasi parameter kanal $y^{\beta\alpha}$ dan $y^{\alpha\beta}$ akan diolah dengan metode *Savitzky Golay Filter* untuk mendapatkan parameter kanal hasil pra proses $z^{\beta\alpha}$ dan $z^{\alpha\beta}$. Kuantisasi dilakukan dengan menggunakan beberapa kuantisasi multilevel yaitu Adaptive, ASBG dan 2-Ary untuk mendapatkan *preliminary key* $K^{\beta\alpha}$ dan $K^{\alpha\beta}$. Perbedaan bit yang terjadi akan dikoreksi di tahap rekonsiliasi informasi dengan menggunakan BCH (255,87). Blok bit dari *preliminary key* yang tidak mampu dikoreksi akan dibuang dan sisa dari blok bit tersebut akan menjadi *synchronized key* $S^{\beta\alpha}$ dan $S^{\alpha\beta}$. Bit dari *synchronized key* akan masuk di tahap *privacy amplification* sehingga bisa didapatkan *secret key* $\varepsilon^{\beta\alpha}$ dan $\varepsilon^{\alpha\beta}$ sepanjang 256 bit. Evaluasi terhadap performansi skema SKG dengan kombinasi metode *Savitzky Golay Filter* dan kuantisasi multilevel dilakukan dengan mengimplementasikan skema SKG di Matlab dengan nilai koefisien korelasi 0,65. Terdapat 3 evaluasi yang akan dilakukan yaitu peningkatan *reciprocity* dengan menggunakan metode *Savitzky Golay Filter*, serta pengujian parameter KDR dan KGR dari masing-masing tahap. Detil Parameter yang digunakan dalam simulasi ditunjukkan pada Tabel 3.18.



Gambar 3.25 Model simulasi skema SKG dengan metode pra proses *Savitzky Golay Filter*.

Tabel 3.18 Parameter simulasi skema SKG dengan kombinasi metode *Savitzky Golay Filter* dan kuantisasi multilevel.

No	Parameter	Keterangan
1	Jumlah data	10.000
2	Distribusi data	Rayleigh dengan varian=4
3	Savitzky Golay Filter	$c_n = 2$ dan jumlah data di masing-masing *frame* adalah 155
4	Kuantisasi adaptive	$S_B = 50$
5	Kuantisasi ASBG	$C = 2$
6	Kuantisasi 2-Ary	$\alpha = 0.1$
7	Metode rekonsiliasi informasi	BCH(255,87)
8	Metode *privacy amplification*	Universal hash 256 bit serta SHA-256

Tabel 3.19 menunjukkan peningkatan koefisien korelasi dari estimasi parameter kanal $y^{\alpha\beta}, y^{\beta\alpha}$ dengan menggunakan metode *Savitzky Golay Filter*. Dari hasil pengujian yang dilakukan terlihat bahwa metode yang diusulkan mampu meningkatkan *reciprocity* dari estimasi parameter kanal dibeberapa variasi koefisien korelasi yang digunakan. Semakin tinggi peningkatan koefisien korelasi estimasi parameter kanal hasil pra proses yang diperoleh maka diharapkan semakin rendah KDR yang dihasilkan. Tabel 3.20 menunjukkan perbandingan KDR yang dihasilkan dari tiap-tiap skema yang digunakan. Skema1, 3 dan 5 menggunakan sistem *direct* kuantisasi dengan kuantisasi multilevel yang digunakan adalahAdaptive (skema 1), 2-Ary (skema 3), dan ASBG (skema 5). Skema usulan 3 menggunakan mekanisme yang telah dijelaskan pada Algoritma 3 dan 4. Untuk pengujian keamanan, dengan cara yang sama kami

membangkitkan dua bilangan acak dengan panjang $n = 10.000$, $x_e = [x_e(1), x_e(2), ..., x_e(n)]^T$ yang berkorelasi dengan x_α berdistribusi Rayleigh dan $x_{e'} = [x_{e'}(1), x_{e'}(2), ..., x_{e'}(n)]^T$ yang berkorelasi dengan x_β berdistribusi Rician. Estimasi parameter kanal yang diperoleh adalah $y^{\alpha e}$ dan $y^{\beta e'}$. Diasumsikan $y^{\alpha\beta}$ dan $y^{\beta\alpha}$ adalah data dari pengguna yang sah yang memiliki koefisien korelasi tinggi, sedangkan $y^{\alpha e}$ dan $y^{\beta e'}$ adalah data dari penyadap yang memiliki koefisien korelasi sangat rendah.

Hasil pengujian di Tabel 3.20 menunjukkan bahwa skema usulan 3 menunjukkan nilai KDR $K^{\alpha\beta}$ dan $K^{\beta\alpha}$ yang lebih rendah dibandingkan dengan skema yang lain pada semua data dengan variasi nilai koefisien korelasi. Hal ini tejadi karena skema usulan 3 menggunakan data hasil pra proses yang memiliki koefisien korelasi yang tinggi sehingga kemungkinan untuk mendapatkan bit yang sama juga tinggi. Kondisi ini mengakibatkan lebih rendahnya nilai KDR yang diperoleh. Pada pengujian keamanan, diasumsikan penyadap mengetahui algoritma pra proses dan kuantisasi yang digunakan namun tidak mengetahui parameter dari masing-masing algoritma tersebut. Analisa keamanan dilakukan dengan melakukan rekonsiliasi informasi terhadap bit hasil kuantisasi yang diperoleh. Secara keseluruhan terlihat bahwa skema SKG hasil simulasi yang dibangun dapat memenuhi persyaratan keamanan karena KDR dari $K^{\beta\alpha}$, $K^{\alpha e}$ serta $K^{\alpha\beta}$, $K^{\beta e'}$ skema usulan 3 telah melebihi 0,4 sehingga sulit bagi penyadap untuk mendapatkan *preliminary key* yang sama pada saat tahap rekonsiliasi informasi.

Tabel 3.19 Peningkatan koefisien korelasi hasil simulasi dengan menggunakan metode Savitzky Golay Filter.

Koefisien korelasi $y^{\alpha\beta}, y^{\beta\alpha}$	**Peningkatan koefisien korelasi dengan *Savitzky Golay Filter***
0,65	0,6792

Tabel 3.21 menunjukkan KGR yang dihasilkan dari semua skema. KGR_{ik} yang diperoleh setelah kuantisasi cenderung stabil untuk semua data dengan variasi nilai koefisien korelasi. Hal ini terjadi karena pada tahap ini faktor penentu KGR yang utama adalah metode kuantisasi yang digunakan serta waktu komputasi dari masing-masing proses. Perbedaan terlihat saat KGR_r karena saat tahap ini blok data yang tidak mampu dikoreksi akan dibuang. Semakin tinggi nilai KDR maka KGR_r yang dihasilkan juga akan semakin rendah. Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 3 memiliki KGR_r yang lebih tinggi jika dibandingkan dengan skema yang lain. Hal ini terjadi karena skema yang diusulkan memiliki KDR yang lebih rendah sehingga tidak banyak blok data yang terbuang. Hasil dari KGR_{pa} tidak terlalu berbeda dengan KGR_r karena pada tahap ini nilai yang dihasilkan hanya tergantung dari waktu komputasi dari *privacy amplification* .

Tabel 3.20 Perbandingan KDR hasil simulasi antara skema 1,3,5 serta usulan 3.

Estimasi parameter kanal	**Koefisien korelasi**	**KDR**			
		Skema 1	**Skema 3**	**Skema 5**	**Skema usulan 3**
$y^{\alpha\beta}$ dan $y^{\beta\alpha}$	0,65	0,3405	0,3421	0,3422	0,1522
$y^{\beta\alpha}$ dan $y^{\alpha e}$	0,007	0.5015	0.4994	0.4160	0.4974
$y^{\alpha\beta}$ dan $y^{\beta e'}$	0,01	0.4978	0.4966	0.4206	0.4959

Tabel 3.21 Perbandingan KGR hasil simulasi antara skema 1,3,5 serta usulan 3.

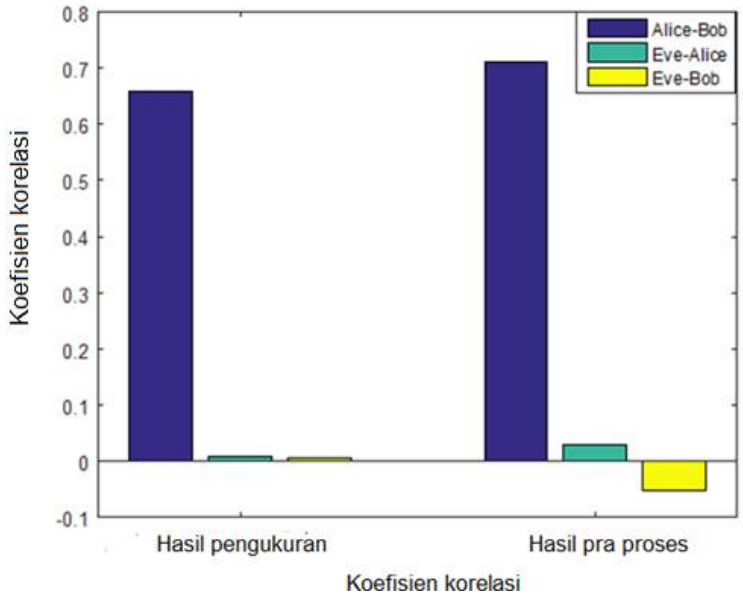
Koefisien korelasi	**KGR**	**Skema 1**	**Skema 3**	**Skema 5**	**Skema usulan 3**
0,65	KGR_{ik} (bps)	4237,29	3377,11	4106,78	875,27
	KGR_r (bps)	10,07	9,45	11,70	56,02
	KGR_{pa} (bps)	9,50	8,89	10,90	53,20

3.6.2 Hasil Eksperimen Skema SKG dengan Kombinasi Metode *Savitzky Golay Filter* dengan kuantisasi Multilevel

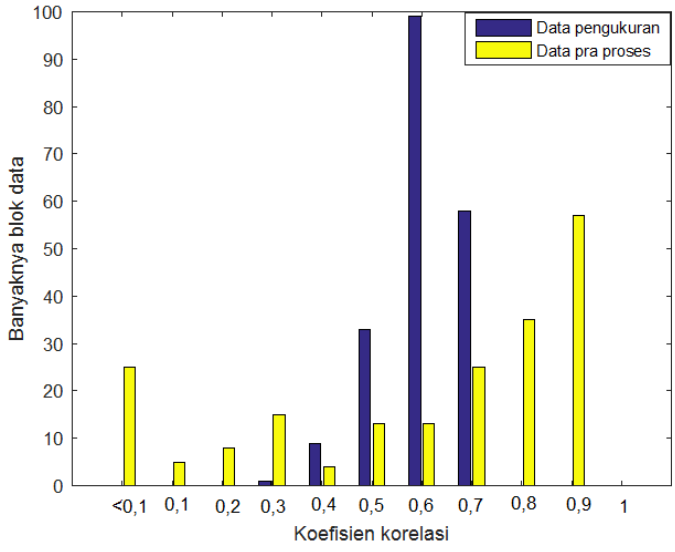
Pada bagian ini akan dibahas evaluasi performansi dari hasil eksperimen skema SKG dengan kombinasi metode Savitzky Golay Filter dan kuantisasi multilevel yang dilakukan pada skenario 3. Evaluasi yang dilakukan meliputi evaluasi peningkatan *reciprocity* dengan menggunakan metode Savitzky Golay Filter serta evaluasi parameter performansi KDR, KGR serta *randomness* (keacakan).

3.6.2.1 Evaluasi Peningkatan *Reciprocity* dengan Menggunakan Metode *Savitzky Golay Filter*

Kami menggunakan parameter kanal RSS hasil pengukuran yang didapat dengan menggunakan mekanisme pengujian di skenario 3. Gambar 3.26 menunjukkan perbandingan koefisien korelasi hasil pengukuran dan pra proses masing-masing pengguna. Dari hasil pengujian terlihat bahwa dua penggguna yang sah memiliki korelasi yang tinggi sehingga bisa digunakan sebagai sumber ekstraksi *secret key*. Eve sebagai penyadap memiliki korelasi yang rendah sehingga sulit bagi Eve untuk mendapatkan kunci yang sama dengan dengan pengguna yang sah. Penambahan metode pra proses menunjukkan adanya peningkatan koefisien korelasi antara kedua pengguna yang sah dari 0,6549 hingga 0,7119. Sedangkan koefisien korelasi penyadap tidak mengalami peningkatan bahkan cenderung turun pada data Bob-Eve. Hasil tersebut menunjukkan bahwa penambahan metode pra proses tidak mengurangi keamanan dari skema SKG yang dibangun. Detil peningkatan korelasi di masing-masing blok data pengguna yang sah dapat dilihat pada Gambar 3.27. Dari hasil pengujian yang dilakukan terlihat adanya peningkatan blok data pra proses yang memiliki koefisien korelasi 0,8 dan 0,9. Kondisi ini mengakibatkan peningkatan koefisien korelasi secara keseluruhan dari parameter kanal hasil pra proses.



Gambar 3.26 Perbandingan koefisien korelasi hasil pengukuran dan pra proses di skenario 3 (*Savitzky Golay Filter*).



Gambar 3.27 Jumlah koefisien korelasi di masing-masing blok pada skenario 3 (*Savitzky Golay Filter*).

3.6.2.2 Evaluasi Performansi Kombinasi Metode *Savitzky Golay Filter* dengan Kuantisasi Multilevel

Pada bagian ini kami melakukan evaluasi performansi skema kombinasi metode *Savitzky Golay Filter* dengan kuantisasi multilevel. Evaluasi dilakukan di masing-masing skenario dengan menggunakan parameter KDR, KGR, serta keacakan. Sama dengan sistem simulasi, pada validasi dengan eksperimental ini terdapat 4 skema yang akan kami bandingkan yaitu skema 1, 3, dan 5 serta skema usulan 3. Skema 1, 3, dan 5 menggunakan sistem *direct* kuantisasi dengan kuantisasi multilevel yang digunakan adalah Adaptive (skema 1), 2-Ary (skema 3), ASBG (skema 5). Skema usulan 3 menggunakan mekanisme yang telah dijelaskan pada Algoritma 3 dan 4. Parameter yang digunakan untuk menjalankan masing-masing skema sama dengan parameter yang digunakan di simulasi seperti yang terlihat pada Tabel 3.18. Parameter performansi yang akan dianalisa adalah KGR, KDR serta keacakan. Nilai KDR didapatkan dari perbedaan bit yang dihasilkan kedua pengguna yang sah setelah tahap kuantisasi. Nilai KGR didapatkan setelah tahap kuantisasi, rekonsiliasi informasi serta *privacy amplification*. Keacakan dari *secret key* diuji dengan menggunakan NIST *statistical suite*.

Parameter KDR yang akan dianalisa meliputi KDR pengguna yang sah serta KDR penyadap. KDR pengguna yang sah didapatkan dengan membandingkan bit hasil kuantisasi dari masing-masing pengguna yang sah. KDR penyadap didapatkan dengan membandingkan bit hasil kuantisasi dari penyadap dengan pengguna yang sah. Diasumsikan penyadap mengetahui algoritma pra proses dan kuantisasi yang digunakan namun tidak mengetahui parameter dari masing-masing algoritma tersebut. Analisa keamanan dilakukan dengan melakukan rekonsiliasi informasi terhadap bit hasil kuantisasi yang diperoleh. Hasil pengujian KDR pengguna yang sah di Tabel 3.22 menunjukkan bahwa skema usulan 3 memiliki KDR terendah di semua skenario. Penurunan KDR yang didapat mencapai 46,13 % dibandingkan dengan skema yang eksisting. Semakin rendah KDR yang diperoleh maka semakin tinggi KGR_r dan KGR_{pa} yang diperoleh. Hal ini terjadi karena semakin besar kemungkinan blok data

tersebut mampu dikoreksi saat tahap rekonsiliasi informasi sehingga jumlah blok data yang terbuang menjadi berkurang. Hasil pengujian KDR penyadap menunjukkan nilai KDR diatas 40% untuk semua skenario sehingga sangat kecil kemungkinan penyadap mendapatkan kunci yang sama dengan pengguna yang sah.

Tabel 3.23 menunjukkan hasil pengujian KGR. Pengujian KGR_{ik} yang diperoleh setelah tahap kuantisasi cenderung stabil untuk semua skenario. Hal ini terjadi karena pada tahap ini faktor penentu KGR yang utama adalah metode kuantisasi yang digunakan serta waktu komputasi dari masing-masing proses. Perbedaan terlihat saat KGR_r karena saat tahap ini blok data yang tidak mampu dikoreksi akan dibuang. Semakin tinggi nilai KDR maka KGR_r yang dihasilkan juga akan semakin rendah. Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan 3 memiliki KGR_r yang lebih tinggi jika dibandingkan dengan skema yang eksisting. Peningkatan KGR_r yang didapat mencapai 2,29 kali dibandingkan dengan skema yang eksisting. Hasil dari KGR_{pa} tidak terlalu berbeda dengan KGR_r karena pada tahap ini nilai yang dihasilkan hanya tergantung dari penambahan waktu komputasi dari *privacy amplification*. Secara keseluruhan dapat dikatakan bahwa skema yang dibangun dapat memenuhi standarisasi dari (Moore, 2001). KGR_{pa} yang didapat sebesar 8,0283 bps yang artinya dibutuhkan waktu sebanyak 31,89 detik untuk mendapatkan 256 bit *secret key*.

Hasil dari tahap *privacy amplification* adalah kandidat 256 bit *secret key* yang akan digunakan untuk mengacak pesan yang dikirim. *Input* dari tahap ini adalah *synchronized key* yang akan ditingkatkan keacakannya dengan menggunakan Universal hash. Proses selanjutnya adalah pengujian keacakan dengan menggunakan NIST sehingga bisa diketahui nilai p. Jika nilai yang dihasilkan melebihi 0,01 maka *synchronized key* akan menjadi kandidat *secret key*, dimana kandidat yang dipilih adalah kandidat yang memiliki nilai *approximate entropy* tertinggi. Tabel 3.24 menunjukkan hasil pengujian NIST untuk kandidat *secret key* yang memiliki *approximate entropy* tertinggi di masing-masing pengujian. Hasil pengujian yang dilakukan menunjukkan bahwa *secret key* yang dihasilkan di semua skenario telah

memenuhi persayaratan keacakan yang diharapkan karena semua nilai p di masing-masing tes telah melebihi 0,01.

Tabel 3.22 Perbandingan KDR hasil eksperimen antara skema 1,3,5 serta usulan 3.

Pengguna	**KDR**			
	Skema 1	**Skema 3**	**Skema 5**	**Skema usulan 3**
Alice-Bob	0,2758	0,3349	0,3345	0,1804
Alice-Eve	0,4655	0,4992	0,4922	0,6393
Bob-Eve	0,6508	0,5025	0,4905	0,4121

Tabel 3.23 Perbandingan KGR hasil eksperimen antara skema 1,3,5 serta usulan 3.

Nama	**KGR (bps)**		
	KGR_{ik}	KGR_{r}	KGR_{pa}
Skema 1	18,0734	6,4582	6,3524
Skema 3	16,2866	2,4810	2,4415
Skema 5	18,1192	2,9372	2,8898
Skema usulan 3	17,8015	8,1607	8,0283

Tabel 3.24 Hasil pengujian NIST dari skema usulan 3.

NIST Test	**Skema usulan 3**
Approximate entropy	0,9608
Frequency	0,4532
Block Frequency	0,7380
Runs	0,9719
Longest of runs	0,6193
Cusum (fwd)	0,5731
Cusum (rev)	0,3382

3.7 Matrik Perbandingan Parameter Performansi Skema SKG Kombinasi Metode Pra Proses dan Kuantisasi Multilevel dengan Skema yang Eksisting

Pada bagian ini akan dibandingkan evaluasi parameter performansi dari skema SKG yang dibangun dengan beberapa kombinasi metode pra proses dan kuantisasi multilevel. Parameter performansi yang dibandingkan meliputi koefisien korelasi, KGR, KDR, durasi waktu serta kompleksitas. Koefisien korelasi digunakan untuk membandingkan koefisien korelasi awal dengan koefisien korelasi hasil pra proses sehingga bisa diketahui peningkatan *reciprocity* (kemiripan) parameter kanal. KGR digunakan untuk mengetahui banyaknya bit yang bisa dibangkitkan per detik. Semakin tinggi nilai KGR berarti semakin banyak bit yang dapat dibangkitkan oleh skema SKG tersebut. KGR yang akan dianalisa sebagai perbandingan antara skema yang diusulkan (skema usulan 1, 2, dan 3) serta skema yang eksisting adalah KGR_{pa}, dimana KGR diperoleh setelah tahap terakhir yaitu *privacy amplification*. KDR digunakan untuk mengetahui banyaknya ketidakcocokan bit yang dihasilkan antara kedua pengguna. Semakin tinggi KDR yang dihasilkan maka semakin banyak blok data yang terbuang karena ketidakmampuan teknik rekonsiliasi untuk melakukan koreksi terhadap ketidakcocokan/perbedaan bit yang dihasilkan. Durasi waktu digunakan untuk mengetahui berapa lama waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG. Kompleksitas digunakan untuk mengetahui seberapa jauh keefektifan sebuah algoritma dalam meminimumkan waktu dan ruang, dimana waktu dan ruang suatu algoritma ini bergantung pada ukuran masukan (n), yang menyatakan jumlah data yang diproses.

Tabel 3.25 menunjukkan perbandingan kompleksitas dari skema usulan 1 hingga 3 serta skema yang eksisting. Kami melakukan pengujian kompleksitas di tiap tahapan skema SKG. Skema usulan kami menggunakan 5 tahap yang meliputi channel probing, pra proses, kuantisasi, rekonsiliasi informasi, dan *privacy amplification*. Beberapa skema yang eksisting menggunakan 4 tahap dengan menghilangkan tahap pra proses. Analisa kompleksitas hanya dilakukan pada 4 tahap terakhir karena 4 tahap tersebut kompleksitasnya tergantung dari algoritma yang dibuat. Secara keseluruhan terlihat

bahwa skema usulan kami memiliki jumlah tahap yang lebih banyak dengan kompleksitas yang sama di tahap kuantisasi hingga rekonsiliasi informasi. Hal ini terjadi karena kompleksitas algoritma yang dihasilkan sama sama tergantung dari jumlah blok data serta data dari masing-masing blok. Untuk tahap pra proses, skema usulan 1 sebagai pengembangan dari skema 4 lebih kompleks jika dibandingkan dengan skema yang eksisting. Pada skema 4 tidak ada pembagian data parameter kanal RSS menjadi beberapa blok, sehingga kompleksitas hanya tergantung dari jumlah data yang ada. Kompleksitas paling tinggi didapat pada skema usulan 2 karena adanya 2 metode pra proses yang digunakan dengan masing-masing tahap memiliki kompleksitas $o(nm)$ dan $o(n)$. Meskipun skema usulan kami memiliki tahapan yang lebih banyak jika dibandingkan dengan beberapa skema yang eksisting sehingga meningkatkan durasi waktu yang dibutuhkan, namun jika KDR yang dihasilkan lebih rendah maka KGR yang dihasilkan juga akan lebih tinggi.

Tabel 3.25 Perbandingan kompleksitas tahapan skema SKG

Skema	**Kompleksitas masing-masing tahapan skema SKG**					
	Pra proses		**Kuantisasi**	**Rekonsiliasi informasi**	**Privacy**	
	Pra proses 1	**Pra proses 2**			**Universal hash**	**SHA-256**
Skema usulan	$O(pq)$	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema usulan	$O(pq)$	$O(n)$	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema usulan	$O(pq)$	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 1	-----	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 2	-----	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 3	-----	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 4	$O(n)$	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 5	-----	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 6	$O(pq)$	-----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$

Hasil perbandingan keseluruhan parameter performansi pada pengujian simulasi dan eksperimen ditunjukkan pada Tabel 3.26. Metode pra proses yang diusulkan (Kalman Filter dan MPR) menunjukkan peningkatan koefisien korelasi yang lebih signifikan dibandingkan dengan metode pra proses yang eksisting (Kalman Filter eksisting dan Regresi Polinomial). Penggunaan metode pra proses Kalman Filter memberikan hasil yang lebih signifikan karena banyaknya parameter yang dapat diubah/dimodifikasi sehingga bisa didapatkan peningkatan koefisien korelasi yang lebih optimal jika dibandingkan dengan metode yang lain. Hasil pengujian yang dilakukan juga menunjukkan bahwa semua skema yang diusulkan (skema usulan 1,2 dan 3) memiliki KDR yang lebih rendah jika dibandingkan dengan skema yang eksisting. Kondisi ini akan meningkatkan KGR_r dan KGR_{pa} yang dihasilkan karena semakin banyak blok data yang mampu dikoreksi sehingga jumlah blok data yang dibuang juga akan berkurang. Skema usulan 1 menghasilkan nilai KGR_{pa} di semua skenario yang lebih tinggi jika dibandingkan dengan skema usulan yang lain serta skema yang eksisting. Hal ini terjadi karena skema usulan 1 menghasilkan KDR yang jauh lebih rendah jika dibandingkan dengan skema yang lain. Skema usulan 2 membutuhkan durasi waktu yang lebih lama jika dibandingkan dengan skema yang lain. Skema tersebut mengusulkan metode pra proses yang merupakan gabungan antara dua metode pra proses yaitu Regresi Polinomial dengan Moving average. Lamanya durasi waktu tersebut juga berpengaruh terhadap KGR_{pa} yang dihasilkan, dimana skema usulan 2 memiliki KGR_{pa} yang lebih rendah jika dibandingkan dengan skema usulan 1 dan 3. Namun secara keseluruhan dapat dilihat bahwa semua skema usulan memiliki KGR_{pa} yang lebih tinggi dan KDR yang lebih rendah jika dibandingkan dengan skema yang eksisting.

Tabel 3.26. Matrik Perbandingan Parameter Performansi Skema SKG dengan Kombinasi Metode Pra Proses dan Kuantisasi Multilevel

Pengujian	Skenario	Skema	Simulasi							Eksperimen						
			Koefisien Korelasi		KGR (bps)			KDR	Waktu / menit	Koefisien Korelasi		KGR (bps)			KDR	Durasi / menit
			Awal	Pra proses	KGR_{ik}	KGR_r	KGR_{pa}			Awal	Pra proses	KGR_{ik}	KGR_r	KGR_{pa}		
Kombinasi metode Kalman dan kuantisasi multilevel	1	Skema usulan 1	0,81	0,99	670,24	60,93	57,86	0,02	5,74	0,81	0,91	17,96	9,44	9,24	0,11	35,93
		Skema 1	0,81	----	3642,9	51,57	48,67	0,26	5,33	0,81	-----	18,00	6,29	6,22	0,27	35,67
		Skema 2	0,81	----	3606,9	58,77	55,58	0,26	5,32	0,81	-----	18,05	8,82	8,68	0,23	35,60
		Skema 3	0,81	-----	3214,2	48,80	46,23	0,26	5,33	0,81	-----	16,36	7,27	7,15	0,25	35,51
		Skema 4	0,81	0,81	669,12	56,60	53,71	0,23	5,75	0,81	0,80	18,02	7,47	7,35	0,26	35,92
	2	Skema usulan 1	0,69	0,98	671,37	60,89	57,83	0,03	5,74	0,69	0,85	17,94	9,44	9,24	0,14	35,94
		Skema 1	0,69	-----	3683,2	28,71	27,19	0,32	5,33	0,69	-----	18,08	6,49	6,39	0,26	35,64
		Skema 2	0,69	-----	3604,3	54,06	51,11	0,26	5,33	0,69	-----	18,10	8,76	8,62	0,22	35,66

Pengujian	Skenario	Skema	Simulasi							Eksperimen						
			Koefisien Korelasi		KGR (bps)			KDR	Waktu / menit	Koefisien Korelasi		KGR (bps)			KDR	Durasi / menit
			Awal	Pra proses	KGR_{ik}	KGR_r	KGR_{pa}			Awal	Pra proses	KGR_{ik}	KGR_r	KGR_{pa}		
Kombinasi metode Kalman dan kuantisasi multilevel	2	Skema 3	0,69	-----	3185,8	23,59	22,22	0,32	5,35	0,69	-----	16,30	2,52	2,48	0,32	35,63
		Skema 4	0,69	0,70	668,9	46,68	44,44	0,26	5,74	0,69	0,69	18,00	4,70	4,60	0,30	35,93
	3	Skema usulan 1	0,65	0,97	670,4	60,87	57,88	0,03	5,74	0,65	0,83	17,95	9,39	9,20	0,15	35,94
		Skema 1	0,65	-----	3686,6	19,53	18,49	0,34	5,33	0,65	-----	18,07	6,45	6,35	0,28	35,63
		Skema 2	0,65	-----	3585,5	5,47	51,77	0,26	5,32	0,65	-----	18,08	8,81	8,66	0,24	35,65
		Skema 3	0,65	-----	3396,2	15,79	14,95	0,34	5,33	0,65	-----	16,30	2,48	2,44	0,33	35,64
		Skema 4	0,65	0,65	670,6	40,30	38,55	0,28	5,72	0,65	0,67	18,00	4,04	3,95	0,32	35,94
Kombinasi metode MPR dan kuantisasi multilevel	4	Skema usulan 2	0,71	0,72	470,5	47,20	45,99	0,14	5,97	0,71	0,78	17,39	7,22	7,10	0,14	36,33
		Skema 3	0,71	-----	3461,5	29,48	27,57	0,31	5,35	0,71	-----	16,30	3,97	3,90	0,31	35,67

Pengujian	Skenario	Skema	Simulasi							Eksperimen						
			Koefisien Korelasi		KGR (bps)			KDR	Waktu / menit	Koefisien Korelasi		KGR (bps)			KDR	Durasi / menit
			Awal	Pra proses	KGR_{ik}	KGR_r	KGR_{pa}			Awal	Pra proses	KGR_{ik}	KGR_r	KGR_{pa}		
Kombinasi metode MPR dan kuantisasi multilevel	4	Skema 5	0,71	-----	4008,0	33,66	31,69	0,31	5,37	0,71	-----	18,12	4,35	4,28	0,31	35,58
		Skema 6	0,71	0,71	588,2	41,03	39,16	0,27	5,87	0,71	0,74	17,57	6,48	6,38	0,24	36,13
Kombinasi metode Savitzky Golay Filter dan kuantisasi multilevel	3	Skema usulan 3	0,65	0,68	875,2	56,02	53,20	0,15	5,63	0,65	0,68	17,80	8,16	8,03	0,18	35,94
		Skema 1	0,65	-----	4237,2	10,07	9,50	0,34	5,34	0,65	-----	18,07	6,46	6,35	0,28	35,61
		Skema 3	0,65	-----	3377,1	9,45	8,89	0,34	5,45	0,65	-----	16,29	2,48	2,44	0,33	35,63
		Skema 5	0,65	-----	4106,7	11,70	10,90	0,34	5,38	0,65	-----	18,12	2,94	2,89	0,33	35,63

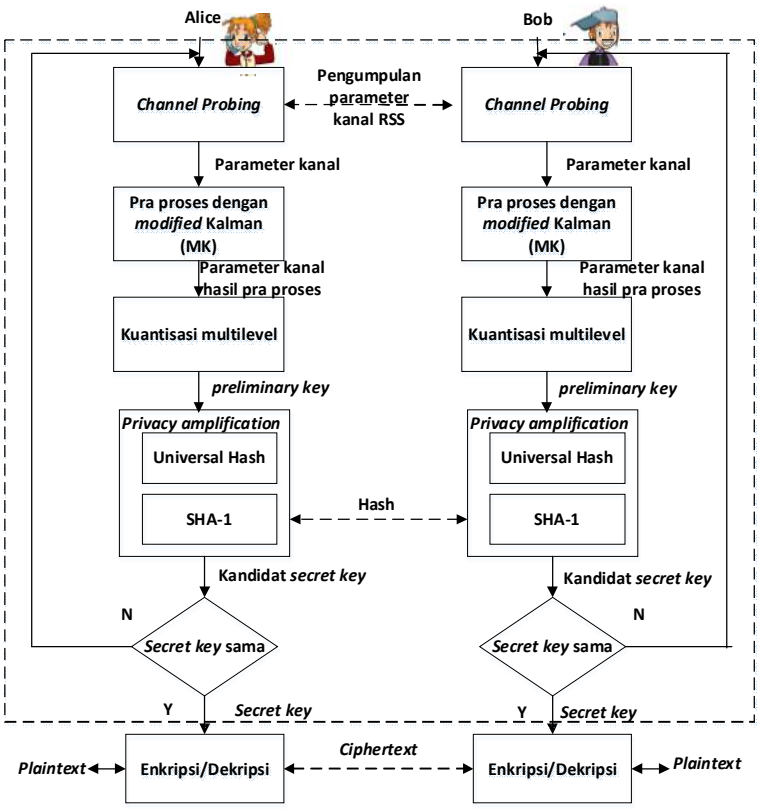
--Halaman ini sengaja dikosongkan--

BAB 4
PENYEDERHAAN SKEMA SKG DENGAN MENGGUNAKAN KOMBINASI METODE *MODIFIED* KALMAN (MK) DAN *COMBINED MULTILEVEL QUANTIZATION* (CMQ)

4.1 Skema SKG dengan Kombinasi Metode *Modified* Kalman (MK) dan *Combined Multilevel Quantization* (CMQ)

Skema SKG yang kami usulkan terdiri dari 4 tahap yaitu *channel probing,* pra proses, kuantisasi multilevel serta *privacy amplification* yang ditunjukkan pada Gambar 4.1. Untuk menyederhanakan prosedur pembangkitan kunci Alice ditunjuk sebagai inisiator. Dibandingkan dengan langsung mengubah parameter kanal RSS hasil pengukuran kedalam bentuk bit (*direct* kuantisasi), kami memilih untuk menambahkan tahap pra proses dengan menggunakan metode MK. Beberapa penelitian (Zhan dkk, 2017; Yuliana dkk, 2017b; Ambekar dkk, 2012; Zhan dkk, 2018) menunjukkan bahwa penambahan tahap pra proses sebelum kuantisasi akan mengurangi ketidakcocokan bit yang dihasilkan. Metode yang kami usulkan yaitu *modified* Kalman (MK) merupakan kombinasi dari metode Regresi Polinomial dan *modified* Kalman Filter. Pada tahap ini, parameter kanal RSS hasil pengukuran dibagi menjadi beberapa blok data dan metode MK akan meningkatkan *reciprocity* dari masing-masing blok data. Keuntungan dari mekanisme ini adalah metode pra proses yang diusulkan bekerja lebih efektif sehingga mampu meningkatkan *reciprocity* (kemiripan) yang lebih signifikan untuk beberapa blok data dan ditunjukkan dengan nilai koefisien korelasi yang mendekati 1. Tahap selanjutnya adalah kombinasi metode MK dengan CMQ. Kuantisasi digunakan untuk mengubah parameter kanal RSS hasil pengukuran menjadi bit. Kami menggunakan kuantisasi multilevel untuk menghindari terlalu sedikitnya bit yang dibangkitkan. Pada tahap ini, kuantisasi juga dilakukan per blok data. Adanya beberapa blok data yang memiliki kemiripan yang sangat tinggi dengan koefisien korelasi mendekati 1 juga berpengaruh pada peningkatan yang signifikan dari beberapa blok data sehingga

meningkatkan kemungkinan perolehan *secret key* yang identik antara dua pengguna yang sah tanpa melalui tahap rekonsiliasi informasi. Dibandingkan dengan penelitian lain yang juga menambahkan tahap pra proses (Zhan dkk, 2017; Yuliana dkk, 2017b; Ambekar dkk, 2012; Zhan dkk, 2018), kami dapat menunjukkan bahwa skema SKG yang kami usulkan lebih sederhana karena dapat mengurangi tahap rekonsiliasi informasi. Keuntungan dari hilangnya tahap ini adalah berkurangnya kesulitan implementasi karena tidak ada pertukaran bit *parity* serta peningkatan keamanan skema SKG yang dibangun karena mengurangi kemungkinan bocornya informasi ke penyadap. Pada tahap *privacy amplification*, kami menambahkan Universal hash untuk meningkatkan keacakan dari *secret key* yang dihasilkan sehingga memenuhi persyaratan keacakan dan SHA-1 untuk menjamin bahwa *secret key* yang dihasilkan antara dua pengguna yang sah adalah sama.



Gambar 4.1 Skema SKG dengan kombinasi metode MK dan CMQ.

Pada tahap *channel probing*, Alice dan Bob melakukan pengukuran parameter kanal RSS y^u, dimana *super-scr*ipt u digantikan dengan A untuk Alice serta B untuk Bob. Namun karena perangkat *wireless* yang digunakan memiliki mode *half duplex*, maka kedua pengguna tersebut tidak dapat melakukan kirim dan terima parameter kanal RSS secara bersamaan. Kami menggunakan perintah *ping* untuk memastikan bahwa waktu *request* dan *response* dari pengukuran parameter kanal tidak melebihi *coherence time*. Diakhir tahap *channel probing* diasumsikan Alice dan Bob akan menyimpan sejumlah parameter kanal $y^A = [y^A(1) + y^A(2) + y^A(3) + ... + y^A(n)]$ untuk Alice serta $y^B = [y^B(1) + y^B(2) + y^B(3) + ... + y^B(n)]$ untuk Bob.

Tahap berikutnya adalah tahap pra proses yang bertujuan untuk meningkatkan *reciprocity* parameter kanal RSS hasil pengukuran kedua pengguna. Skema pra proses yang kami usulkan adalah skema *modified* Kalman (MK) yang menggabungkan Regresi Polinomial (Algoritma 8) dan Kalman Filter (Algoritma 9). Pada Algoritma 8, parameter kanal RSS hasil pengukuran y^u akan dibagi menjadi beberapa blok N hingga didapat sejumlah blok N_B yang dituliskan dengan Persamaan (4.1).

$$y_N = [y_N^T(1).....y_N^T(N_B)] \tag{4.1}$$

Masing-masing y_N berisi data RSS sejumlah S_B. Pada penelitian ini, kami menggunakan regresi polinomial orde 2 atau dikenal dengan kuadratik untuk masing-masing blok data RSS yang ditunjukkan sebagai beriku

$$y_\ell = a_0 + a_1 x_\ell + a_2 x_\ell^{\,2} \tag{4.2}$$

Dimana y_ℓ adalah parameter kanal RSS pada waktu x_ℓ dengan $\ell = (1, 2, ..., S_B)$. Koefisien polinomial a_0, a_1 dan a_2 bisa didapatkan dengan menggunakan Persamaan (4.3).

$$\begin{aligned} (S_B)a_0 + (\sum x_\ell)a_1 + (\sum x_\ell^2)a_2 &= \sum y_\ell \\ (\sum x_\ell)a_0 + (\sum x_\ell^2)a_1 + (\sum x_\ell^3)a_2 &= \sum x_\ell y_\ell \end{aligned} \tag{4.3}$$

$$\left(\sum x_\ell^2\right)a_0+(\sum x_\ell^3)a_1+(\sum x_\ell^4)a_2=\sum x_\ell^2 y_\ell$$

Dimana $\ell=1,2,...,S_B$ sedangkan a_0,a_1 dan a_2 adalah 3 koefisien Polinomial yang tidak diketahui. Cara untuk mendapatkan 3 koefisien Polinomial bisa dilihat pada baris 2-19 (Persamaan 4.3), sedangkan parameter kanal RSS hasil pra proses bisa dilihat pada baris 21.

Algoritma 8: Regresi Polinomial

Input : Parameter kanal hasil pengukuran y^u pada waktu x_ℓ
Input : Jumlah blok N_B
Input : Koefisien polinomial a ,
Input : Orde polinomial m
Output : Parameter kanal hasil pra proses h^u

```
1  : S_B = 128
2  : for i ← 1 to N_B do
3  :     for j ← 1 to m+1 do
4  :         for k ← 1 to j do
5  :             d = j + k − 2
6  :             sum = 0
7  :             for ℓ ← 1 to S_B
8  :                 sum = sum + x_ℓ^d
9  :             end for
10 :             c_{j,k} = sum
11 :             c_{k,j} = sum
12 :         end for
13 :         sum = 0
14 :         for ℓ ← 1 to S_B
15 :             sum = sum + x_ℓ^{j−1} . y_{ℓ,i}^u
16 :         end for
17 :         b_{j,1} = sum
18 :         a_{j,1} = c \ b
19 :     end for
20 :     for ℓ ← 1 to S_B
21 :         h_{ℓ,i}^u = a_{1,i} + a_{2,i} . x_ℓ + a_{3,i} . x_ℓ^2
22 :     end for
23 : end for
```

Data parameter kanal RSS hasil dari tahap pra proses regresi polinomial h^u akan diolah dengan menggunakan Kalman Filter (Algoritma 9) sebelum masuk pada tahap

kuantisasi multilevel. Sama dengan tahap sebelumnya, h^u juga akan dibagi menjadi beberapa blok N hingga didapat sejumlah blok N_B yang dituliskan sebagai berikut.

$$h_N = [h_N^T(1).....h_N^T(N_B)] \tag{4.4}$$

Masing-masing h_N berisi data RSS hasil pra proses sejumlah S_B. Algoritma ini bekerja secara rekursif untuk melakukan estimasi *state* dengan menggunakan estimasi apriori dan aposteriori, dimana estimasi tersebut dilakukan untuk masing-masing blok data. Estimasi awal dilakukan dengan persamaan *time update* sedangkan koreksi terhadap estimasi dilakukan dengan persamaan *measurement update*. *Input* dari persamaan *time update* adalah estimasi apriori $\hat{x}_{k-1}$, kovarian *error* apriori P_{k-1}, serta kovarian *noise* proses Q. Persamaan dari *time update* dinyatakan dengan Persamaan (4.5).

$$\hat{x}_k^- = A\hat{x}_{k-1} \tag{4.5}$$

$$P_k^- = A.P_{k-1}.A + Q$$

Dimana A adalah *state* of pengukuran pada waktu $k-1$. Langkah selanjutnya yang dilakukan adalah proses koreksi terhadap estimasi apriori serta kovarian *error* apriori yang dihasilkan. *Input* dari proses koreksi adalah $\hat{x}_k^-$, P_k^-, data RSS hasil pra proses dengan regresi polinomial h^u, kovarian *noise* pengukuran R serta varian dari masing-masing blok data v^u. Kami melakukan modifikasi terhadap proses koreksi yang ditunjukkan dengan Persamaan (4.6).

$$K_k = (P_k^- H / (HHP_k^- + R)) \tag{4.6}$$

$$P_k = P_k^-(1 - K_k H)$$

$$\hat{x}_k = \hat{x}_k^- + K_k(h_{l,N}^u - H\hat{x}_k^-)$$

$$z_k = \hat{x}_k + 0.2 v_N^u$$

H adalah *state* dari pengukuran pada waktu ke k , $\hat{x}_k$ adalah estimasi aposteriori, P_k adalah kovarian *error* aposteriori, K_k adalah Kalman Gain, sedangkan z_k adalah parameter kanal RSS hasil pra proses dengan menggunakan metode MK. Estimasi aposteriori didapat dengan mengolah parameter kanal pra proses hasil Algoritma 8 di masing-masing blok N. Panjang tiap blok adalah l dengan $l = 1, 2, ..., 128$. Kami memodifikasi hasil estimasi aposteriori dengan menambahkan 0,2 kali dari varian masing-masing blok data dan menghilangkan parameter H dengan tujuan untuk meningkatkan *reciprocity* data hasil pra proses z_k. Pemilihan varian dari masing-masing blok sebagai salah satu parameter modifikasi didasarkan pada hasil pengujian yang menunjukkan adanya peningkatan *reciprocity* (kemiripan) parameter kanal hasil pra proses h'' dengan menggunakan parameter tersebut. Kami menggunakan nilai 0,2 sebagai faktor pengali dari varian masing-masing blok karena didapatkannya beberapa blok data dengan koefisien korelasi antara 0,9979 hingga 0,9999 sehingga bisa diperoleh blok data dengan KDR 0. Jika nilai faktor pengali kurang dari 0,2 maka blok data yang dihasilkan memiliki koefisien korelasi dibawah 0,9979 dan menurunkan kemungkinan dihasilkannya blok data dengan KDR 0. Sebaliknya jika nilai faktor pengali melebihi 0,2 maka semakin besar kemungkinan didapatkannya blok data dengan KDR 0 karena adanya blok data dengan koefisien korelasi diatas 0,9979. Namun permasalahan yang terjadi adalah peningkatan kemungkinan dihasilkannya blok data dengan koefisien korelasi diatas 0,9979 dari pengguna yang sah juga diikuti dengan peningkatan yang koefisien korelasi yang signifikan dari beberapa blok data penyadap hingga mencapai 0,99. Kondisi ini mengurangi tingkat keamanan dari skema SKG yang dibangun. Detil dari mekanisme metode MK dijelaskan pada Algoritma 9. Kami melakukan inisialisasi beberapa parameter yang menghasilkan konfigurasi terbaik di baris 1-2. Proses *time udate* dapat dilihat pada baris 4-5 dan baris 12-13 (Persamaan 4.5), sedangkan modifikasi dari proses *measurement update* dapat dilihat pada baris 6-10 dan baris 14-18 (Persamaan 4.6).

Algoritma 9: *Modified* Kalman (MK)

Input : Parameter kanal hasil pra proses dengan regresi polinomial h^u

Input : *State* pengukuran pada waktu ke $k-1$ A, *state* pengukuran pada waktu ke k H

Input : Kovarian *noise* proses Q, kovarian *noise* pengukuran R

Input : Estimasi apriori $\hat{x}_k^-$, kovarian *error* apriori P_k^-

Input : Estimasi aposteriori $\hat{x}_k$, kovarian *error* aposteriori P_k

Input : Inisialisasi awal $\hat{x}_0$, P_0

Input : Jumlah blok N_B, ukuran masing-masing blok S_B, varian dari masing-masing blok v^u

Output : Parameter kanal hasil pra proses dengan metode MK z^u

1 : $A = 2{,}13$, $H = 2{,}13$, $Q = 0{,}0001$, $R = 4{,}6$

2 : $\hat{x}_0 = 0$, $P_0 = 1$

3 : **for** $i \leftarrow 1$ **to** N_B **do**

4 : $\hat{x}_{k_{1,i}}^- = A.\hat{x}_0$

5 : $P_{k_{1,i}}^- = A.A.P_0 + Q$

6 : $K_{k_{1,i}} = P_{k_{1,i}}^- / (P_0 + R)$

7 : $P_{k_{1,i}} = P_{k_{1,i}}^- (1 - K_{k_{1,i}})$

8 : $\hat{x}_{k_{1,i}} = \hat{x}_{k_{1,i}}^- + K_{k_{1,i}} (h_{1,i}^u - H.\hat{x}_{k_{1,i}}^-)$

9 : $z_{k_{1,i}}^u = \hat{x}_{k_{1,i}}$

10 : $z_{k_{1,i}}^u = z_{k_{1,i}}^u + 0.2.\mathrm{v}_i^u$

11 : **for** $j \leftarrow 2$ **to** S_B **do**

12 : $\hat{x}_{k_{j,i}}^- = A.\hat{x}_{j-1,i}$

13 : $P_{k_{j,i}}^- = A.A.P_{j-1,i} + Q$

14 : $K_{k_{j,i}} = P_{k_{j,i}}^- / (P_{j,i} + R)$

15 : $P_{k_{j,i}} = P_{k_{j,i}}^- (1 - K_{k_{j,i}})$

16 : $\hat{x}_{k_{j,i}} = \hat{x}_{k_{j,i}}^- + K_{k_{j,i}} (h_{j,i}^u - H.\hat{x}_{k_{j,i}}^-)$

17 : $z_{k_{j,i}}^u = \hat{x}_{k_{j,i}}$

18 : $z_{k_{j,i}}^u = z_{k_{j,i}}^u + 0.2.\mathrm{v}_i^u$

19 : **end for**

20 : **end for**

Setelah tahap pra proses, parameter kanal hasil pra proses dengan *modified* Kalman z^u akan diubah menjadi bit dengan menggunakan kuantisasi multilevel sehingga

diperoleh *preliminary key*. Sama dengan tahap sebelumnya, pada tahap ini parameter kanal RSS juga akan dibagi menjadi beberapa blok. Algoritma 10 menunjukkan detil mekanisme dari metode *combined multilevel quantization* (CMQ) yang mengkombinasikan antara metode MK dengan kuantisasi multilevel. *Input* dari algoritma ini adalah z^u, rata-rata dari masing-masing blok μ^u, serta varian dari masing-masing blok v^u. Penentuan *preliminary key* didasarkan pada *Gray coding* b_k di masing-masing level, sedangkan penentuan level didasarkan pada rata-rata dan varian dari masing-masing blok. Data yang berada diluar level akan dibuang. Kami memilih jumlah parameter kanal RSS tiap blok sebanyak $S_B = 128$ karena jumlah tersebut memberikan parameter performansi yang terbaik jika dibandingkan dengan jumlah yang lain. Peningkatan *reciprocity* yang signifikan dari tahap pra proses akan menghasilkan beberapa *preliminary key* yang identik sehingga tidak membutuhkan tahap rekonsiliasi informasi. Tahap ini membutuhkan sinkronisasi dalam komunikasi yang dilakukan serta koneksi jaringan yang bagus. Jika koneksi jaringan buruk maka proses sinkronisasi akan diulang sehingga skema SKG yang dibangun tidak efisien.

Preliminary key yang didapat sebagai *output* dari tahap kuantisasi adakalanya tidak memenuhi persyaratan keacakan. Pada tahap *privacy amplification* kami menambahkan Universal hash untuk memastikan sejumlah kecil kesamaan dengan menggunakan properti aritmatika tertentu. Penambahan fungsi ini akan meningkatkan keacakan *preliminary key* sehingga dapat memenuhi persyaratan *approximate entropy* minimum. Pengujian keacakan dilakukan dengan menggunakan National Institute of Standards and Technology (NIST). *Preliminary key* yang memenuhi persyaratan akan diproses lebih lanjut sehingga bisa digunakan sebagai kunci di *cryptosystem*. Kami menggunakan SHA-1 untuk menjamin bahwa kunci yang didapat dua pengguna yang sah adalah sama. Alice sebagai inisiator mengirim *hash* dari beberapa *preliminary key* ke Bob. Bob juga membangkitkan *hash* dan membandingkan hasilnya dengan Alice. *Hash* yang sama menunjukkan *preliminary key* yang sama. Blok *preliminary key* yang sama akan digunakan sebagai kandidat *secret key*, sedangkan blok yang berbeda akan dibuang. SHA-1 menghasilkan 160-bit *hash digest* sehingga mengirimkan keseluruhan

hash tersebut akan meningkatkan waktu komunikasi antara dua pengguna. Pada penelitian ini, kami hanya mengirimkan 6 bit dari masing-masing blok untuk mendapatkan 98% kebenaran selama proses verifikasi.

Algoritma 10: *Combined Multilevel Quantization* (CMQ)

Input : Parameter kanal hasil pra proses dengan metode MK z^u
Input : Jumlah blok N_B, ukuran masing-masing blok S_B
Input : Varian dari masing-masing blok v^u, rata-rata masing-masing blok μ^u, level kuantisasi L, jumlah bit yang akan diekstrak C
Output : *Preliminary key* K^u

$C = 2$
Construct Gray code b_k ($k \leftarrow 1$ **to** $L = 2^C$)
Masukkan kedalam level yang berbeda [level 1, level 4]
for $i \leftarrow 1$ **to** N_B **do**
  for $j \leftarrow 1$ **to** S_B **do**
    if $z_{j,i}^u < \mu_i^u - \mathrm{v}_i^u$ %level 1
      $K_{j,i}^u = b_1$
    else if $\mu_i^u - \mathrm{v}_i^u < z_{j,i}^u < \mu_i^u$ %level 2
      $K_{j,i}^u = b_2$
    else if $\mu_i^u < z_{j,i}^u < \mu_i^u - \mathrm{v}_i^u$ %level 3
      $K_{j,i}^u = b_3$
    else if $z_{j,i}^u > \mu_i^u - \mathrm{v}_i^u$ %level 4
      $K_{j,i}^u = b_4$
    else
      $z_{j,i}^u$ dibuang
    end if
  end for
end for

4.2 Parameter Performansi yang Digunakan pada Skema SKG dengan Metode MK dan CMQ

Terdapat 4 parameter yang digunakan untuk menentukan performansi dari skema SKG yang diusulkan dengan ringkasan sebagai berikut:

1. Koefisien korelasi Pearson : digunakan untuk menghitung ketergantungan linear antara dua data parameter kanal RSS. Nilai yang dihasilkan berkisar antara −1 hingga 1, dimana −1 menunjukkan korelasi negatif, 0 menunjukkan tidak ada korelasi, sedangkan 1 menunjukkan korelasi yang sempurna. Kami menggunakan parameter ini untuk menentukan keberhasilan dari metode MK yang ditunjukkan dengan peningkatan koefisien korelasi dari pengguna yang sah. Detil pengujian dilakukan dengan membandingkan koefisien korelasi dari blok data parameter kanal RSS hasil pengukuran dengan hasil pra proses menggunakan metode MK. Hasil yang diharapkan adalah adanya peningkatan koefisien korelasi dari beberapa blok data hingga mendekati 1. Semakin mendekati 1 maka semakain besar kemungkinan didapatkannya *secret key* yang identik.
2. *Key disagreement rate* (KDR): digunakan untuk mengetahui jumlah ketidakcocokan bit dari 128- bit di satu blok data RSS. Parameter ini merupakan parameter pertama yang digunakan untuk menentukan kesuksesan dari metode CMQ. Pada penelitian ini kami berupaya untuk menghasilkan skema SKG yang simpel dengan menghilangkan tahap rekonsiliasi informasi. Salah satu persyaratan yang harus dipenuhi untuk menghilangkan tahap ini adalah didapatkannya KDR dengan nilai 0 sehingga bisa didapatkan *secret key* yang benar-benar identik tanpa melalui proses koreksi. Detil pengujian dilakukan dengan membandingkan setiap 128-bit dari hasil CMQ antara dua pengguna yang sah.
3. *Key generation rate* (KGR): digunakan untuk mengetahui banyaknya 128-bit kunci yang dihasilkan dalam satu kali proses skema SKG. Parameter ini merupakan parameter kedua yang digunakan untuk menentukan kesuksesan dari metode CMQ. KGR didapatkan dengan menghitung jumlah bit *secret key* yang berhasil dibangkitkan dalam satu periode waktu tertentu. Bisa dikatakan bahwa tujuan dari parameter ini adalah untuk menentukan kecepatan dari skema SKG yang dibangun dalam mendapatkan *secret key*. Dengan pertimbangan rekomendasi 802.1x (Moore, 2001), *refresh secret key* harus dilakukan setiap 1

jam. Nilai KGR akan memenuhi persyaratan ini jika *secret key* bisa didapatkan dalam rentang waktu tersebut.

4. Keacakan: digunakan untuk menentukan keacakan dari *secret key* yang dihasilkan. Pengujian nilai p dari beberapa parameter dilakukan dengan menggunakan tes NIST. *Secret key* akan memenuhi persyaratan keacakan jika $p \geq 0.01$. Pada penelitian ini, kami menggunakan 6 tes keacakan dari total 15 tes yang ada pada NIST. Tes tersebut meliputi *approximate entropy*, *frequency (monobit) test, Frequency test within a block, runs test, Longest-Run-of-Ones in a Block test,* serta *Cumulative sums test*.

4.3 Skenario Pengujian Eksperimental

Pada bagian ini dijelaskan tentang skenario pengujian yang meliputi jenis perangkat/*software* yang digunakan serta skenario pengukuran. Bagian perangkat/*software* berisi tipe perangkat/*software* serta jumlah perangkat yang digunakan,sedangkan skenario pengukuran berisi mekanisme pengukuran serta lingkungan pengujian.

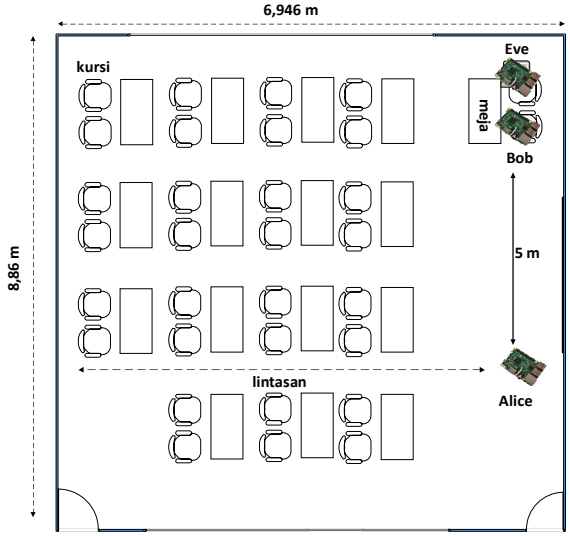
4.3.1 Perangkat/*Software* yang Digunakan

Skema SKG dibangun pada 3 perangkat Raspbery Pi 3 Tipe B. Terdapat 2 perangkat yang menjadi pengguna yang sah yaitu Alice dan Bob, sedangkan perangkat lainnya menjadi penyadap (Eve). Masing-masing perangkat dilengkapi dengan TL-WN722N 802.11 b/g/n wireless card. Gambar perangkat yang digunakan terlihat pada Gambar 3.4 di sub bab 3.3.1. Sistem operasi yang digunakan adalah Linux Raspbian Stretch dengan versi kernel 4.14.74. Pengumpulan data parameter kanal RSS pada tahap *channel probing* dilakukan dengan menggunakan *software* Wireshark menggunakan mekanisme yang telah dijelaskan pada sub bab 3.1.1. Data parameter kanal RSS yang terkumpul di masing-masing pengguna baik pengguna yang sah maupun penyadap adalah 4000. Pada penelitian tentang skema SKG, Raspberry Pi sering digunakan sebagai *tool* untuk mengolah parameter kanal RSS hasil pengukuran

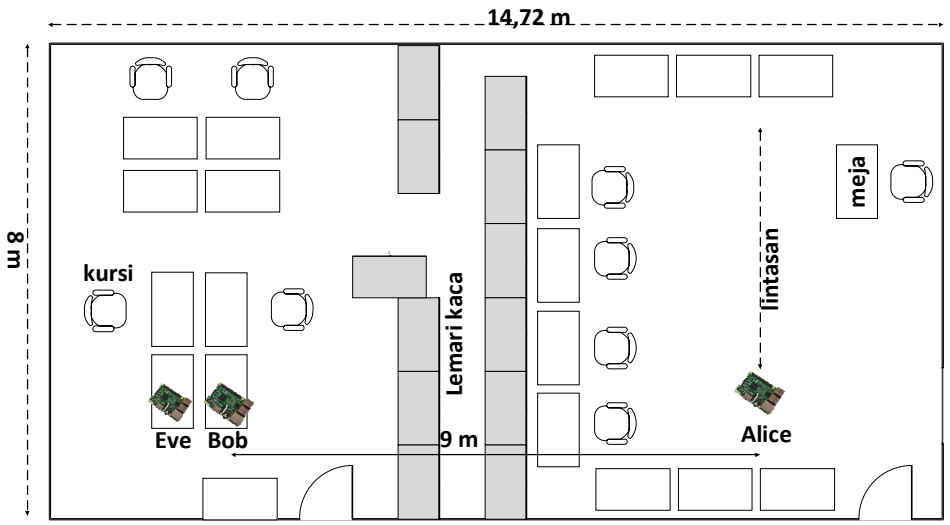
sehingga *secret key* dapat diperoleh (Guillaume dkk, 2015; Lopez dkk, 2017). Pemilihan perangkat ini didasarkan pada kemudahan pemrograman yang digunakan karena menggunakan pemrograman tingkat tinggi yaitu Phyton serta adanya slot tambahan untuk mempermudah konektivitas. Kemudahan ini sangat diperlukan pada berbagai aplikasi IoT.

4.3.2 Skenario Pengujian

Terdapat 2 pengujian yang akan dilakukan pada penelitian ini yaitu skenario 5 dan 6. Seperti yang terlihat pada Gambar 4.2, skenario 5 dilakukan di lingkungan tanpa halangan, sedangkan Gambar 4.3 menunjukkan bahwa skenario 6 dilakukan di lingkungan dengan halangan. Lingkungan yang digunakan skenario 5 sama dengan lingkungan yang digunakan pada skenario 1-3, sedangkan lingkungan yang digunakan skenario 6 sama dengan lingkungan yang digunakan pada skenario 4. Detil lingkungan yang digunakan dari skenario 5 bisa dilihat pada Gambar 3.7 sedangkan lingkungan dari skenario 6 bisa dilihat pada Gambar 3.9.



Gambar 4.2 *Lay out* skenario 5.



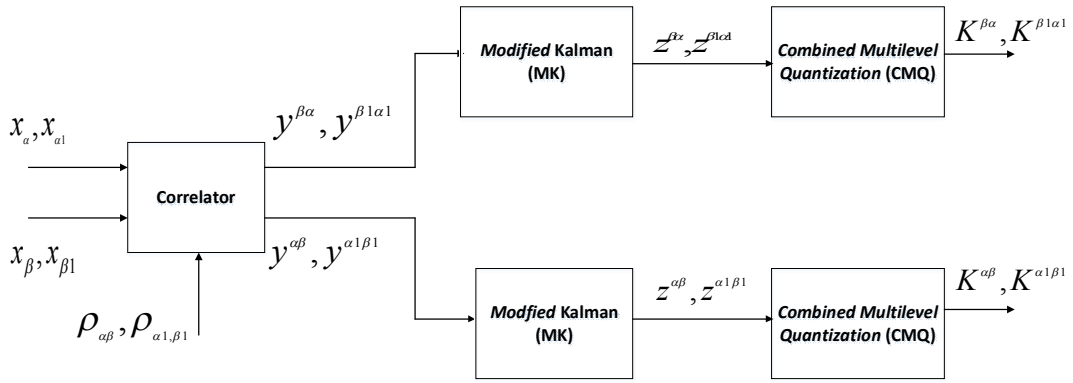
Gambar 4.3 *Lay out* skenario 6.

Pada skenario 5 dan 6 Alice bergerak sepanjang lintasan sedangkan Eve dan Bob diam dengan jarak yang sangat dekat yaitu 10 cm. Pada skenario 5, Alice berjalan sepanjang lintasan dimulai dari jarak 5 m dari Bob. Sedangkan pada skenario 6, Alice berjalan sepanjang lintasan dimulai dari jarak 9 m dari Bob. Pengukuran dilakukan siang hari dengan suhu 24^o C. Tidak ada orang yang lalu lalang selama pengukuran serta tidak ada gangguan yang berarti dari WiFi lain di ruangan tersebut.

4.4 Simulasi Monte Carlo untuk Skema SKG dengan Kombinasi Metode MK dan CMQ

Detil mekanisme simulasi Monte Carlo telah dijelaskan pada sub bab 3.3.1. Pada skema ini kami menggunakan model simulasi yang ditunjukkan oleh Gambar 4.4. Empat bilangan acak yang *independent* dengan panjang data $n = 4.000$, $x_\alpha = [x_\alpha(1), x_\alpha(2), \ldots, x_\alpha(n)]^T$ dan $x_\beta = [x_\beta(1), x_\beta(2), \ldots, x_\beta(n)]^T$ saling berkorelasi dengan distribusi Rician serta $x_{\alpha 1} = [x_{\alpha 1}(1), x_{\alpha 1}(2), \ldots, x_{\alpha 1}(n)]^T$ dan $x_{\beta 1} = [x_{\beta 1}(1), x_{\beta 1}(2), \ldots, x_{\beta 1}(n)]^T$ saling berkorelasi dengan distribusi Rayleigh. Estimasi parameter kanal $y^{\beta\alpha}, y^{\beta 1\alpha 1}$ dan $y^{\alpha\beta}, y^{\alpha 1\beta 1}$ akan diolah dengan metode pra

proses *modified* Kalman (MK) dan *combined multilevel quantization* (CMQ) untuk mendapatkan *preliminary key* $K^{\beta\alpha}, K^{\beta 1\alpha 1}$ dan $K^{\alpha\beta}, K^{\alpha 1\beta 1}$. Evaluasi terhadap performansi skema SKG hasil simulasi dilakukan dengan mengimplementasikan skema tersebut di Matlab dengan nilai koefisien korelasi 0,7 dan 0,6. Pemilihan nilai koefisien korelasi ini disesuaikan dengan koefisien korelasi hasil eksperimen. Pengujian dilakukan dengan melihat keberhasilan metode MK dalam mendapatkan blok data estimasi parameter kanal hasil pra proses yang memiliki koefisien korelasi mendekati 1 serta keberhasilan skema SKG yang dibangun dalam mendapatkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi. Detil Parameter yang digunakan dalam simulasi ditunjukkan pada Tabel 4.1 dimana parameter yang digunakan meliputi jumlah data yang dibangkitkan, distribusi dari data yang dibangkitkan, parameter dari metode MK, serta parameter dari metode CMQ. Parameter yang digunakan pada metode MK meliputi orde polinomial m, panjang data dalam 1 blok S_B, *state* pengukuran pada waktu $k-1$ A, *state* pengukuran pada waktu $k-1$ H, kovarian *noise* proses Q serta kovarian *noise* pengukuran R. Sedangkan parameter yang digunakan pada metode CMQ meliputi jumlah bit yang diekstrak C.

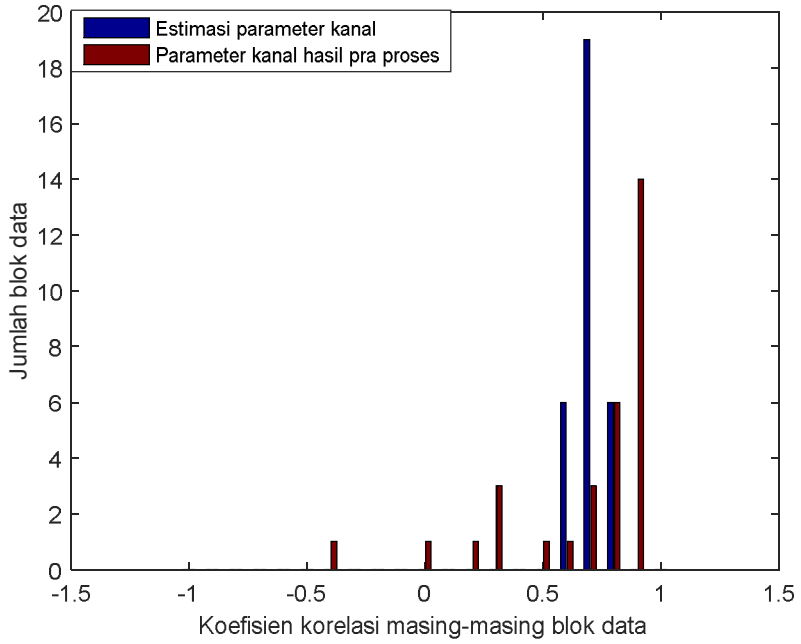


Gambar 4.4 Model simulasi skema SKG dengan Kombinasi Metode MK dan CMQ.

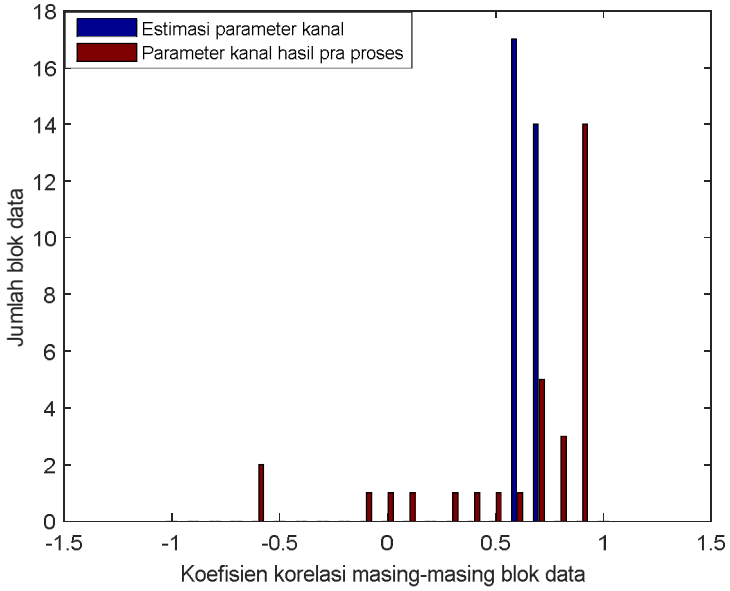
Tabel 4.1 Parameter simulasi skema SKG dengan Kombinasi Metode MK dan CMQ.

No	Parameter	Keterangan
1	Jumlah data n	4000
2	Distribusi data x_α dan x_β	Rician dengan s=4
3	Distribusi data $x_{\alpha 1}$ dan $x_{\beta 1}$	Rayleigh dengan varian=4
4	Orde polynomial m	2
5	Panjang data dalam 1 blok S_B	128
6	*State* pengukuran pada waktu $k-1$ A	2,13
7	*State* pengukuran pada waktu k H	2,13
8	Kovarian *noise* proses Q	0,0001
9	Kovarian *noise* pengukuran R	4,6
10	Jumlah bit yang diekstrak C	2

Gambar 4.5 dan 4.6 menunjukkan banyaknya blok data yang masing-masing berisi 128 estimasi parameter kanal hasil simulasi dan pra proses dari data berdistribusi Rician dan Rayleigh. Hasil pengujian yang dilakukan menunjukkan bahwa blok data estimasi parameter kanal hasil simulasi $y^{\alpha\beta}, y^{\beta\alpha}$ serta $y^{\alpha 1\beta 1}, y^{\beta 1\alpha 1}$ tidak ada yang memiliki koefisien korelasi 0,9. Setelah dilakukan pra proses terlihat adanya peningkatan yang cukup signifikan terhadap jumlah blok data yang memiliki koefisien korelasi 0,9. Jumlah blok data pra proses yang memiliki koefisien korelasi 0,9 lebih banyak didapatkan pada blok data yang berdistribusi Rician. Meningkatnya jumlah blok data yang memiliki koefisien korelasi 0,9 tersebut juga akan meningkatkan kemungkinan didapatkannya *secret key* yang identik dari blok data tersebut tanpa memerlukan tahap rekonsiliasi informasi dengan menggunakan teknik *error correcting*.



Gambar 4.5 Peningkatan koefisien korelasi pada data hasil simulasi berdistribusi Rician.



Gambar 4.6 Peningkatan koefisien korelasi pada data hasil simulasi berdistribusi Rayleigh.

Tabel 4.2 dan 4.3 menunjukkan banyaknya *preliminary key* $K^{\beta\alpha}, K^{\alpha\beta}$ dan $K^{\beta 1\alpha 1}, K^{\alpha 1\beta 1}$ yang dihasilkan dari beberapa variasi KDR dari hasil simulasi data berdistribusi Rician dan rayleigh. Hasil pengujian yang dilakukan menunjukkan bahwa hasil simulasi data Rician dan Rayleigh mampu menghasilkan beberapa *preliminary key* yang identik dengan nilai KDR sebesar 0 sehingga tidak memerlukan tahap rekonsiliasi informasi untuk mendapatkan kandidat *secret key*. Secara keseluruhan terlihat bahwa hasil simulasi data berdistribusi Rician menghasilkan jumlah *preliminary key* identik yang lebih banyak jika dibandingkan dengan data berdistribusi Rayleigh. Kondisi ini terjadi karena adanya peningkatan blok data dengan koefisien korelasi 0,9 yang lebih banyak jika dibandingkan dengan data yang berdistribusi Rayleigh. Peningkatan nilai koefisien tersebut juga meningkatkan kemiripan data pra proses yang dihasilkan sehingga sangat besar kemungkinannya untuk mendapatkan kandidat *secret key* yang identik tanpa memerlukan tahap rekonsiliasi. Hasil lain juga menunjukkan bahwa skema yang eksisting tetap memerlukan tahap rekonsiliasi informasi untuk mendapatkan *secret key* yang identik karena tidak adanya blok data yang memiliki KDR sebesar 0.

Dengan cara yang sama kami membangkitkan dua bilangan acak dengan panjang $n = 4.000$, $x_e = [x_e(1), x_e(2), ..., x_e(n)]^T$ yang berkorelasi dengan x_α berdistribusi Rician dan $x_{e'} = [x_{e'}(1), x_{e'}(2), ..., x_{e'}(n)]^T$ yang berkorelasi dengan x_β juga berdistribusi Rician. Estimasi parameter kanal yang diperoleh adalah $y^{\alpha e}$ dan $y^{\beta e'}$. Dua bilangan acak berikutnya dengan panjang $n = 4.000$, $x_{e1} = [x_{e1}(1), x_{e1}(2), ..., x_{e1}(n)]^T$ yang berkorelasi dengan $x_{\alpha 1}$ berdistribusi Rayleigh dan $x_{e1'} = [x_{e1'}(1), x_{e1'}(2), ..., x_{e1'}(n)]^T$ yang berkorelasi dengan $x_{\beta 1}$ berdistribusi Rician. Estimasi parameter kanal yang diperoleh adalah $y^{\alpha 1e1}$ dan $y^{\beta 1e1'}$. Tabel 4.4 hingga 4.7 menunjukkan banyaknya *preliminary key* yang dihasilkan $y^{\alpha e}$ dan $y^{\beta e'}$ serta $y^{\alpha 1e1}$ dan $y^{\beta 1e1'}$, dimana keempat estimasi parameter kanal tersebut diasumsikan sebagai penyadap. Hasil pengujian menunjukkan bahwa tidak ada *preliminary key* identik yang

berhasil dibangkitkan oleh penyadap karena semua blok data memiliki KDR diatas 0. Secara keseluruhan bisa dikatakan bahwa skema usulan 4 telah memenuhi persyaratan keamanan.

Tabel 4.2 Jumlah 128-bit *preliminary key* hasil simulasi data Rician.

Skema	**KDR**									
	0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
Skema usulan 4	4	30	16	8	2	2	0	0	0	0
Skema 4	0	0	17	45	0	0	0	0	0	0
Skema 7	0	0	4	36	22	0	0	0	0	0
Skema 8	0	0	2	36	16	1	0	0	0	0
Skema 9	0	9	32	20	0	0	0	0	0	0

Tabel 4.3 Jumlah 128-bit *preliminary key* hasil simulasi data Rayleigh.

Skema	**KDR**									
	0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
Skema usulan 4	1	28	20	8	3	2	0	0	0	0
Skema 4	0	0	3	51	8	0	0	0	0	0
Skema 7	0	0	0	28	31	3	0	0	0	0
Skema 8	0	0	0	23	29	3	0	0	0	0
Skema 9	0	0	3	33	24	1	0	0	0	0

Tabel 4.4 Jumlah 128-bit *preliminary key* penyadap $y^{\alpha e}$ hasil simulasi data Rician.

Skema	**KDR**									
	0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
Skema usulan 4	0	12	13	17	8	11	1	0	0	0
Skema 4	0	0	0	4	50	8	0	0	0	0
Skema 7	0	0	0	0	2	32	25	3	0	0
Skema 8	0	0	0	0	3	28	22	2	0	0
Skema 9	0	0	0	53	3	0	0	0	0	0

Tabel 4.5 Jumlah 128-bit *preliminary key* penyadap $y^{\beta e'}$ hasil simulasi data Rician.

Skema	**KDR**									
	0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
Skema usulan 4	0	6	10	20	11	14	1	0	0	0
Skema 4	0	0	0	3	43	16	0	0	0	0
Skema 7	0	0	0	0	1	30	29	2	0	0
Skema 8	0	0	0	0	1	22	30	2	0	0
Skema 9	0	0	3	57	2	0	0	0	0	0

Tabel 4.6 Jumlah 128-bit *preliminary key* penyadap $y^{\alpha 1e1}$ hasil simulasi data Rayleigh.

Skema	**KDR**									
	0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
Skema usulan 4	0	16	7	15	9	13	2	0	0	0
Skema 4	0	0	0	1	36	25	0	0	0	0
Skema 7	0	0	0	0	1	32	27	2	0	0
Skema 8	0	0	0	0	2	26	25	2	0	0
Skema 9	0	0	5	54	2	0	0	0	0	0

Tabel 4.7 Jumlah 128-bit *preliminary key* penyadap $y^{\beta 1e1'}$ hasil simulasi data Rayleigh.

Skema	**KDR**									
	0	**0,1**	**0,2**	**0,3**	**0,4**	**0,5**	**0,6**	**0,7**	**0,8**	**0,9**
Skema usulan 4	0	10	14	18	11	7	2	0	0	0
Skema 4	0	0	0	3	42	17	0	0	0	0
Skema 7	0	0	0	0	3	31	26	2	0	0
Skema 8	0	0	0	0	2	30	23	0	0	0
Skema 9	0	0	7	51	4	0	0	0	0	0

4.5 Hasil Eksperimen Skema SKG dengan Kombinasi Metode MK dan CMQ

Pada bagian ini akan dibahas hasil pengukuran serta evaluasi performansi dari hasil eksperimen skema SKG dengan kombinasi metode MK dan CMQ yang dilakukan pada skenario 5 dan 6. Evaluasi yang dilakukan meliputi evaluasi peningkatan *reciprocity* dengan menggunakan metode MK serta evaluasi performansi kombinasi metode MK dan CMQ.

4.5.1 Hasil Pengukuran

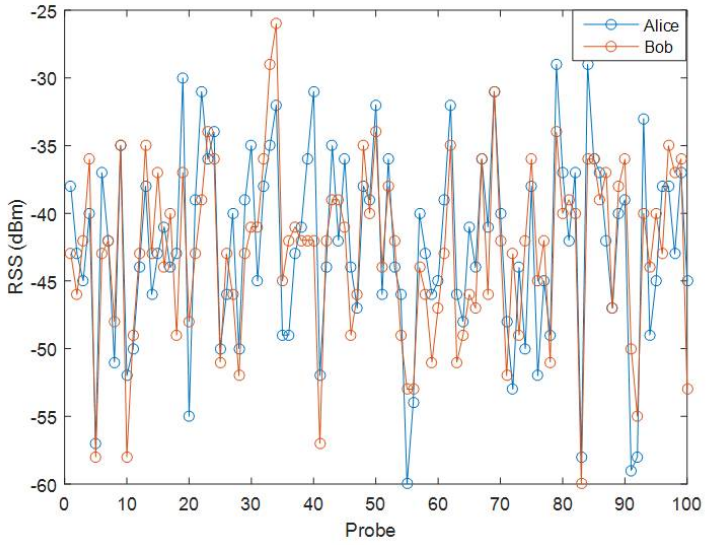
Hasil pengukuran parameter kanal RSS seperti yang terlihat pada Tabel 4.8 menunjukkan adanya korelasi data yang cukup tinggi antar pengguna yang sah. Pada lingkungan tanpa halangan (skenario 5) didapatkan koefisien korelasi 0,7573, sedangkan pada lingkungan dengan halangan (skenario 6) didapatkan korelasi sebesar 0,6988. Lebih kecilnya korelasi data di lingkungan dengan halangan menunjukkan bahwa komponen *multipath* yang terdapat di lingkungan tersebut menyebabkan timbulnya peningkatan perbedaan parameter kanal RSS yang dihasilkan. Komponen tersebut diakibatkan adanya penghalang berupa lemari antara Alice dan Bob sehingga data parameter kanal RSS yang diterima berasal dari beberapa lintasan (*multipath*). Koefisien korelasi yang didapat penyadap sangat rendah atau bisa dikatakan tidak berkorelasi, hal ini menunjukkan bahwa skema SKG yang dibangun telah memenuhi prinsip *spatial decorrelation* sehingga sulit bagi penyadap untuk mendapatkan *secret key* yang sama dengan pengguna yang sah.

Gambar 4.7 dan 4.8 menunjukkan variasi dari pengukuran parameter kanal RSS di skenario 5 dan 6 pada *probe* ke 1 hingga 100 . Hasil pengukuran yang didapatkan menunjukkan bahwa parameter kanal RSS yang didapatkan di skenario 5 cenderung menunjukkan variasi sinyal yang lebih kuat jika dibandingkan dengan skenario 6 yaitu diantara -25 dBm hingga -60 dBm, sedangkan variasi kuat sinyal di skenario 6 adalah -50 hingga -75. Hal ini terjadi karena pada lingkungan tanpa halangan (skenario 5) tidak terdapat penghalang antara Alice dan Bob sehingga kemungkinan untuk mendapatkan sinyal yang lebih kuat juga lebih besar. Pada lingkungan dengan

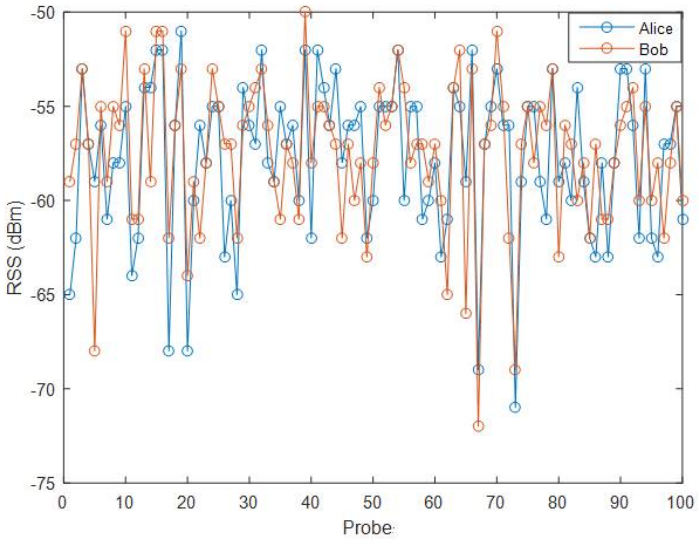
halangan (skenario 6) terdapat penghalang yang mengakibatkan melemahnya sinyal yang diterima.

Tabel 4.8 Koefisien korelasi hasil pengukuran skenario 5 dan 6

Skenario	**Pengguna**	**Koefisien korelasi**
5	Alice- Bob	0,7573
	Alice-Eve	0.0216
	Bob-Eve	0.0153
6	Alice-Bob	0,6988
	Alice-Eve	0.0100
	Bob-Eve	0.0282



Gambar 4.7 Hasil pengukuran parameter kanal RSS di skenario 5.



Gambar 4.8 Hasil pengukuran parameter kanal RSS di skenario 6.

4.5.2 Evaluasi Performansi Skema SKG dengan Kombinasi Metode MK dan CMQ

Di bagian ini, kami menguji keberhasilan skema SKG yang dibangun dengan menggunakan beberapa parameter yang telah ditentukan. Evaluasi ini digunakan untuk menentukan keberhasilan metode yang diusulkan, yaitu MK dan CMQ. Validasi eksperimental dilakukan di dua lingkungan pengujian, yaitu lingkungan tanpa halangan (skenario 5) dan dengan halangan (skenario 6). Keberhasilan metode MK ditunjukkan dengan meningkatnya koefisien korelasi pengguna yang sah. Evaluasi dilakukan dengan membandingkan koefisien korelasi blok data parameter kanal RSS hasil pengukuran dengan hasil pra-proses menggunakan metode MK. Semakin banyak blok data dengan koefisien korelasi mendekati 1, semakin besar kemungkinan untuk mendapatkan *secret key* yang identik. Keberhasilan metode CMQ ditunjukkan oleh keberhasilan memperoleh *secret key* yang identik tanpa memerlukan tahap rekonsiliasi informasi. Tahap ini dapat dihilangkan jika ada blok data RSS yang memiliki KDR dengan nilai 0 dan keberhasilan mendapatkan *secret key* dalam rentang waktu yang direkomendasikan 802.1x. Kecepatan skema SKG untuk mendapatkan *secret key* dalam periode waktu tersebut ditunjukkan oleh parameter KGR. Selain itu, kami juga

melakukan tes NIST untuk memastikan bahwa *secret key* yang dihasilkan telah memiliki $p \geq 0,01$ untuk memenuhi persyaratan keacakan.

4.5.2.1 Evaluasi Peningkatan *Reciprocity* dengan Menggunakan Metode *Modified* Kalman (MK)

Pengujian keberhasilan dari algoritma MK ditunjukkan dengan meningkatnya koefisien korelasi dari pengguna yang sah. Pada pengujian ini, kami membagi membagi parameter kanal RSS menjadi beberapa blok data yaitu 64 dan 128. Tujuan pembagian blok data ini adalah untuk memastikan peningkatan korelasi dari masing-masing blok data sehingga mampu meningkatkan kemiripan *secret key* yang dihasilkan. Pemilihan jumlah parameter kanal RSS di masing-masing blok didasarkan pada metode kuantisasi yang digunakan. Kami menggunakan metode kuantisasi multilevel yang merubah 1 data RSS menjadi 2 bit, sehingga jika 1 blok berisi 64 data RSS maka 1 blok tersebut akan dikonversi menjadi 128 bit. Jika 1 blok berisi 128 parameter kanal RSS maka 1 blok tersebut akan dikonversi menjadi 256 bit. Karena panjang *secret key* yang digunakan adalah 128 bit, maka blok data tersebut akan dibagi menjadi 2 sehingga masing-masing berisi 128 bit.

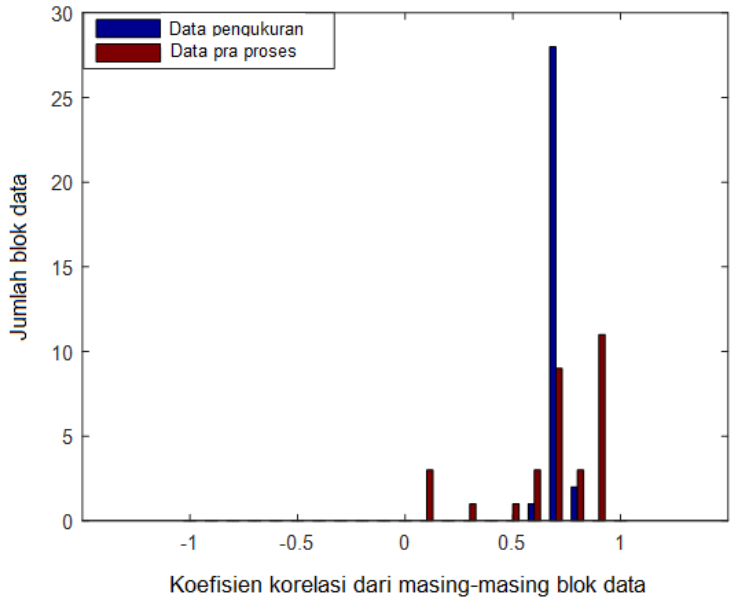
Tabel 4.9 menunjukkan performansi dari algoritma MK dibandingkan dengan hasil pengukuran untuk keseluruhan parameter kanal RSS. Nilai koefisien korelasi yang didapat merupakan nilai dari keseluruhan parameter kanal RSS setelah dilakukan pengolahan parameter kanal RSS per blok dengan menggunakan metode MK. Hasil pengujian yang dilakukan menunjukkan bahwa pembagian parameter kanal RSS menjadi beberapa blok data yang berisi 128 parameter kanal RSS memberikan peningkatan koefisien korelasi pengguna yang sah baik di lingkungan tanpa halangan maupun dengan halangan. Sebenarnya pembagian parameter kanal RSS menjadi blok data yang berisi 64 parameter kanal RSS menghasilkan peningkatan koefisien korelasi yang lebih signifikan di lingkungan dengan halangan dibandingkan dengan blok data yang berisi 128 parameter kanal RSS, namun hal sebaliknya justru terjadi di lingkungan tanpa halangan dimana koefisien korelasi yang didapat mengalami penurunan. Hal ini

terjadi karena adanya penurunan koefisien korelasi saat pengolahan data dengan menggunakan Regresi Polinomial yang eksisting (Algoritma 8) sehingga saat diolah dengan menggunakan *Modified Kalman* (MK) (Algoritma 9) tidak menunjukkan adanya peningkatan koefisien korelasi. Koefisien korelasi penyadap juga mengalami peningkatan namun hasil yang didapat masih jauh dibawah koefisien korelasi yang didapat pengguna yang sah, sehingga masih sulit bagi penyadap untuk mendapatkan *secret key* yang sama dengan pengguna yang sah.

Kami melakukan analisa yang lebih detil terhadap peningkatan koefisien korelasi pengguna yang sah di masing-masing blok data yang berisi 128 parameter kanal RSS seperti yang terlihat pada Gambar 4.9 dan 4.10. Pengujian dilakukan dengan membandingkan koefisien korelasi masing-masing blok data hasil pengukuran dengan hasil pra proses menggunakan metode MK. Hasil pengujian koefisien korelasi pengguna yang sah di lingkungan tanpa halangan pada Gambar 4.9 menunjukkan bahwa kebanyakan blok data parameter kanal RSS hasil pengukuran memiliki koefisien korelasi 0,7. Setelah dilakukan pra proses terlihat adanya peningkatan yang cukup signifikan terhadap jumlah blok data yang memiliki koefisien korelasi 0,9 yaitu antara 0,9114 hingga 0,9999. Terdapat 2 blok data yang memiliki koefisien korelasi 0,9996 dan 0,9999 sehingga sangat besar kemungkinan didapatkannya *secret key* yang identik dari kedua blok data tersebut tanpa memerlukan tahap rekonsiliasi informasi dengan menggunakan teknik *error correcting*.

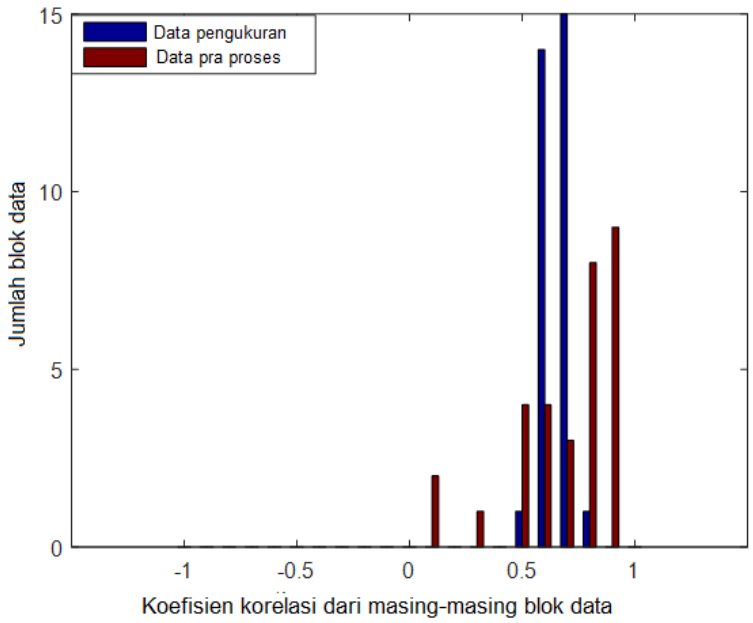
Tabel 4.9 Peningkatan koefisien korelasi dengan menggunakan metode MK

Skenario	**Pengguna**	**Koefisien korelasi hasil pengukuran**	**Peningkatan koefisien korelasi untuk blok parameter kanal RSS**	
			64	**128**
5	Alice-Bob	0,7573	0,7500	0,8195
	Alice-Eve	0,0216	-0,0062	0,2017
	Bob-Eve	0,0153	0,1657	0,1995
6	Alice-Bob	0,6988	0,7782	0,7650
	Alice-Eve	0,0100	0,3016	0,2922
	Bob-Eve	0,0282	0,3682	0,3876



Gambar 4.9 Peningkatan koefisien korelasi dari masing-masing blok data di lingkungan tanpa halangan (skenario 5)

Hasil pengujian masing-masing blok data parameter kanal RSS di lingkungan dengan halangan pada Gambar 4.10 juga menunjukkan adanya peningkatan koefisien korelasi jika dibandingkan dengan blok data parameter kanal RSS hasil pengukuran. Dari hasil pra proses terlihat adanya 9 blok data yang memiliki koefisien korelasi 0,9 dengan *range* nilai antara 0,9028 hingga 0,9979. Satu blok diantaranya memiliki koefisien korelasi sebesar 0,9979 sehingga besar kemungkinan blok data tersebut menghasilkan *secret key* yang identik tanpa memerlukan tahap rekonsiliasi informasi dengan menggunakan teknik *error correcting*. Secara umum terlihat bahwa metode MK menghasilkan peningkatan koefisien korelasi yang lebih baik di lingkungan tanpa halangan. Hal ini terlihat dari lebih banyaknya blok data yang memiliki koefisien korelasi 0,9 jika dibandingkan dengan lingkungan dengan halangan sehingga memiliki kemungkinan yang lebih besar untuk menghasilkan *secret key* yang identik. Kondisi ini terjadi karena secara keseluruhan data parameter kanal RSS hasil pra proses di lingkungan tanpa halangan menghasilkan koefisien korelasi yang lebih tinggi jika dibandingkan dengan data parameter kanal RSS hasil pra proses di lingkungan dengan halangan.



Gambar 4.10 Peningkatan koefisien korelasi dari masing-masing blok data di lingkungan dengan halangan (skenario 6)

Dari keseluruhan pengujian yang telah dilakukan terlihat bahwa metode MK mampu meningkatkan koefisien korelasi secara signifikan di beberapa blok data hingga mencapai 0,9 sehingga meningkatkan kemungkinan untuk mendapatkan *secret key* yang identik. Peningkatan jumlah blok data yang memiliki koefisien korelasi 0,9 mencapai 35,48% di lingkungan tanpa halangan dan 29,03% di lingkungan dengan halangan. Hal ini menunjukkan keberhasilan dari penambahan metode MK di skema SKG yang dibangun karena kemampuannya untuk meningkatkan *reciprocity* parameter kanal RSS hasil pengukuran.

4.5.2.2 Evaluasi Performansi Penggunaan Metode CMQ

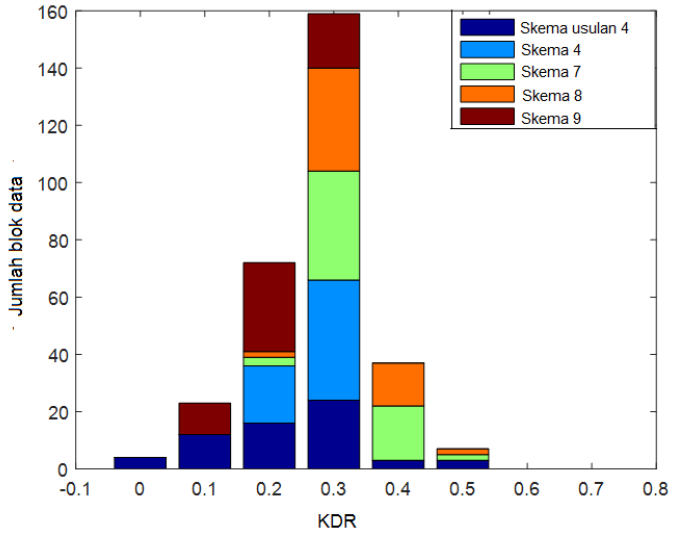
Pada bagian ini, kami membandingkan performansi antara skema SKG yang mengkombinasikan metode MK dan CMQ (skema usulan 4) dengan beberapa skema yang eksisting. Pada skema ini kami menggunakan metode CMQ yang mengolah data parameter kanal RSS hasil pra proses z^u dengan metode MK menjadi *preliminary key* K^u. Skema kuantisasi yang digunakan merupakan skema kuantisasi multilevel yang

menggunakan rata-rata μ^u dan varian v^u (Ambekar dkk, 2012) untuk menentukan level dari masing-masing data parameter kanal RSS. Terdapat 4 skema eksisting yang akan digunakan sebagai pembanding, dimana skema tersebut meliputi skema 4, 7 hingga 9. Skema 4 (Ambekar dkk, 2012) juga menggunakan rata rata dan varian untuk menentukan level dari masing-masing data RSS, namun rata-rata dan varian didapatkan dari blok data yang masing-masing berisi 10 parameter kanal RSS. Skema 7 (Premnath dkk, 2013) menggunakan interval dari data parameter kanal RSS yang telah diurutkan, dimana skema ini mengunakan nilai $C = 2$ sebagai jumlah bit yang akan diekstrak pada tiap interval. Skema 8 (Zeng dkk, 2010) menggunakan *guard band* di masing-masing interval data RSS dengan nilai α sebagai rasio perbandingan *guard band* dengan total data parameter kanal RSS sebesar 0,1. Skema 9 (Yuliana dkk, 2017b) merupakan pengembangan dari skema 4. Dibandingkan skema 4 yang menggunakan 2 parameter, maka skema 9 ini menggunakan 3 parameter yaitu rata-rata, standar deviasi serta α sebagai parameter yang akan dikalikan dengan standar deviasi. Nilai α yang digunakan adalah sebesar 0,01.

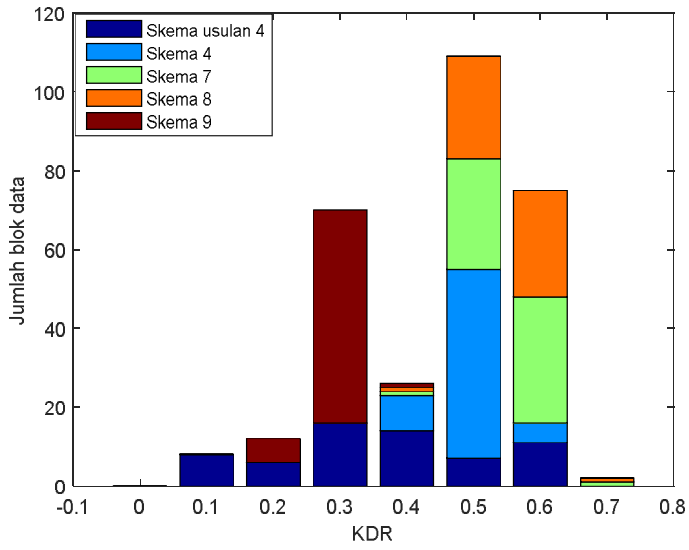
Pengujian performansi dari skema usulan 4 dilihat dari beberapa parameter yaitu KDR, KGR serta keacakan. Pengujian KDR bertujuan untuk mengetahui perbedaan bit yang dihasilkan dari tahap kuantisasi multilevel terhadap total bit dalam satu blok data. Karena skema SKG yang dibangun tidak menggunakan tahap rekonsiliasi informasi, maka kandidat *secret key* bisa didapatkan jika KDR yang didapatkan sebesar 0. KGR menunjukkan banyaknya bit yang dihasilkan dalam satu waktu tahapan skema SKG. Semakin tinggi nilai KGR maka semakin cepat waktu yang dibutuhkan untuk mendapatkan *secret key*. Parameter keacakan bertujuan untuk mengetahui tingkat keacakan dari *secret key* yang dihasilkan. Tingkat keacakan yang dihasilkan dapat dilihat dari nilai *significance level* α. Semakin tinggi nilai α yang dihasilkan maka semakin acak nilai *secret key* yang dihasilkan. Pada sistem kriptografi, nilai α minimal yang harus terpenuhi adalah 0,01($p \geq \alpha$).

Gambar 4.11 menunjukkan hasil perbandingan KDR antar pengguna yang sah yang dihasilkan pada pengujian di skenario 5 antara skema usulan 4 dengan beberapa skema

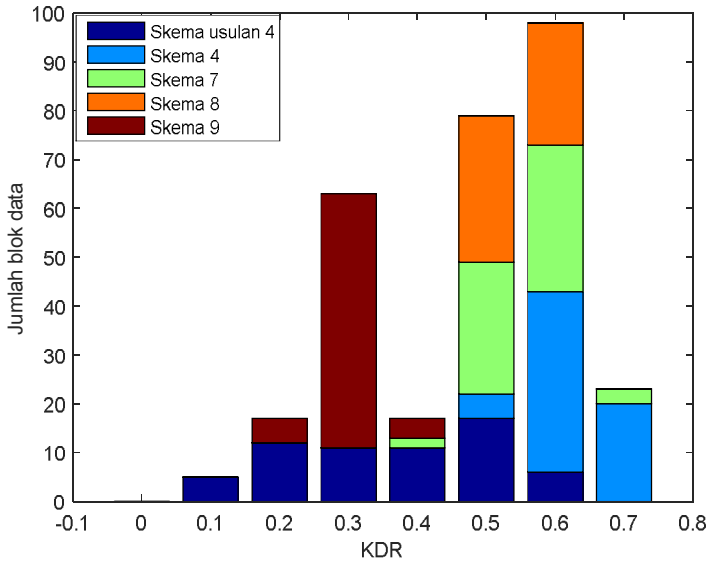
yang eksisting. Hasil pengujian KDR pengguna yang sah menunjukkan bahwa skema usulan 4 mampu menghasilkan 4 kandidat *secret key* yang identik tanpa memerlukan tahap rekonsiliasi informasi karena KDR yang dihasilkan bernilai 0. Kondisi ini terjadi karena adanya peningkatan koefisien korelasi hingga mencapai 0,9999 pada beberapa blok data dengan digunakannya algoritma MK. Peningkatan nilai koefisien tersebut juga meningkatkan kemiripan data pra proses yang dihasilkan sehingga sangat besar kemungkinannya untuk mendapatkan *secret key* yang identik tanpa memerlukan tahap rekonsiliasi. Hasil pengujian juga menunjukkan bahwa tidak ada *secret key* identik yang dihasilkan skema yang eksisting karena nilai KDR yangg dihasilkan melebihi 0 sehingga tetap diperlukan teknik *error correcting* untuk melakukan rekonsiliasi informasi. Gambar 4.12 dan 4.13 menunjukkan KDR yang didapatkan antara penyadap dan pengguna yang sah. Terlihat bahwa KDR yang dihasilkan tidak ada yang bernilai 0 sehingga penyadap tidak mendapatkan *secret key* yang identik dengan pengguna yang sah. Dibandingkan dengan KDR antar pengguna yang sah terlihat bahwa KDR yang didapatkan penyadap dengan pengguna yang sah memiliki nilai yang lebih tinggi yaitu antara 0,5 hingga 0,6. Dari hasil ini bisa dikatakan bahwa banyak blok data penyadap yang memiliki perbedaan bit dengan blok data pengguna yang sah, sehinggga semakin sulit bagi penyadap untuk mendapatkan *secret key* yang identik.



Gambar 4.11 KDR pengguna yang sah di skenario 5.

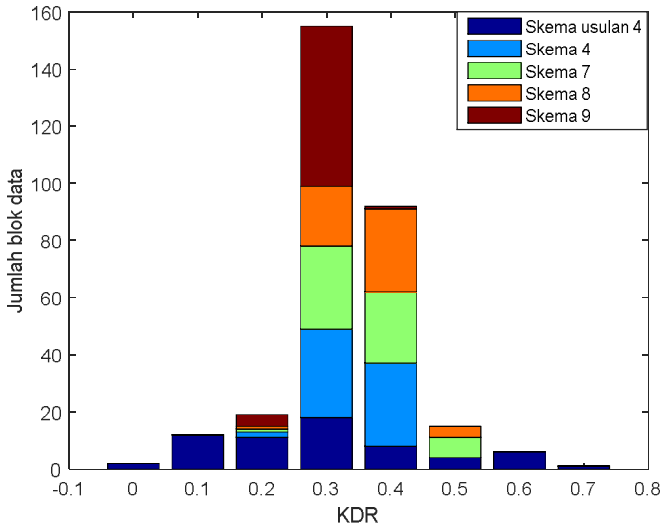


Gambar 4.12 KDR penyadap (Alice-Eve) di skenario 5.

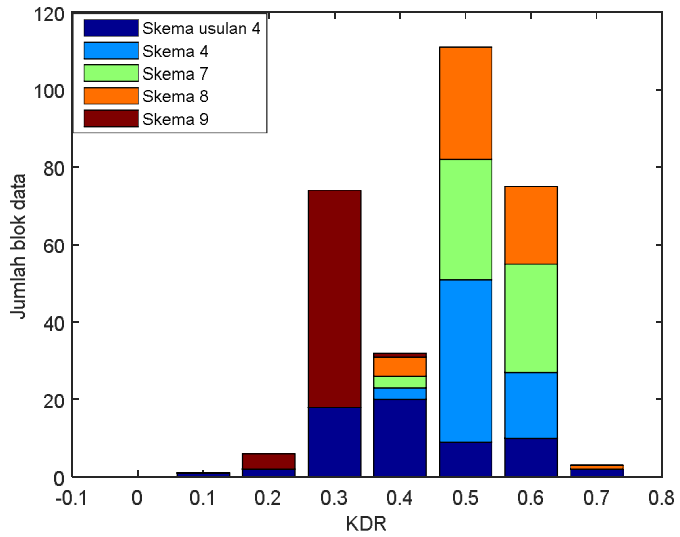


Gambar 4.13 KDR penyadap (Bob-Eve) di skenario 5.

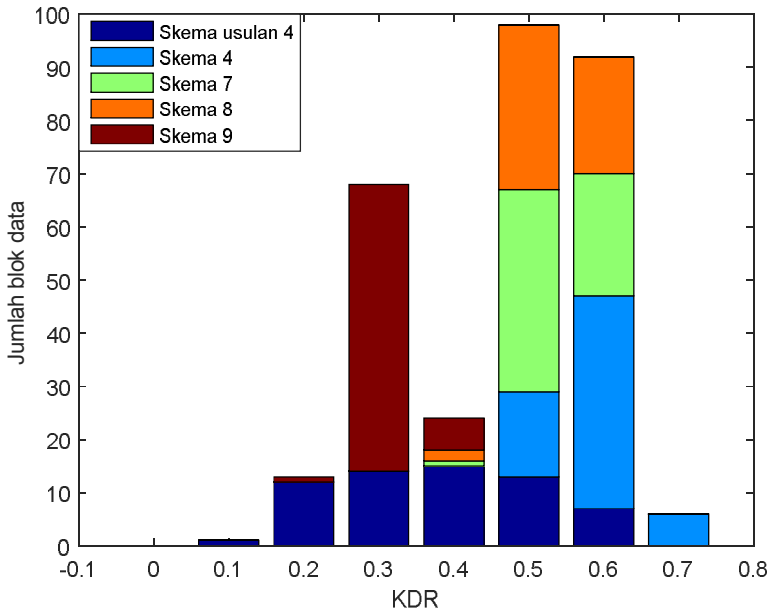
Gambar 4.14 menunjukkan nilai KDR yang didapatkan pengguna yang sah di skenario 6. Hasil pengujian yang dilakukan menunjukkan bahwa skema usulan kami mampu menghasilkan 2 *secret key* yang identik tanpa memerlukan teknik *error correcting* karena terdapat 2 blok data yang memiliki nilai KDR 0. Jumlah *secret key* identik yang dihasilkan masih lebih sedikit jika dibandingkan dengan pengujian di lingkungan tanpa halangan. Hal ini terjadi karena secara keseluruhan nilai koefisien korelasi di lingkungan dengan halangan masih lebih kecil jika dibandingkan dengan lingkungan tanpa halangan, selain itu jumlah blok data yang mengalami peningkatan koefisien korelasi hingga 0,9 juga lebih sedikit jika dibandingkan dengan lingkungan tanpa halangan. Gambar 4.15 dan 4.16 menunjukkan KDR antara pengguna yang sah dengan penyadap. Hasil pengujian yang dilakukan menunjukkan bahwa tidak ada KDR yang bernilai 0, sehingga penyadap tidak mendapatkan *secret key* yang identik dengan pengguna yang sah. Dibandingkan dengan pengujian di lingkungan tanpa halangan, maka nilai KDR yang didapat penyadap di lingkungan dengan halangan cenderung lebih tinggi yaitu di antara 0,5 hingga 0,7. Hal ini menunjukkan semakin sulitnya penyadap untuk mendapatkan *secret key* identik karena semakin banyaknya blok data penyadap yang memiliki ketidakcocokan bit dengan blok data pengguna yang sah.



Gambar 4.14 KDR pengguna yang sah di skenario 6.



Gambar 4.15 KDR penyadap (Alice-Eve) di skenario 6



Gambar 4.16 KDR penyadap (Bob-Eve) di skenario 6

Parameter pengujian berikutnya adalah keacakan dengan menggunakan NIST. Terdapat 6 pengujian yang dilakukan untuk memastikan keacakan kandidat *secret key* yang dihasilkan dari tahap *privacy amplification*. Dari hasil pengujian di Tabel 4.10

terlihat bahwa semua *secret key* yang dihasilkan telah memenuhi persyaratan keacakan dengan nilai p melebihi 0,01 untuk semua pengujian. Prioritas dari pemilihan kunci sebagai *secret key* adalah kunci 4, 3, 1 dan 2. Pemilihan ini didasarkan pada nilai *approximate entropy* dari masing-masing kunci. Jika prioritas pertama gagal pada tahap verifikasi maka kunci berikutnya yang akan digunakan sebagai *secret key* adalah prioritas kedua yaitu kunci 3. Secara umum, kunci 4 memiliki nilai p yang lebih tinggi jika dibandingkan dengan kunci yang lain. Hasil pengujian *approximate entropy* menunjukkan nilai p hingga 0,9801. Semakin tinggi nilai pengujian menunjukkan tingginya nilai ketidakteraturan bit yang dihasilkan sehingga rangkaian kunci yang dihasilkan semakin acak. Nilai p tertinggi dari hasil *frequency (monobit) test* adalah 0,859684. Semakin tinggi hasil pengujian menunjukkan proporsi bit 1 dan 0 yang hampir sama atau mendekati 1/2 sehingga bisa didapatkan distribusi yang sesuai dengan persyaratan keacakan. Pada *frequency test within a block* nilai tertinggi didapat pada kunci 1 yaitu sebesar 0,5295. Hal ini menunjukkan bahwa kunci 1 memiliki proporsi bit 1 yang lebih mendekati separuh blok sehingga sesuai dengan yang diharapkan pada asumsi keacakan. Hasil *runs test* dari kunci 1 juga menunjukkan nilai p yang lebih besar dibandingkan dengan kunci lainnya yaitu sebesar 0,9200. Hasil tersebut menunjukkan bahwa osilasi yang terjadi pada kunci tersebut lebih cepat jika dibandingkan dengan kunci yang lain. Pengujian *Longest-Run-of-Ones in a Block* menunjukkan bahwa kunci 4 memiliki panjang bit 1 yang lebih konsisten terhadap panjang bit 1 yang diharapkan dari sebuah rangkaian kunci yang acak. Hasil pengujian *cumulative sums* (*forward* dan *backward*) menunjukkan bahwa jumlah kumulatif dari kunci yang dihasilkan sesuai dengan jumlah kumulatif yang diharapkan dari sebuah rangkaian acak. Terlalu banyak bit 1 atau 0 diawal rangkaian kunci (mode 0) serta diakhir kunci (mode 1) akan mengakibatkan nilai p yang dihasilkan terlalu kecil sehingga tidak memenuhi persyaratan keacakan.

Tabel 4.10 Tes NIST Skema usulan 4 skenario 5

Tes NIST	**Nilai** p			
	Kunci 1	**Kunci 2**	**Kunci 3**	**Kunci 4**
Approximate Entropy	0,5949	0,0122	0,8411	0.9801
Frequency (Monobit)	0,2888	0,3768	0,7237	0,8597
Frequency Test within a Block	0,5295	0,0791	0,3239	0,4186
Runs	0,9200	0,1887	0,3823	0,7215
Longest-Run-of-Ones in a Block	0,3909	0,5083	0,4960	0,8770
Cumulative Sums (forward)	0,3146	0,7375	0,6548	0,8920
Cumulative Sums (backward)	0,4314	0,4314	0,9493	0,8188

Hasil tes keacakan NIST pada skenario 6 ditunjukkan pada Tabel 4.11. Terdapat 2 kunci dengan prioritas pertama sebagai *secret key* yaitu kunci 1 dengan nilai *approximate entropy* sebesar 0,9167. Jika verifikasi gagal maka kunci 2 dapat digunakan sebagai kunci alternatif. Secara keseluruhan dapat dikatakan bahwa semua *secret key* yang dihasilkan telah memenuhi persyaratan keacakan karena nilai p yang dihasilkan telah melebihi 0,01. Kunci 1 menunjukkan ketidakteraturan yang jauh lebih tinggi jika dibandingkan dengan kunci 2. Hal ini ditunjukkan dengan nilai p kunci 1 yang lebih tinggi jika dibandingkan dengan kunci 2 pada pengujian *approximate entropy*. Untuk memenuhi persyaratan keacakan. kunci yang diperoleh harus memiliki proporsi bit 1 dan 0 yang mendekati 1/2. Hasil *frequency (monobit) test* menunjukkan bahwa kunci 1 memiliki proporsi bit 1 dan 0 yang lebih mendekati 1/2 sehingga memiliki nilai p yang lebih tinggi jika dibandingkan dengan kunci 2. Hasil yang sama juga diperoleh pada pengujian *frequency test within a block*. dimana kunci 1 memiliki proporsi bit 1 yang lebih mendekati separuh blok sehingga memiliki memiliki nilai p yang lebih tinggi dibandingkan kunci 2. Pada pengujian *runs* terlihat bahwa kunci 2

berosilasi lebih cepat jika dibandingkan dengan kunci 1. selain itu kunci 2 juga memiliki panjang bit 1 yang lebih konsisten terhadap panjang bit 1 yang diharapkan dari sebuah rangkaian kunci yang acak dibandingkan dengan kunci 1. Kunci 2 memiliki banyak bit 1 atau 0 yang lebih banyak diawal serta diakhir rangkaian kunci sehingga nilai p yang dihasilkan lebih kecil jika dibandingkan kunci 1. Secara keseluruhan terlihat bahwa kunci 1 memiliki nilai p yang lebih baik jika dibandingkan dengan kunci 2. Keseluruhan hasil pengujian NIST di lingkungan tanpa halangan dan dengan halangan menunjukkan nilai p yang telah melebihi 0,01 sehingga bisa dikatakan bahwa *secret key* yang dihasilkan telah memenuhi persyaratan keacakan dengan kepercayaan hingga 99%.

Tabel 4.11 Tes NIST skema usulan 4 skenario 6

Tes NIST	**Nilai** p	
	Kunci 1	**Kunci 2**
Approximate Entropy	0,9167	0,1825
Frequency (Monobit)	0,5959	0,0216
Frequency Test within a Block	0,7568	0,6359
Runs	0,4632	0,5020
Longest-Run-of-Ones in a Block	0,1517	0,2029
Cumulative Sums (forward)	0,8920	0,0267
Cumulative Sums (backward)	0,4314	0,0340

KGR merupakan parameter performansi yang digunakan dengan tujuan untuk menentukan kecepatan dari skema SKG yang dibangun dalam mendapatkan *secret key*. Hasil dari pengujian KGR pada Tabel 4.12 menunjukkan nilai KGR yang lebih tinggi di lingkungan tanpa halangan (skenario 5) yaitu sebesar 0,92 bps sehingga dibutuhkan waktu kurang lebih 2,32 menit untuk mendapatkan 128 bit *secret key* yang akan digunakan untuk mengacak pesan pesan dengan menggunakan metode AES-128. Skema SKG yang dibangun telah memenuhi rekomendasi 802.1x karena waktu yang dibutuhkan untuk membangkitkan *secret key* kurang dari 1 jam yaitu 2,32 menit. Demikian juga dengan hasil pengujian di lingkungan dengan halangan yang membutuhkan waktu 4,74 menit untuk membangkitkan 128 bit *secret key*. Rata-rata nilai *approximate entropy* di kedua lingkungan pengujian berkisar antara 0,5 hingga 0,6, dengan nilai rata-rata yang lebih rendah didapatkan di lingkungan dengan halangan (skenario 6). Dari semua pengujian yang telah dilakukan dapat dikatakan bahwa kombinasi metode MK dan CMQ mampu menghasilkan skema SKG yang sederhana dengan menghilangkan tahap rekonsiliasi informasi. Keberhasilan ini ditunjukkan dengan dihasilkannya beberapa blok data yang memiliki nilai KDR 0. Hasil pengujian yang dilakukan di lingkungan dengan halangan dan tanpa halangan juga menunjukkan waktu yang dibutuhkan untuk mendapatkan *secret key* jauh dibawah 1 jam yaitu 2,32 menit (skenario 5) serta 4,74 menit (skenario 6) dengan KGR mencapai 0,92 bps (skenario 5) dan 0,45 bps (skenario 6).

Tabel 4.12 KGR skema usulan 4 di skenario 5 dan 6

Skenario	**KGR (bps)**	**Rata-rata *approximate entropy***
5 (tanpa halangan)	0,92	0,61
6 (dengan halangan)	0,45	0,55

4.6 Matrik Perbandingan Parameter Performansi Skema SKG Kombinasi Metode MK dan CMQ dengan Skema yang Eksisting

Pada bagian ini akan dibandingkan performansi skema SKG kombinasi metode MK dan CMQ dengan skema yang eksisting. Parameter performansi yang dibandingkan meliputi Jumlah 128-bit blok data hasil kuantisasi dengan variasi KDR antara 0 hingga 0,1, KGR, kompleksitas, serta durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG. Parameter KDR digunakan untuk mengetahui jumlah ketidakcocokan bit dari 128-bit di satu blok data RSS. Pada penelitian ini akan diuji jumlah blok data dengan KDR yang dihasilkan dimasing-masing blok tersebut. Jika terdapat blok data dengan KDR yang bernilai 0, maka tidak dibutuhkan tahap rekonsiliasi informasi utnuk mendapatkan *secret key* yang identik. KGR digunakan untuk mengetahui banyaknya 128-bit kunci yang dapat dibangkitkan dalam satu kali tahapan skema SKG, sedangkan durasi waktu digunakan untuk mengetahui lamanya waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG. Parameter KGR yang digunakan sebagai perbandingan adalah KGR_{pa}. Kompleksitas digunakan untuk mengetahui seberapa jauh keefektifan sebuah algoritma dalam meminimumkan waktu dan ruang, dimana waktu dan ruang suatu algoritma ini bergantung pada ukuran masukan (n), yang menyatakan jumlah data yang diproses.

Table 4.13 menunjukkan perbandingan kompleksitas dari skema usulan 4 serta skema yang eksisting. Kami melakukan pengujian kompleksitas di tiap tahapan skema SKG. Skema usulan kami menggunakan 4 tahap yang meliputi channel probing, pra proses, kuantisasi, dan *privacy amplification*. Skema yang eksisting menggunakan 5 tahap dengan menambahkan tahap rekonsiliasi informasi. Analisa kompleksitas hanya dilakukan pada 4 tahap terakhir karena 4 tahap tersebut kompleksitasnya tergantung dari algoritma yang dibuat. Secara keseluruhan terlihat bahwa skema usulan kami memiliki jumlah tahap yang lebih sedikit dengan kompleksitas yang sama di tahap kuantisasi dan privacy amplification. Pada tahap pra proses skema usulan kami menghasilkan kompleksitas yang paling tinggi karena adanya 2 metode pra proses yang digunakan dengan masing-masing tahap memiliki kompleksitas $o(nm)$. Meskipun

skema usulan kami memiliki kompleksitas yang lebih tinggi di tahap pra proses dibandingkan dengan beberapa skema yang eksisting namun dengan berkurangnya tahap rekonsiliasi informasi akan mengurangi durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG secara signifikan. Hal ini terjadi karena pada tahap rekonsiliasi informasi terdapat mekanisme pembangkitan parity yang akan semakin meningkat jika data yang harus dikoreksi semakin banyak.

Tabel 4.13 Perbandingan kompleksitas tahapan skema SKG usulan 4

Skema	**Kompleksitas masing-masing tahapan skema SKG**					
	Pra proses		**Kuantisasi**	**Rekonsiliasi informasi**	**Privacy**	
	Pra proses 1	**Pra proses 2**			**Universal hash**	**SHA-1**
Skema usulan 4	$O(pq)$	$O(pq)$	$O(pq)$	----	$O(p^2)$	$O(p)$
Skema 4	$O(n)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 7	$O(n)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 8	$O(n)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 9	$O(n)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$

Tabel 4.14 menunjukkan matrik perbandingan performansi skema SKG kombinasi metode MK dan CMQ dengan skema yang eksisting. Dari pengujian parameter KDR terlihat bahwa tidak ada 128-bit blok data hasil kuantisasi yang memiliki KDR sebesar 0 pada skema SKG yang eksisting sehingga masih dibutuhkan tahap rekonsiliasi informasi untuk mendapatkan *secret key* yang identik. Skema usulan 4 terbukti mampu untuk mendapatkan *secret key* yang identik tanpa melalui tahap rekonsiliasi informasi, dimana hal ini ditunjukkan dengan didapatkannya beberapa128-bit blok data hasil

kuantisasi dengan nilai KDR 0. Hasil pengujian parameter KGR dari skema yang eksisting menunjukkan nilai yang lebih tinggi jika dibandingkan dengan skema usulan 4. Hal ini terjadi karena skema eksisting menggunakan tahap rekonsiliasi informasi untuk melakukan koreksi terhadap perbedaan bit antara kedua pengguna sehingga meningkatkan kemungkinan untuk mendapatkan 128-bit blok data yang identik. Kelebihan dari skema usulan 4 terletak pada dihilangkannya tahap rekonsiliasi informasi untuk mendapatkan *secret key* yang identik sehingga mampu mengurangi durasi waktu yang dibutuhkan dalam satu tahapan skema SKG. Dari hasil pengujian terlihat adanya penurunan yang signifikan dari durasi waktu yang dibutuhkan hingga sebesar 0,42 (simulasi) dan 0,63 (eksperimen) dari skema yang eksisting. Penurunan durasi waktu ini sangat berguna untuk implementasi skema SKG pada perangkat dengan keterbatasan sumber daya.

Tabel 4.14 Matrik Perbandingan performansi skema SKG kombinasi metode MK dan CMQ dengan skema yang eksisting.

Skenario	Skema	Simulasi												Eksperimen											
		KDR										KGR / bps	Durasi / menit	KDR										KGR / bps	Durasi / menit
		0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9			0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9		
5	Skema usulan 4	4	30	16	8	2	2	0	0	0	0	9,22	0,93	4	12	16	24	3	3	0	0	0	0	0,92	9,28
	Skema 4	0	0	17	45	0	0	0	0	0	0	58,1	2,17	0	0	20	42	0	0	0	0	0	0	7.69	14,99
	Skema 7	0	0	4	36	22	0	0	0	0	0	44,2	2,03	0	0	3	38	19	2	0	0	0	0	5.94	14,36
	Skema 8	0	0	2	36	16	1	0	0	0	0	36,5	2,04	0	0	2	36	15	2	0	0	0	0	5.63	14,40
	Skema 9	0	9	32	20	0	0	0	0	0	0	57,2	2,20	0	11	31	19	0	0	0	0	0	0	8.67	15,01
6	Skema usulan 4	1	28	20	8	3	2	0	0	0	0	2,29	0,93	2	12	11	18	8	4	6	1	0	0	0,45	9,48
	Skema 4	0	0	3	51	8	0	0	0	0	0	48,8	2,18	0	0	2	31	29	0	0	0	0	0	4.42	14,95
	Skema 7	0	0	0	28	31	3	0	0	0	0	29,1	2,05	0	0	1	29	25	7	0	0	0	0	3.87	14,32
	Skema 8	0	0	0	23	29	3	0	0	0	0	28,0	2,05	0	0	1	21	29	4	0	0	0	0	3.42	14,33
	Skema 9	0	0	3	33	24	1	0	0	0	0	58,8	2,21	0	5	43	13	0	0	0	0	0	0	8.36	15,05

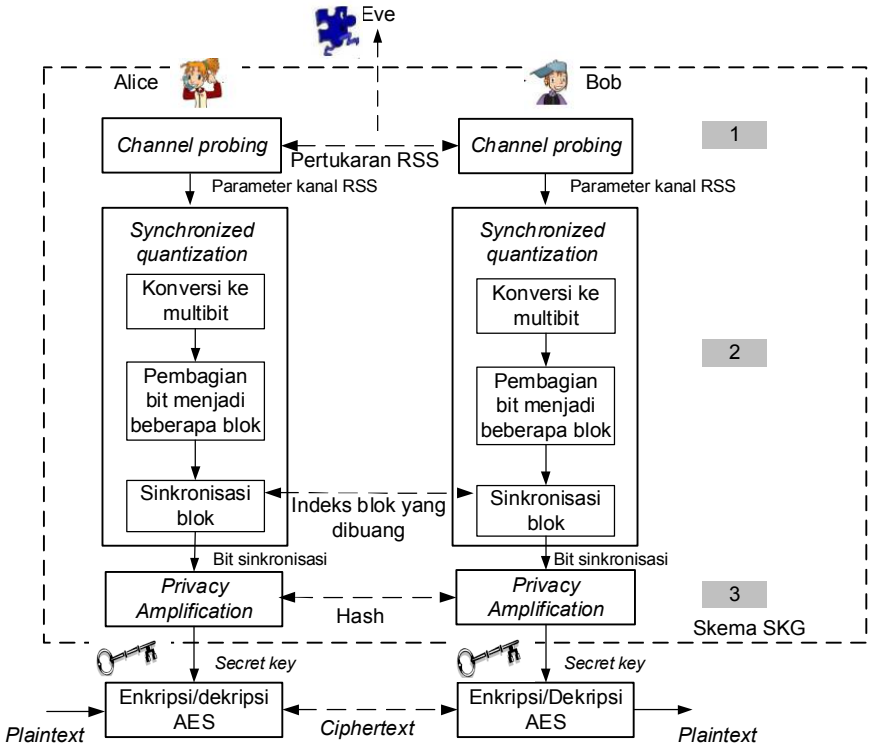
BAB 5
EFISIENSI SKEMA SKG PADA *INTERNET OF THINGS* (IoT) DENGAN MENGGUNAKAN *SYNCHRONIZED QUANTIZATION* (SQ)

5.1 Skema SKG SSE

Beberapa penelitian yang eksisting (Zhan dkk, 2019; Cheng dkk, 2017; Jiang dkk, 2018) menggunakan protokol pembangkitan kunci yang terdiri dari 4 tahap yaitu *channel probing*, kuantisasi, rekonsiliasi informasi serta *privacy amplification*. Hasil yang didapatkan menunjukkan bahwa *direct* kuantisasi dapat mengakibatkan tingginya ketidakcocokan bit yang dihasilkan ditahap kuantisasi. Penambahan tahap pra proses pada (Ambekar dkk, 2012; Zhan dkk, 2017; Zhan dkk, 2018; McGuire 2014; Ali dkk 2010; Yuliana dkk, 2018a; Yuliana dkk, 2018b) bertujuan untuk mengurangi ketidakcocokan bit yang dihasilkan. Namun dibandingkan dengan (Yuliana dkk, 2019a) maka penelitian yang menggunakan 5 langkah tersebut cenderung kurang efisien dengan adanya penambahan tahap pra proses dan rekonsiliasi informasi sehingga meningkatkan waktu komputasi. Tahap rekonsiliasi informasi digunakan untuk mengoreksi perbedaan bit yang dihasilkan kedua pengguna yang sah. Semakin tinggi perbedaan bit yang terjadi akan meningkatkan kompleksitas komputasional pada tahap tersebut karena semakin banyak blok data yang harus dikoreksi.

Untuk mengatasi permasalahan tersebut kami mengusulkan skema SKG *signal strength exchange* (SSE) sebagai skema untuk membangkitkan *secret key* yang terdiri dari dari 3 tahap yaitu *channel probing*, *synchronized quantization* (SQ), serta *privacy amplification* seperti yang terlihat pada Gambar 5.1. Skema tersebut lebih sederhana jika dibandingkan dengan skema yang eksisting sehingga diharapkan mampu mengurangi waktu komputasi, *overhead* komunikasi serta sesuai untuk perangkat IoT dengan keterbatasan sumber daya. Pengukuran parameter kanal RSS dilakukan di dua lingkungan yang berbeda yaitu lingkungan dengan penghalang (skenario 5) dan tanpa

penghalang (skenario 6). Pada waktu pengukuran Alice sebagai salah satu pengguna yang sah dipilih sebagai inisiator. Hasil pengukuran parameter kanal RSS akan diubah menjadi bit dengan menggunakan proses kuantisasi. Sebagai bagian dari skema SKG SSE, kami juga mengusulkan metode kuantisasi baru yaitu *synchronized quantization* (SQ) yang melakukan sinkronisasi pada tahap kuantisasi. Sinkronisasi dilakukan antara kedua pengguna yang sah untuk memastikan bahwa *secret key* yang dihasilkan benar-benar sama sehingga bisa menghilangkan tahap rekonsiliasi informasi sebagai bagian dari skema pembangkitan kunci. Selain hilangnya rekonsiliasi informasi, keuntungan lain dari penggunaan metode SQ adalah hilangnya tahap pra proses. Hal ini terjadi karena metode SQ mampu menghasilkan bit kunci yang benar-benar sama langsung dari parameter kanal RSS hasil pengukuran. Pada langkah *privacy amplification* kami menggunakan Universal hash untuk mengaburkan bagian kunci yang bocor ke penyadap dan SHA-1 untuk memastikan bahwa kunci yang dihasilkan kedua pengguna yang sah adalah sama.



Gambar 5.1 Skema SKG SSE.

Tahap pertama dari skema SKG SSE adalah *channel probing* yang melakukan mekanisme pengukuran parameter kanal RSS antar pengguna yang sah. Alice sebagai inisiator melakukan *ping* dan Bob sebagai responder memberikan respons. Masing-masing pengguna menyimpan parameter kanal RSS hasil pengukuran sehingga didapatkan $y^A = [y^A(1) + y^A(2) + ... + y^A(n)]$ dan $y^B = [y^B(1) + y^B(2) + ... + y^B(n)]$ untuk Alice dan Bob. *Reciprocity* dari parameter kanal RSS didapatkan dengan memastikan waktu *ping* dan respons dari pengukuran tidak melebihi *coherence time*.

Tahap kedua adalah konversi parameter kanal hasil pengukuran y^u menjadi bit dengan menggunakan metode *Synchronized Quantization* (SQ). *Subscript u* bisa digantikan dengan A untuk Alice serta B untuk Bob. Metode ini bekerja dengan menggunakan 3 parameter yaitu standar deviasi σ^u, rata-rata μ^u serta a untuk menentukan bit yang dihasilkan di masing-masing area. Pada penelitian ini parameter standar deviasi dan rata-rata dihitung dari keseluruhan parameter kanal RSS hasil pengukuran, sedangkan parameter a digunakan sebagai pembagi dari standar deviasi parameter kanal RSS hasil pengukuran. Ketiga parameter tersebut digunakan untuk menentukan area dari masing-masing parameter kanal. Penentuan konversi bit Q^u dari masing-masing area ditentukan dengan menggunakan *Gray coding* seperti yang ditunjukkan oleh Persamaan (5.1). Dari persamaan tersebut terlihat bahwa seluruh parameter kanal akan dikonversi menjadi multi bit dan tidak ada parameter kanal yang terbuang. Rangkaian multibit K^u yang dihasilkan terlihat di Persamaan (5.2).

$$Q^u = \begin{cases} y^u \le \mu^u - (\dfrac{\sigma^u}{a}) & ,00 \\ \mu^u - (\dfrac{\sigma^u}{a}) < y^u < \mu^u & ,01 \\ \mu^u \le y^u < \mu^u + (\dfrac{\sigma^u}{a}) & ,11 \\ y^u \ge \mu^u + (\dfrac{\sigma^u}{a}) & ,10 \end{cases} \tag{5.1}$$

$$K^u = [Q^u(1), Q^u(2), ...Q^u(n)]^T \tag{5.2}$$

Tidak ada parameter kanal yang terbuang sehingga panjang dari K^u adalah N, dimana $N = 2xn$. Rangkaian K^u yang diperoleh akan dipecah menjadi beberapa blok sejumlah B_N dimana masing-masing blok berisi 3 bit sehingga didapatkan $K_B = [K_B^T..K_B^T(N_B)]$. Langkah selanjutnya adalah sinkronisasi dari blok bit K_B. Blok akan disimpan jika ketiga bit dalam blok adalah sama (yaitu 000 atau 111). Jika ketiga bit dalam blok berbeda maka blok akan dibuang. Sinkronisasi dilakukan dengan melakukan pertukaran indeks blok yang dibuang antara kedua pengguna yang sah. Setelah sinkronisasi selesai maka blok bit yang tersisa tersebut akan dikonversi kembali menjadi satu rangkaian bit. Penjelasan detil dari metode SQ yang dijalankan di masing-masing pengguna bisa dilihat pada Algoritma 11. Kami melakukan inisialisasi 2 parameter yaitu a and C yang mampu menghasilkan konfigurasi paling optimal seperti yang ditunjukkan pada baris 1. Penentuan jumlah area dan konversi bit dari masing-masing parameter kanal ditunjukkan pada baris 2-3. Mekanisme konversi dari parameter kanal RSS kedalam bentuk multi bit ditunjukkan pada baris 4–14 (Persamaan (5.1) dan (5.2)), sedangkan pembagian bit kedalam beberapa blok dan sinkronisasi masing-masing blok ditunjukkan pada baris 15-26.

Tahap terakhir adalah *privacy amplification* yang terdiri dari mekanisme keacakan dan verifikasi. Mekanisme peningkatan keacakan digunakan untuk meningkatkan keacakan dari bit hasil sinkronisasi dan menghilangkan kemungkinan adanya informasi yang diperoleh penyadap saat tahap blok sinkronisasi. Rangkaian bit hasil sinkronisasi Key_u akan ditingkatkan keacakannya dengan menggunakan Universal Hash. Metode ini bekerja dengan secara acak memilih fungsi *hash* dengan sifat matematika tertentu yang dapat memastikan keacakan dari data yang dihasilkan. Keuntungan dari metode ini adalah kecilnya kemungkinan untuk mendapatkan data yang sama meskipun data tersebut juga dipilih oleh penyadap. Pada skema SKG ini, peningkatan keacakan dilakukan pada Key_u yang telah dibagi menjadi beberapa blok bit kunci. Masing-masing blok terdiri dari 128-bit kunci dan akan diuji dengan menggunakan NIST. Blok yang telah memenuhi persyaratan akan digunakan sebagai *secret key*.

Algoritma 1: *Synchronized Quantization* (SQ)

Input : Parameter kanal RSS hasil pengukuran y^u sebanyak n

Input : Standar deviasi dari keseluruhan parameter kanal RSS σ^u, rata-rata dari keseluruhan parameter kanal RSS μ^u

Input : Jumlah konversi bit dari masing-masing parameter kanal C

Input : Panjang bit hasil konversi N, jumlah blok bit N_B

Output : Rangkaian bit hasil sinkronisasi Key^u

1 : $a = 0,6 - 0,85$, $C = 2$

2 : Penentuan jumlah area 2^C

3 : Penentuan C bit di masing-masing area dengan *Gray Coding* $[Q_1^u, Q_{2^C}^u]$

4 : **for** $i \leftarrow 1$ **to** n **do**

5 : | **if** $y_i^u \le \mu_i^u - \left(\sigma_i^u / a\right)$ %area 1

6 : | $K_i^u = Q_1^u$

7 : | **else if** $\mu_i^u - \left(\sigma_i^u / a\right) < y_i^u < \mu_i^u$ %area 2

8 : | $K_i^u = Q_2^u$

9 : | **else if** $\mu_i^u \le y_i^u < \mu_i^u + \left(\sigma_i^u / a\right)$ %area 3

10 : | $K_i^u = Q_3^u$

11 | **else if** $y_i^u \ge \mu_i^u + \left(\sigma_i^u / a\right)$ %area 4

12 : | $K_i^u = Q_4^u$

13 : **end if**

14 : **end for**

15 : **for** $i \leftarrow 1$ **to** N_B

16 : | $K_{B_i} = 0$

16 : | **for** $j \leftarrow 1$ **to** 3

17 : | | $K_{B_i} = K_{B_i} + K_{j,i}^u$

18 : | **end for**

19 : | **if** $K_{B_i} == 3$

20 : | | $Key_i^u = 1$

21 : | **else if** $K_{B_i} == 0$

22 : | | $Key_i^u = 0$

23 : | **else**

24 : | | Key_i^u dibuang

25 : | **end if**

26 : **end for**

Mekanisme verifikasi dilakukan untuk memastikan bahwa kunci yang digunakan oleh pengguna yang sah adalah sama. Pada penelitian ini, blok 128-bit *secret key* yang telah memenuhi persyaratan keacakan akan dijadikan *hash* dengan menggunakan SHA-1. Kami memilih metode ini karena tingginya keamanan dari hash yang dihasilkan serta sering digunakan untuk fungsi *one-way* sehingga kesamaan kunci dapat dilihat tanpa membuka informasi apapun ke penyadap. SHA-1 membangkitkan *hash* sepanjang 160 bit sehingga waktu komunikasi antara kedua pengguna yang sah akan meningkat jika semua bit tersebut dikirim. Namun SHA-1 memiliki kemampuan untuk mendeteksi bit yang berbeda meskipun sangat sedikit, sehingga hanya 6 bit dari hash yang akan dikirim dengan kemampuan koreksi hingga 98%. Hubungan antara panjang bit ℓ kemampuan koreksi c dinyatakan dengan Persamaan (5.3).

$$1-\left(\frac{1}{2}\right)^{\ell} \geq c$$
$$\ell = \lceil \log_{1/2}(1-c) \rceil \tag{5.3}$$

5.2 Parameter Performansi yang Digunakan pada Skema SKG SSE

Kami melakukan evaluasi skema SKG yang dibangun dengan menggunakan beberapa parameter yaitu key generation rate (KGR), key disagreement rate (KDR), keacakan, waktu komputasi serta *overhead* komunikasi. KGR, waktu komputasi dan *overhead* komunikasi merupakan parameter yang *implementational dependent* karena sangat dipengaruhi oleh kemampuan perangkat yang digunakan. KDR dan keacakan merupakan parameter yang *implementational independent* karena tidak dipengaruhi oleh kemampuan perangkat yang digunakan namun dipengaruhi oleh metode yang digunakan di masing-masing tahap skema SKG. Ringkasan dari masing-masing parameter dijelaskan sebagai berikut.

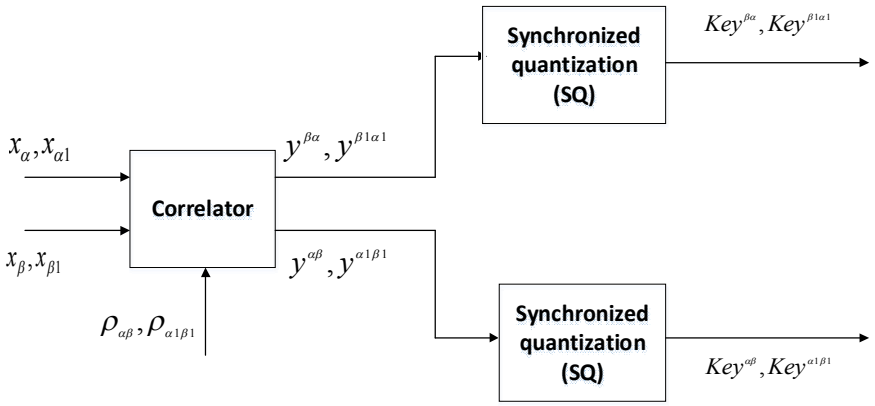
1. *Key generation rate* (KGR) : banyaknya bit yang identik selama durasi komunikasi skema SKG. Tujuan dari skema SKG SSE ini adalah untuk melakukan perbaruan kunci setiap 15 menit. Waktu perbaruan kunci ini telah memenuhi persyaratan yang diusulkan oleh (Moore, 2001) karena waktu tersebut masih dibawah 1 jam.

2. *Key Disagreement rate* (KDR) : Jumlah perbedaan bit dari 128-bit kunci hasil sinkronisasi yang diperoleh setelah tahap SQ. Nilai KDR yang diharapkan adalah 0 untuk 128-bit hasil sinkronisasi yang didapat pengguna yang sah dan KDR diatas 0 untuk untuk 128-bit hasil sinkronisasi yang didapat dari penyadap.
3. Keacakan : 128-bit kunci hasil sinkronisasi yang dihasilkan diuji dengan menggunakan 6 tes keacakan dari NIST yaitu *approximate entropy, frequency (monobit) test, Frequency test within a block, runs test, Longest-Run-of-Ones in a Block test,* serta *Cumulative sums test* untuk menghasilkan nilai P. Nilai P minimal yang diharapkan adalah 0,01 sehingga dapat memenuhi persyaratan keacakan.
4. Waktu komputasi : lamanya waktu yang dibutuhkan untuk menyelesaikan masing-masing tahap dalam skema SKG. Semakin rendah kompleksitas dari tahap yang dilakukan maka semakin rendah waktu komputasi yang dihasilkan sehingga sesuai untuk perangkat IoT yang memiliki keterbatasan daya dan komputasi.
5. *Overhead* komunikasi : banyaknya *byte* yang dikirimkan untuk komunikasi dua pengguna. Pada skema SKG SSE *overhead* komunikasi sangat dipengaruhi oleh banyaknya indeks blok yang dibuang pada tahap *synchronized quantization* (SQ) serta banyaknya *hash* yang dikirim pada saat *privacy amplification*.

5.3 Simulasi Monte Carlo untuk Skema SKG SSE

Detil mekanisme simulasi Monte Carlo telah dijelaskan pada sub bab 3.3.1. Pada skema ini kami menggunakan model simulasi yang ditunjukkan oleh Gambar 5.2. Empat bilangan acak yang *independent* dengan panjang data $n = 4.000$, $x_\alpha = [x_\alpha(1), x_\alpha(2), ..., x_\alpha(n)]^T$ dan $x_\beta = [x_\beta(1), x_\beta(2), ..., x_\beta(n)]^T$ saling berkorelasi dengan distribusi Rician serta $x_{\alpha 1} = [x_{\alpha 1}(1), x_{\alpha 1}(2), ..., x_{\alpha 1}(n)]^T$ dan $x_{\beta 1} = [x_{\beta 1}(1), x_{\beta 1}(2), ..., x_{\beta 1}(n)]^T$ saling berkorelasi dengan distribusi Rayleigh. Estimasi parameter kanal $y^{\beta\alpha}, y^{\beta 1\alpha 1}$ dan $y^{\alpha\beta}, y^{\alpha 1\beta 1}$ akan diolah dengan metode *Synchronized quantization* (SQ) untuk mendapatkan bit kunci hasil sinkronisasi

$Key^{\beta\alpha}, Key^{\beta 1\alpha 1}$ dan $Key^{\alpha\beta}, Key^{\alpha 1\beta 1}$. Evaluasi terhadap performansi skema SKG SSE hasil simulasi dilakukan dengan mengimplementasikan skema tersebut di Matlab dengan nilai koefisien korelasi tertentu. Pengujian dilakukan dengan melihat banyaknya kunci hasil sinkronisasi yang dapat dibangkitkan dengan model simulasi yang digunakan.



Gambar 5.2 Model simulasi skema SKG SSE.

Detil Parameter yang digunakan dalam simulasi ditunjukkan pada Tabel 5.1 dimana parameter yang digunakan meliputi jumlah data yang dibangkitkan, serta distribusi dari data yang dibangkitkan. Parameter yang digunakan pada metode SQ meliputi parameter pembagi standar deviasi yaitu a yang bernilai antara 0,6 hingga 0,8 serta jumlah ekstraksi bit C sebesar 2 sehingga didapatkan jumlah area sebanyak 2^C. Tabel 5.2 menunjukkan perbandingan banyaknya kunci hasil sinkronisasi yang dapat dibangkitkan. Dari hasil pengujian yang dilakukan terlihat bahwa hasil simulasi data berdistribusi Rician menghasilkan jumlah 128-bit kunci yang lebih banyak jika dibandingkan dengan hasil simulasi data berdistribusi Rayleigh. Hal ini terjadi karena pengolahan metode SQ mengakibatkan kebanyakan data berdistribusi Rician berada di area 2 dan dan 3 sehingga kunci hasil sinkronisasi yang dihasilkan didominasi oleh bit 1. Variasi yang rendah dari bit yang dihasilkan meningkatkan probabilitas didapatkannya 128-bit kunci hasil sinkronisasi yang identik. Hasil pengujian metode SQ di data berdistribusi Rayleigh menunjukkan penurunan jumlah 128-bit kunci hasil sinkronisasi yang identik. Semakin meningkatnya jumlah estimasi parameter kanal di

area 1 dan 4 juga meningkatkan probabilitas didapatkannya 3 sekuensial bit yaitu 000 dan dikonversi ke 0. Semakin tinggi variasi bit 1 dan 0 dari 128-bit kunci yang dihasilkan maka semakin tinggi kemungkinan didapatkannya perbedaan bit kunci hasil sinkronisasi yang dihasilkan kedua pengguna sehingga semakin sedikit 128-bit kunci identik yang dihasilkan.

Tabel 5.1 Parameter simulasi skema SKG SSE.

No	Parameter	Keterangan
1	Jumlah data n	4000
2	Distribusi data x_α dan x_b	Rician dengan s=4
3	Distribusi data $x_{\alpha 1}$ dan x_{b1}	Rayleigh dengan varian=4
4	Koefisien korelasi $y^{\alpha\beta}$ dan $y^{\beta\alpha}$	0,7
5	Koefisien korelasi $y^{\alpha 1\beta 1}$ dan $y^{\beta 1\alpha 1}$	0,6
6	Koefisien korelasi $y^{\beta\alpha}$ dan $y^{\alpha e}$	0,02
7	Koefisien korelasi $y^{\alpha\beta}$ dan $y^{\beta e'}$	0,01
8	Koefisien korelasi $y^{\beta 1\alpha 1}$ dan $y^{\alpha 1e1}$	0,01
9	Koefisien korelasi $y^{\alpha 1\beta 1}$ dan $y^{\beta 1e1'}$	0,02
10	Pembagi standar deviasi a	$0,6 - 0,85$
11	C	2

Tabel 5.2 Jumlah 128-bit kunci hasil sinkronisasi dari skema SKG SSE hasil simulasi data berdistribusi Rician dan Rayleigh.

a	Jumlah 128-bit kunci yang identik dari distribusi data	
	Rician	Rayleigh
0,6	4	2
0,65	3	2
0,7	3	-
0,75	3	-
0,8	2	-
0,85	1	-

Dengan cara yang sama kami membangkitkan dua bilangan acak dengan panjang $n = 4.000$, $x_e = [x_e(1), x_e(2), ..., x_e(n)]^T$ yang berkorelasi dengan x_α berdistribusi Rician dan $x_{e'} = [x_{e'}(1), x_{e'}(2), ..., x_{e'}(n)]^T$ yang berkorelasi dengan x_β juga berdistribusi Rician. Estimasi parameter kanal yang diperoleh adalah $y^{\alpha e}$ dan $y^{\beta e'}$. Dua bilangan acak berikutnya dengan panjang n 4000, $x_{e1} = [x_{e1}(1), x_{e1}(2), ..., x_{e1}(n)]^T$ yang berkorelasi dengan $x_{\alpha 1}$ berdistribusi Rayleigh dan $x_{e1'} = [x_{e1'}(1), x_{e1'}(2), ..., x_{e1'}(n)]^T$ yang berkorelasi dengan $x_{\beta 1}$ berdistribusi Rician. Estimasi parameter kanal yang diperoleh adalah $y^{\alpha 1 e1}$ dan $y^{\beta 1 e1'}$. 128-bit kunci yang dihasilkan oleh $y^{\alpha\beta}$ dan $y^{\beta\alpha}$ dinyatakan dengan Ka_s sedangkan 128-bit kunci yang dihasilkan $y^{\alpha e}$ dan $y^{\beta e'}$. dinyatakan dengan Ke_s dan Kb_s. 128-bit kunci yang dihasilkan oleh $y^{\alpha 1\beta 1}$ dan $y^{\beta 1\alpha 1}$ dinyatakan dengan $Ka1_s$ sedangkan 128-bit kunci yang dihasilkan $y^{\alpha 1 e1}$ dan $y^{\beta 1 e1'}$. dinyatakan dengan $Ke1_s$ dan $Kb1_s$. Pada pengujian kemanan, diasumsikan $y^{\alpha\beta}$ dan $y^{\beta\alpha}$ serta $y^{\alpha 1\beta 1}$ dan $y^{\beta 1\alpha 1}$ adalah data dari pengguna yang sah yang memiliki koefisien korelasi tinggi, sedangkan $y^{\alpha e}$ dan $y^{\beta e'}$ adalah data dari penyadap yang memiliki koefisien korelasi sangat rendah. Nilai KDR didapat dari jumlah perbedaan bit antara Ka_s, Ke_s; Ka_s, Kb_s; $Ka1_s, Ke1_s$; serta $Ka1_s$, $Kb1_s$. Untuk memenuhi persyaratan keamanan, diharapkan tidak ada 128-bit kunci yang dihasilkan penyadap dan ditunjukkan dengan nilai KDR diatas 0. Tabel 5.3 hingga 5.9 menunjukkan nilai KDR yang dihasilkan antara penyadap dan pengguna yang sah. Hasil pengujian yang dilakukan menunjukkan bahwa nilai KDR yang diperoleh berkisar antara 0,0469 hingga 0,2969 sehingga bisa dikatakan bahwa Skema SKG SSE hasil simulasi telah memenuhi persyaratan keamanan karena semua KDR yang dihasilkan bernilai diatas 0. Tidak ada 128-bit kunci identik yang berhasil dibangkitkan oleh penyadap.

Tabel 5.3 KDR antara Ka_s, Ke_s dan Kb_s untuk $a = 0,6$ dari skema SKG SSE hasil simulasi data berdistribusi Rician.

KDR untuk nilai $a = 0,6$				
Ka_s	$Ke_s - 1$	$Ke_s - 2$	$Kb_s - 1$	$Kb_s - 2$
$Ka_s - 1$	0,0703	0,0547	0,0781	0,0703
$Ka_s - 2$	0,0625	0,0469	0,0703	0,0625
$Ka_s - 3$	0,0547	0,0547	0,0781	0,0703
$Ka_s - 4$	0,0781	0,0625	0,0703	0,0781

Tabel 5.4 KDR antara Ka_s, Ke_s dan Kb_s untuk $a = 0,65$ dari skema SKG SSE hasil simulasi data berdistribusi Rician.

KDR untuk nilai $a = 0,65$				
Ka_s	$Ke_s - 1$	$Ke_s - 2$	$Kb_s - 1$	$Kb_s - 2$
$Ka_s - 1$	0,0781	0,0703	0,0938	0,0781
$Ka_s - 2$	0,0938	0,0859	0,1250	0,0938
$Ka_s - 3$	0,0859	0,0781	0,1172	0,0703

Tabel 5.5 KDR antara Ka_s, Ke_s dan Kb_s untuk $a = 0,7$ dari skema SKG SSE hasil simulasi data berdistribusi Rician.

KDR untuk nilai $a = 0,7$				
Ka_s	$Ke_s - 1$	$Ke_s - 2$	$Kb_s - 1$	$Kb_s - 2$
$Ka_s - 1$	0,1094	0,1328	0,1484	0,1016
$Ka_s - 2$	0,1328	0,1563	0,1719	0,1250
$Ka_s - 3$	0,1484	0,1250	0,1563	0,1250

Tabel 5.6 KDR antara Ka_s, Ke_s dan Kb_s untuk $a = 0,75$ dari skema SKG SSE hasil simulasi data berdistribusi Rician.

KDR untuk nilai $a = 0,75$			
Ka_s	$Ke_s - 1$	$Kb_s - 1$	$Kb_s - 2$
$Ka_s - 1$	0,1484	0,1641	0,1328
$Ka_s - 2$	0,1641	0,1953	0,1797
$Ka_s - 3$	0,1563	0,2031	0,1563

Tabel 5.7 KDR antara Ka_s, Ke_s dan Kb_s untuk $a = 0,8$ dan $a = 0,85$ dari skema SKG SSE hasil simulasi data berdistribusi Rician.

KDR untuk nilai $a = 0,8$ **dan** $a = 0,85$							
a	Ka_s	$Ke_s - 1$	$Kb - 1$	a	Ka_s	$Ke_s - 1$	$Kb_s - 1$
0,8	$Ka_s - 1$	0,2344	0,2500	0,85	$Ka_s - 1$	0,2969	0,2969
	$Ka_s - 2$	0,2734	0,2422		-		

Tabel 5.8 KDR antara $Ka1_s$, $Ke1_s$ dan $Kb1_s$ untuk $a = 0,6$ dari skema SKG SSE hasil simulasi data berdistribusi Rayleigh.

KDR untuk nilai $a = 0,6$			
$Ka1_s$	$Ke1_s - 1$	$Kb1_s - 1$	$Kb1_s - 2$
$Ka1_s - 1$	0,0234	0,0469	0,0031
$Ka1_s - 2$	0,0078	0,0313	0,0234

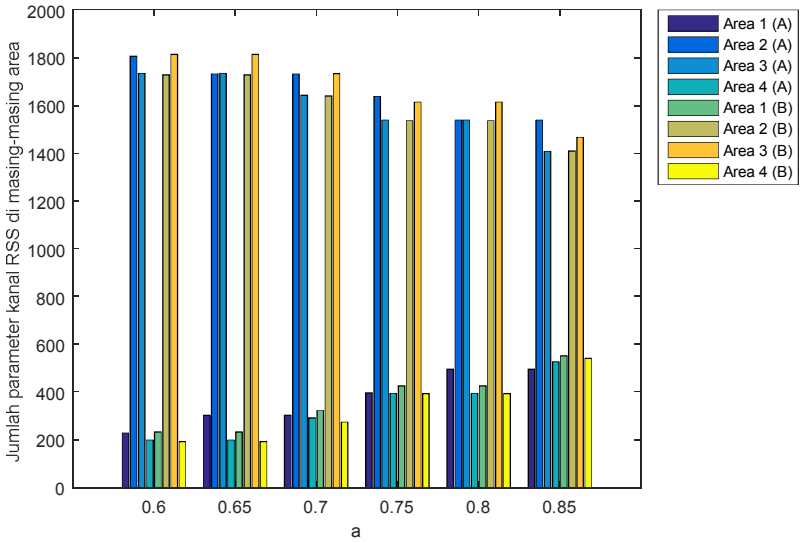
Tabel 5.9 KDR antara $Ka1_s$, $Ke1_s$ dan $Kb1_s$ untuk $a = 0,65$ dari skema SKG SSE hasil simulasi data berdistribusi Rayleigh.

KDR untuk nilai $a = 0,65$			
$Ka1_s$	$Ke1_s - 1$	$Kb1_s - 1$	$Kb1_s - 2$
$Ka1_s - 1$	0,0313	0,0469	0,0703
$Ka1_s - 2$	0,0313	0,0469	0,0703

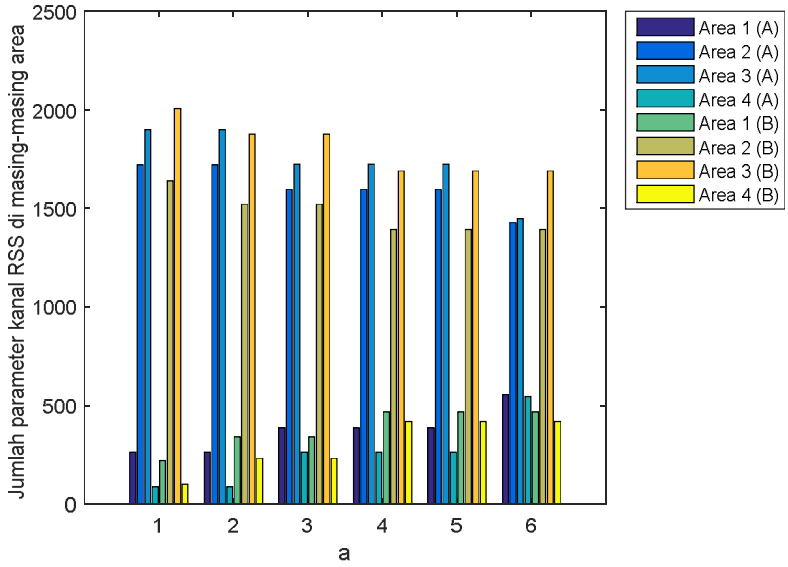
5.4 Evaluasi Performansi dari skema SKG SSE

Pada skema SKG ini kami mengolah parameter kanal RSS hasil pengukuran yang didapat dari skenario 5 dan 6. Detil implementasi dari skenario 5 dan 6 telah dijelaskan pada sub bab 4.4.1. Parameter kanal hasil pengukuran juga telah ditunjukkan pada sub bab 4.4.2. Metode SQ melakukan konversi multi bit dengan membagi parameter kanal RSS ke dalam beberapa area. Jumlah parameter kanal RSS di masing-masing area sangat dipengaruhi oleh pemilihan a sebagai parameter pembagi standar deviasi. Pada bagian ini pengguna Alice dan Bob akan dituliskan sebagai A dan B sedangkan penyadap Eve akan dituliskan sebagai E. Parameter kanal RSS antara A dan B disebut sebagai $A - B$, parameter kanal RSS yang didapat E dari A disebut sebagai $A - E$ sedangkan parameter kanal RSS yang didapat E dari B disebut sebagai $B - E$. Gambar 5.3 dan 5.4 menunjukkan parameter kanal RSS A dan B di masing-masing area di lingkungan dengan halangan dan tanpa halangan. Hasil pengujian yang dilakukan terhadap semua nilai a menunjukkan tingginya parameter kanal RSS yang berada di area 2 dan 3. Kondisi ini meningkatkan kemungkinan didapatkannya 3 bit sekuensial yaitu 111 dan dikonversi ke 1. Bit kunci hasil sinkronisasi yang dihasilkan didominasi oleh bit 1. Semakin tinggi nilai a maka semakin tinggi kemungkinan didapatkannya variasi bit 1 dan 0 dari bit kunci hasil sinkronisasi yang dihasilkan. Hal ini terjadi karena semakin meningkatnya jumlah parameter kanal RSS di area 1 dan 4 sehingga meningkatkan probabilitas didapatkannya 3 sekuensial bit yaitu 000 dan

dikonversi ke 0. Semakin tinggi variasi 1 dan 0 dari kunci yang dihasilkan maka semakin tinggi kemungkinan didapatkannya perbedaan bit kunci hasil sinkronisasi yang dihasilkan kedua pengguna.



Gambar 5.3 Jumlah parameter kanal RSS ($A - B$) di masing-masing area dengan skema SKG SSE (skenario 5).



Gambar 5.4 Jumlah parameter kanal RSS ($A - B$) di masing-masing area skema SKG SSE (skenario 6).

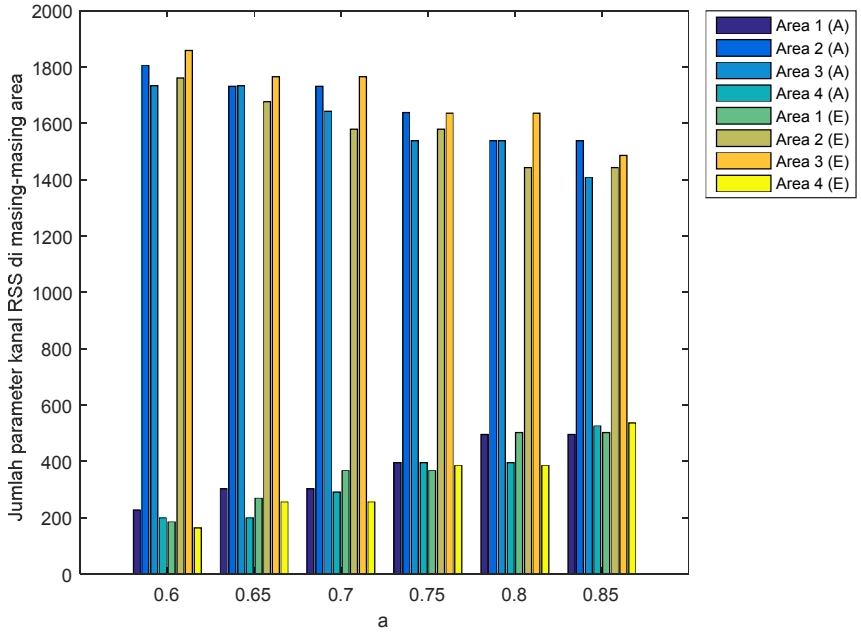
Tabel 5.10 menunjukkan jumlah kunci hasil sinkronisasi yang identik dengan panjang 128-bit, 192-bit and 256-bit yang berhasil dibangkitkan dari dua skenario. Bit kunci hasil sinkronisasi yang identik didapatkan jika KDR yang dihasilkan kedua pengguna yang sah adalah 0. Hasil pengujian di skenario 5 menunjukkan bahwa semakin tinggi nilai a maka semakin sedikit kunci hasil sinkronisasi identik yang dihasilkan. Jumlah kunci hasil sinkronisasi identik tertinggi didapat saat parameter $a = 0,6$ dan $a = 0,65$. Pada parameter ini, kebanyakan parameter kanal RSS berada di area 2 dan 3 sehingga kunci hasil sinkronisasi yang dihasilkan didominasi oleh bit 1. Variasi yang rendah dari bit yang dihasilkan meningkatkan probabilitas didapatkannya kunci hasil sinkronisasi yang identik. Hasil pengujian di skenario 6 menunjukkan bahwa kunci hasil sinkronisasi yang identik hanya didapatkan saat $a = 0,6$ dan $a = 0,65$. Semakin tinggi perbedaan jumlah parameter kanal di masing-masing area maka semakin tinggi pula variasi bit 1 dan 0 sehingga semakin sulit untuk mendapatkan kunci hasil sinkronisasi yang identik. Metode enkripsi yang digunakan untuk mengacak pesan adalah Advanced Encryption Standard (AES) dengan panjang kunci 128-bit, 192-bit, and 256-bit. Pada skema SKG ini, kami fokus pada 128-bit kunci karena skema ini menghasilkan lebih banyak kunci hasil sinkronisasi dengan panjang 128 bit. Semakin banyak kunci yang dihasilkan maka semakin tinggi nilai KGR yang diperoleh sehingga dapat meningkatkan performansi dari skema SKG yang dibangun.

Gambar 5.5 dan 5.6 menunjukkan jumlah parameter kanal RSS dari penyadap E yang didapat dari A ($A - E$) serta B ($B - E$) di masing-masing area pada skenario 5. Sedangkan Gambar 5.7 dan 5.8 menunjukkan jumlah parameter kanal RSS dari penyadap E yang didapat dari A ($A - E$) serta B ($B - E$) di masing-masing area pada skenario 6. Dari semua skenario terlihat bahwa jumlah RSS dari penyadap E yang didapat dari A kebanyakan berada di area 2 dan 3 untuk semua nilai a. Kondisi ini mengakibatkan semakin tingginya probabilitas untuk mendapatkan 3 sekuensial bit yaitu 111 and dikonversi ke bit 1. Jumlah parameter kanal RSS dari penyadap E yang didapat dari B juga kebanyakan berada di area 2 dan 3 untuk semua nilai a, namun terdapat perbedaan jumlah RSS yang signifikan dari area 2 dan 3. Hal inilah yang

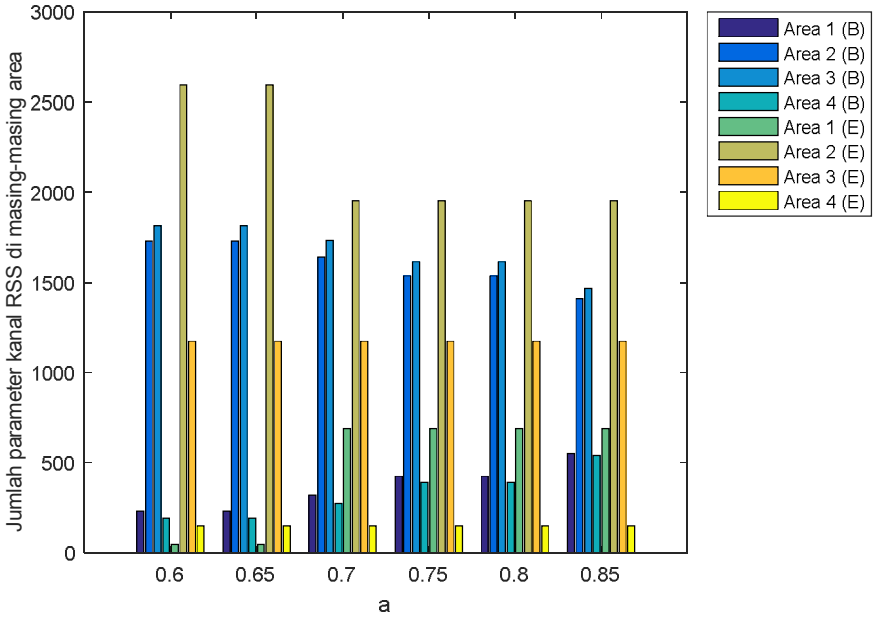
mengakibatkan semakin rendahnya probabilitas untuk mendapatkan 3 sekuensial bit yaitu 111.

Tabel 5.10 Jumlah kunci hasil sinkronisasi yang identik ($A - B$) dari skema SKG SSE.

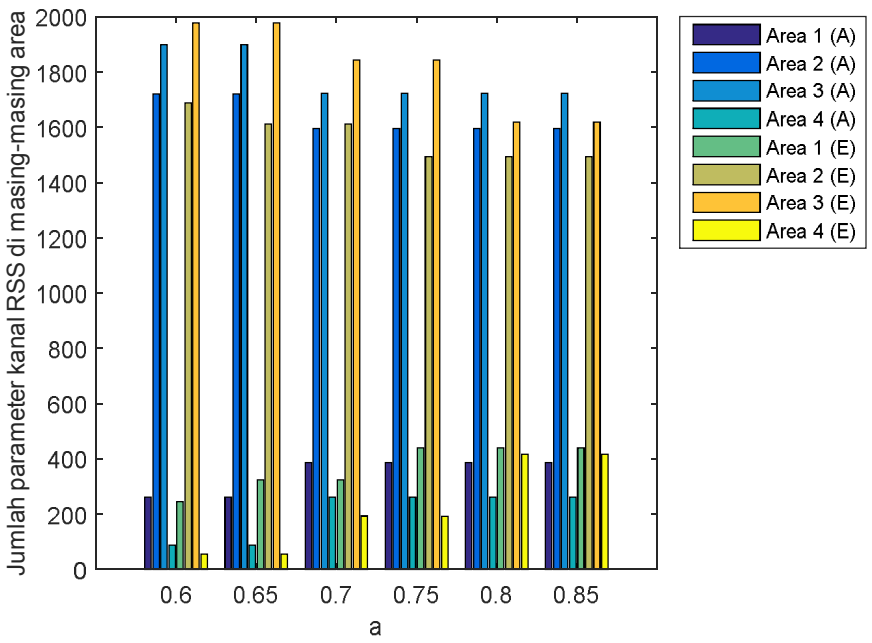
Jumlah bit kunci	*a*	**Jumlah kunci yang identik**	
		Skenario 5	**Skenario 6**
128	0,6	4	4
	0,65	4	1
	0,7	3	-
	0,75	2	-
	0,8	2	-
	0,85	1	-
192	0,6	2	3
	0,65	2	-
	0,7	2	-
	0,75	1	-
	0,8	1	-
	0,85	-	-
256	0,6	2	2
	0,65	2	-
	0,7	1	-
	0,75	1	-
	0,8	1	-
	0,85	-	-



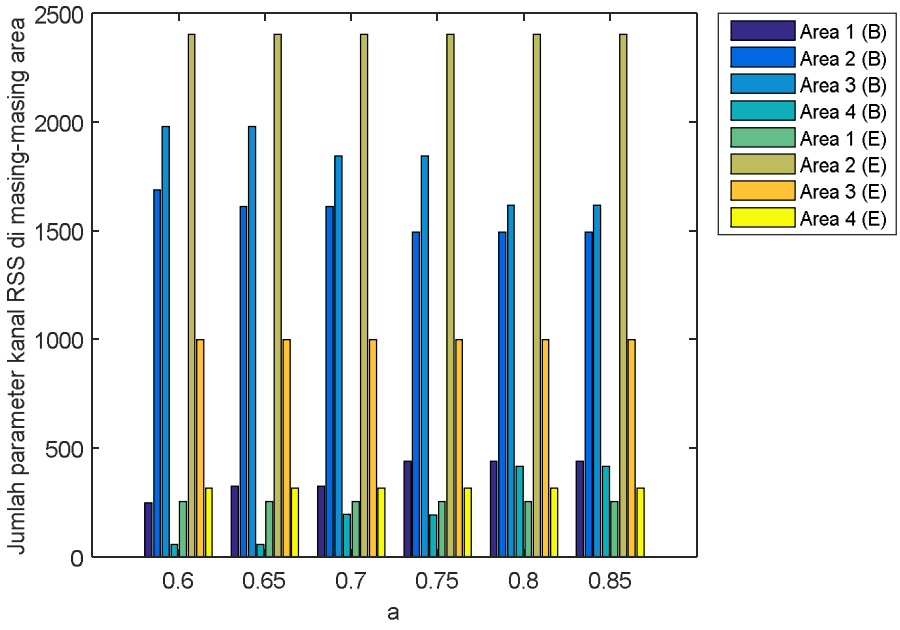
Gambar 5.5 Jumlah parameter kanal RSS ($A - E$) di masing-masing area skema SKG SSE (skenario 5).



Gambar 5.6 Jumlah parameter kanal RSS ($B - E$) di masing-masing area skema SKG SSE (skenario 5).



Gambar 5.7 Jumlah parameter kanal RSS ($A - E$) di masing-masing area skema SKG SSE (skenario 6).



Gambar 5.8 Jumlah parameter kanal RSS ($B - E$) di masing-masing area skema SKG SSE (skenario 6).

Pada skema SKG ini, penyadap diasumsikan mengetahui semua algoritma yang digunakan. Jumlah 128-bit kunci hasil sinkronisasi yang dibangkitkan oleh penyadap serta KDR antara penyadap dan pengguna yang sah ditunjukkan oleh Tabel 5.11 hingga 5.17. 128-bit kunci yang dihasilkan oleh pengguna yang sah dinyatakan dengan Ka ($A-B$) sedangkan 128-bit kunci yang dihasilkan penyadap dinyatakan dengan Ke ($A-E$) dan Kb ($B-E$). Nilai KDR didapat dari jumlah perbedaan bit antara Ka dan Ke serta Kb dan Ke. Untuk memenuhi persyaratan keamanan, diharapkan tidak ada 128-bit kunci yang dihasilkan penyadap dan ditunjukkan dengan nilai KDR diatas 0. Hasil pengujian dikedua skenario menunjukkan lebih sedikitnya jumlah kunci hasil sinkronisasi yang dihasilkan $B-E$ jika dibandingkan dengan $A-E$. Hal ini terjadi karena rendahnya probabilitas untuk mendapatkan 3 sekuensial bit yaitu 111 karena signifikannya perbedaan jumlah RSS yang berada di area 2 dan 3. Hasil pengujian di lingkungan skenario 5 juga menunjukkan bahwa semakin tinggi nilai a maka semakin tinggi ketidakcocokan kunci yang dihasilkan antara penyadap dan pengguna yang sah. Tingginya ketidakcocokan kunci ini diakibatkan oleh semakin tingginya variasi 0 dan 1 yang dihasilkan sehingga meningkatkan perbedaan bit yang dihasilkan. Dari hasil pengujian di skenario 6 tidak terlalu terlihat perbedaan ketidakcocokan kunci yang dihasilkan antara nilai $a = 0.6$ dan $a = 0.65$. Hal ini terjadi karena jumlah RSS yang hampir sama di masing-masing area untuk kedua nilai parameter a tersebut. Secara keseluruhan dapat dikatakan bahwa skema SKG SSE yang dibangun telah memenuhi persyaratan keamanan karena tidak ada kunci hasil sinkronisasi identik yang berhasil dibangkitkan oleh penyadap.

Tabel 5.11 Jumlah kunci hasil sinkronisasi ($A-E$ dan $B-E$) dari skema SKG SSE.

Skenario	**Jumlah kunci Ke untuk nilai a**						**Jumlah kunci Kb untuk nilai a**					
	0,6	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**	**0,6**	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**
5	2	2	2	2	1	1	1	1	1	1	1	1
6	3	1	-	-	-	-	3	1	-	-	-	-

Tabel 5.12. KDR antara penyadap dan pengguna yang sah untuk $a = 0,6$ dan $a = 0,65$ dari skema SKG SSE (skenario 5).

KDR untuk masing-masing nilai a									
a	Ka	$Ke-1$	$Ke-2$	$Kb-1$	a	Ka	$Ke-1$	$Ke-2$	$Kb-1$
0,6	$Ka-1$	0,0391	0,0469	0,0234	0,65	$Ka-1$	0,0547	0,0703	0,0234
	$Ka-2$	0,0703	0,0781	0,0547		$Ka-2$	0,0938	0,1094	0,0625
	$Ka-3$	0,0703	0,0781	0,0547		$Ka-3$	0,0703	0,1016	0,0547
	$Ka-4$	0,0703	0,0781	0,0547		$Ka-4$	0,0859	0,1016	0,0703

Tabel 5.13. KDR antara penyadap dan pengguna yang sah untuk $a = 0,7$ dan $a = 0,75$ dari skema SKG SSE (skenario 5).

KDR untuk masing-masing nilai a								
a	Ka	$Ke-1$	$Ke-2$	$Kb-1$	a	Ka	$Ke-1$	$Kb-1$
0,7	$Ka-1$	0,1172	0,1172	0,2891	0,75	$Ka-1$	0,1406	0,2969
	$Ka-2$	0,1406	0,1406	0,3125		$Ka-2$	0,1875	0,2969
	$Ka-3$	0,1484	0,1328	0,2734		-	-	-

Tabel 5.14. KDR antara penyadap dan pengguna yang sah untuk $a = 0,8$ dan $a = 0,85$ dari skema SKG SSE (skenario 5).

KDR untuk masing-masing nilai a							
a	Ka	$Ke-1$	$Kb-1$	a	Ka	$Ke-1$	$Kb-1$
0,8	$Ka-1$	0,2109	0,3047	0,85	$Ka-1$	0,2969	0,4063
	$Ka-2$	0,2344	0,3281		-	-	-

Tabel 5.15. KDR antara penyadap dan pengguna yang sah untuk $a = 0,6$ dari skema SKG SSE (skenario 6).

KDR untuk nilai $a = 0,6$				
Ka	$Ke-1$	$Ke-2$	$Ke-3$	$Kb-1$
$Ka-1$	0,0625	0,0703	0,0547	0,0547
$Ka-2$	0,0391	0,0469	0,0313	0,0313
$Ka-3$	0,0547	0,0625	0,0469	0,0469
$Ka-4$	0,0469	0,0547	0,0391	0,0391

Tabel 5.16. KDR antara penyadap dan pengguna yang sah untuk $a = 0,65$ dari skema SKG SSE (skenario 6).

KDR untuk nilai $a = 0,65$				
Ka	$Ke-1$	$Ke-2$	$Ke-3$	$Kb-1$
$Ka-1$	0,0547	0,0781	0,0547	0,0391
$Ka-2$	-	-	-	-
$Ka-3$	-	-	-	-
$Ka-4$	-	-	-	-

Waktu komputasi didapatkan dengan menghitung waktu yang dibutuhkan pada tahap SQ dan *privacy amplification*. Pada tahap SQ terdapat 2 waktu yang dihitung yaitu waktu komputasi dari konversi multi bit dan pembagian bit menjadi beberapa blok, serta waktu komunikasi dari pertukaran indeks blok yang terbuang untuk memastikan bahwa kunci hasil sinkronisasi yang dihasilkan adalah kunci yang identik sehingga dapat menghilangkan tahap rekonsiliasi informasi. Pada tahap *privacy*

amplification juga terdapat dua waktu yang akan dihitung yaitu waktu komputasi dari peningkatan keacakan dan mekanisme verifikasi serta waktu komunikasi dari pertukaran *hash* antara dua pengguna yang sah. Pengujian *overhead* komunikasi dilakukan dengan menghitung ukuran *file* yang dikirim untuk sinkronisasi antara dua pengguna yang sah. Sinkronisasi dilakukan saat tahap SQ dan *privacy amplification*. Tabel 5.17 hingga 5.20 menunjukkan waktu komputasi dan komunikasi yang dibutuhkan untuk mendapatkan 128-bit kunci untuk masing-masing nilai a di dua skenario sedangkan pengujian *overhead* komunikasi ditunjukkan pada Tabel 5.21 dan 5.22. Hasil pengujian yang dilakukan menunjukkan tidak signifikannya perbedaan waktu komputasi untuk masing-masing nilai a di kedua skenario, baik di tahap SQ maupun *privacy amplification*. Perbedaan waktu komputasi justru terjadi pada tahap SQ dan *privacy amplification*. Hal ini terjadi karena data yang diproses pada tahap SQ untuk masing-masing nilai a adalah parameter kanal RSS yang sama. Sedangkan data yang diproses pada tahap *privacy amplification* adalah sisa data dari SQ. Pengujian waktu komunikasi juga menunjukkan tidak signifikannya perbedaan waktu untuk masing-masing nilai a di tahap SQ dan privacy amplification. Hal ini terjadi karena tidak ada perbedaan yang signifikan dari *overhead* komunikasi yang dihasilkan.

Tabel 5.17. Pengujian waktu komputasi untuk masing-masing nilai a pada tahap SQ.

Skenario	**Waktu komputasi (s)**					
	0,6	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**
5	24,54	24,35	24,41	24,45	24,42	24,51
6	24,30	24,32	-	-	-	-

Tabel 5.18. Pengujian waktu komunikasi untuk masing-masing nilai *a* pada tahap SQ.

Skenario	**Waktu komunikasi (s)**					
	0,6	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**
5	4,23	4,33	4,41	4,40	4,39	4,48
6	4,32	4,33	-	-	-	-

Tabel 5.19. Pengujian waktu komputasi untuk masing-masing nilai *a* pada tahap *privacy amplification*.

Skenario	**Waktu komputasi (s)**					
	0,6	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**
5	15,05	15,19	15,28	15,12	15,23	15,17
6	15,42	15,42	-	-	-	-

Tabel 5.20. Pengujian waktu komunikasi untuk masing-masing nilai *a* pada tahap *privacy amplification*.

Skenario	**Waktu komunikasi (s)**					
	0,6	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**
5	4,22	4,25	4,31	4,27	4,33	4,35
6	4,23	4,24	-	-	-	-

Tabel 5.21. Pengujian *overhead* komunikasi untuk masing-masing nilai a pada tahap SQ.

Skenario	***Overhead* komunikasi (byte)**					
	0,6	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**
5	17962	17904	18381	18852	18791	19460
6	16995	17361	-	-	-	-

Tabel 5.22. Pengujian *overhead* komunikasi untuk masing-masing nilai a pada tahap *privacy amplification*.

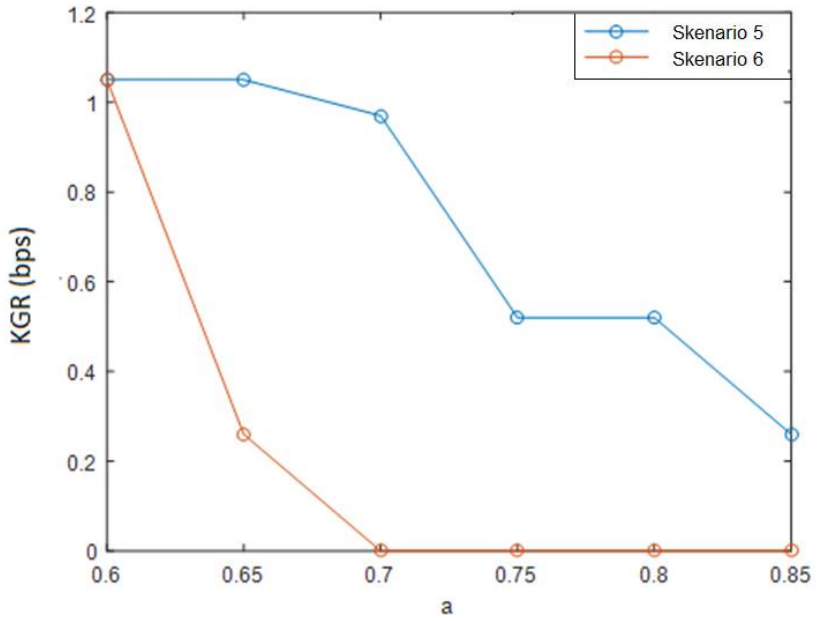
Skenario	***Overhead* komunikasi (byte)**					
	0,6	**0,65**	**0,7**	**0,75**	**0,8**	**0,85**
5	11276	11276	11270	11270	11270	11270
6	11276	11276	-	-	-	-

Pada skema ini parameter KGR didapat dengan menghitung banyaknya bit kunci yang identik selama durasi komunikasi skema SKG SSE. Kami melakukan pengujian dengan melakukan variasi dari parameter a antara 0,6 hingga 0,85. Pemilihan variasi nilai tersebut didasarkan pada upaya untuk mendapatkan 128-bit kunci yang sama antara kedua pengguna yang sah dan memastikan bahwa tidak ada 128-bit kunci penyadap yang sama. Gambar 5.9 menunjukkan bahwa semakin tinggi nilai a maka semakin rendah KGR yang dihasilkan karena semakin sedikitnya jumlah 128-bit kunci yang identik. Hal ini terjadi karena meningkatnya nilai a juga akan meningkatkan variasi 0 dan 1 dari kunci yang dihasilkan sehingga memperkecil kemungkinan didapatkannya kunci yang identik. Hasil pengujian yang dilakukan di skenario 5 menunjukkan bahwa KGR tertinggi didapat saat $a = 0,6$ dan $a = 0,65$ yaitu 1,05 bps bps sedangkan KGR terendah didapat saat $a = 0,85$ yaitu 0,26 bps. Nilai yang didapat

menunjukkan bahwa waktu yang dibutuhkan untuk mendapatkan 128-bit kunci berkisar antara 2,03 menit hingga 8,21 menit. Sedangkan hasil pengujian yang dilakukan di skenario 6 menunjukkan bahwa KGR tertinggi didapat saat $a = 0,6$ yaitu 1,05 bps sedangkan KGR terendah didapat saat $a = 0,65$ yaitu 0,26 bps. Nilai yang didapat menunjukkan bahwa waktu yang dibutuhkan untuk mendapatkan 128-bit kunci berkisar antara 2,03 menit hingga 8,21 menit. Secara keseluruhan dapat dikatakan bahwa skema SKG SSE mampu menghasilkan kunci dibawah 1 jam sehingga telah memenuhi persyaratan waktu maksimal refresh key yang diusulkan oleh (Moore, 2001). Pada paper ini untuk meningkatkan keamanan kami melakukan *refresh* kunci setiap 15 menit.

Pengujian keacakan dilakukan untuk memastikan bahwa 128-bit kunci hasil sinkronisasi telah memenuhi persyaratan keacakan. Pada penelitian ini, kami menggunakan bit kunci yang dihasilkan dengan pemilihan $a = 0,6$. Nilai a ini dipilih karena lebih banyaknya 128-bit kunci yang berhasil dibangkitkan di kedua skenario. Selain itu syarat keamanan juga berhasil dipenuhi karena tidak ada 128-bit kunci yang dihasilkan penyadap sama dengan 128-bit kunci yang dihasilkan pengguna yang sah. Terdapat 6 tes keacakan yang dilakukan yaitu *approximate entropy*, *frequency (monobit) test, Frequency test within a block, runs test, Longest-Run-of-Ones in a Block test,* serta *Cumulative sums test*. Masing-masing tes akan menghasilkan nilai P yang merupakan nilai probabilitas keacakan dari 128-bit kunci ($0 \leq P \leq 1$). Semakin mendekati 1 maka semakin acak 128-bit kunci yang dihasilkan. Agar memenuhi persyaratan keacakan maka nilai P minimal dari 128-bit kunci yang dihasilkan adalah 0,01. Detil kegunaan dari masing-masing tes dijelaskan sebagai berikut**.** *Frequency (monobit) test* digunakan untuk mengetahui rasio 0 dan 1 dari 128-bit kunci. *Frequency test within a block* bertujuan untuk mengetahui rasio 1 dari masing masing blok dalam 128-bit kunci. Penentuan apakah fluktuasi 0 atau 1 dalam 128-bit kunci terlalu cepat atau lambat dapat diketahui dengan *runs test*, sedangkan penentuan apakah fluktuasi 0 atau 1 dari masing-masing blok dalam 128-bit kunci terlalu cepat atau lambat dapat diketahui dengan *Longest-Run-of-Ones in a Block test*. *Approximate entropy test*

digunakan untuk menentukan frekuensi dari semua kemungkinan interseksi bit dari masing-masing blok dalam 128 bit kunci. *Cumulative sums test* digunakan untuk menentukan apakah jumlah akumulatif dari rangkaian pecahan 128-bit kunci yang diuji terlalu besar atau terlalu kecil terhadap jumlah akumulatif dari rangkaian yang acak.



Gambar 5.9 KGR dari berbagai variasi nilai a

Tabel 5.23 dan 5.24 menunjukkan hasil pengujian NIST di skenario 5 dan 6. Pada kedua skenario terlihat bahwa semua kunci yang dihasilkan telah memenuhi persyaratan keacakan untuk 6 tes karena nilai P yang dihasilkan telah melebihi 0,01. Prioritas dari kunci yang akan dipilih sebagai *secret key* pada skema SKG SSE adalah $Ka-4$, $Ka-1$, $Ka-2$, serta $Ka-3$. Pemilihan prioritas ini didasarkan pada hasil tes *Approximate entropy*. Jika $Ka-4$ gagal digunakan sebagai *secret key* pada fase verifikasi maka $Ka-1$ yang akan digunakan sebagai *secret key* demikian seterusnya. Nilai P tertinggi dari tes *Approximate entropy* saat skenario 5 adalah 0,9484 dan 0,9403 saat skenario 6. Hal ini menunjukkan bahwa $Ka-4$ yang didapat saat skenario 6 memiliki keteraturan yang lebih tinggi jika dibandingkan dengaan $Ka-4$ yang didapat saat skenario 5.

Tabel 5.23 Tes NIST dari skema SKG SSE pada skenario 5

Tes	**Nilai p di skenario 5**			
	$Ka-1$	$Ka-2$	$Ka-3$	$Ka-4$
Approximate entropy	0,4540	0,3491	0,0863	0,9484
Frequency (Monobit)	0,4795	1,0000	0,2159	1,0000
Frequency Test within a Block	0,1532	0,0239	0,3540	0,2202
Runs	0,8941	0,5959	0,2260	0,4795
Longest-Run-of-Ones in a Block	0,4098	0,9404	0,7529	0,4203
Cumulative Sums (forward)	0,5748	0,6547	0,3697	0,7375
Cumulative Sums (backward)	0,1542	0,6547	0,3697	0,7375

Tabel 5.24 Tes NIST dari skema SKG SSE pada skenario 6

Tes	**Nilai p di skenario 6**			
	$Ka-1$	$Ka-2$	$Ka-3$	$Ka-4$
Approximate entropy	0,2941	0,4552	0,2806	0,9403
Frequency (Monobit)	0,3768	0,8597	1,0000	1,0000
Frequency Test within a Block	0,9170	0,9326	0,4530	0,8666
Runs	0,1356	0,2900	0,5959	0,4795
Longest-Run-of-Ones in a Block	0,1806	0,0359	0,8893	0,5788
Cumulative Sums (forward)	0,6548	0,8188	0,9842	0,3697
Cumulative Sums (backward)	0,6548	0,9493	0,9842	0,3697

5.5 Perbandingan Performansi antara Skema SKG SSE dengan Skema yang Eksisting

Terdapat 2 parameter performansi yaitu waktu komputasi serta *overhead* komunikasi yang digunakan untuk membandingkan skema SKG SSE dengan skema eksisting yang juga diimplementasikan pada perangkat IoT dengan keterbatasan daya dan komputasi. Pemilihan parameter tersebut didasarkan pada pertimbangan untuk mendapatkan skema SKG yang efisien dari segi waktu komputasi serta *overhead* komunikasi yang dihasilkan. Semakin sedikit waktu komputasi yang dibutuhkan serta *overhead* komunikasi yang dikirim maka semakin efisien skema SKG yang dibangun. Terdapat 5 skema eksisting yang digunakan sebagai pembanding yaitu skema 10 hingga 14. Skema 10 (Zhang dkk, 2016) menggunakan 4 tahap dimana parameter kanal RSS akan dikuantisasi dengan mengunakan sistem *cumulative distribution function* (CDF). Skema 11 (Yuliana dkk, 2019b) menggunakan 5 tahap dimana parameter kanal RSS akan dibagi menjadi beberapa blok yang masing-masing berisi 50 data RSS. Masing-masing blok di pra proses dengan menggunakan metode Kalman dan hasil yang didapat akan dikonversi menjadi multi bit dengan metode kuantisasi yang diusulkan oleh (Ambekar dkk, 2012). Skema 12 (Guillaume dkk, 2015) menggunakan 5 tahap dalam membangun skema SKG. Parameter kanal RSS akan di pra proses dengan menggunakan Regresi Polinomial orde 3. Hasil dari pra proses akan dibagi menjadi beberapa blok yang masing-masing berisi 250 bit. Masing-masing blok juga akan dikonversi menjadi multi-bit dengan metode kuantisasi yang diusulkan oleh (Ambekar dkk, 2012). Skema 13 (Margelis dkk, 2015) bekerja dengan melakukan pra proses terhadap parameter kanal RSS dengan menggunakan metode *discrete cosine transform* (DCT). Hasil dari pra proses akan dikuantisasi dengan menggunakan beberapa parameter yang meliputi rata-rata dan standar deviasi. Skema 14 (Zenger dkk, 2018) menggunakan 4 tahap dimana masing-masing parameter kanal RSS akan dibagi menjadi beberapa blok yang masing-masing berisi 128 bit. Masing-masing blok akan dikonversi ke multi bit dengan menggunakan metode kuantisasi yang diusulkan oleh (Premnath dkk, 2013). Skema SKG yang eksisting masih membutuhkan tahap

rekonsiliasi informasi untuk melakukan koreksi terhadap perbedaan bit yang dihasilkan kedua pengguna. Pada penelitian ini metode rekonsiliasi informasi yang digunakan adalah BCH (255,87) sedangkan *privacy amplification* menggunakan metode Universal Hash dan SHA-1.

Pengujian waktu komputasi di kedua skenario dibagi menjadi 2 bagian yaitu bagian A dan B. Pada pengujian skema SKG SSE bagian A terdiri dari tahap SQ sedangkan bagian B terdiri dari *privacy amplification*. Pada pengujian skema yang eksisting ini bagian A terdiri dari metode pra proses hingga rekonsiliasi informasi sedangkan bagian B juga terdiri dari *privacy amplification*. Masing-masing bagian dibagi menjadi 2 yaitu waktu komputasi dan komunikasi. Tabel 5.25 dan 5.26 menunjukkan perbandingan waktu komputasi dan komunikasi antara skema SKG SSE dengan skema yang eksisting. Hasil pengujian yang dilakukan menunjukkan bahwa skema SKG SSE mampu mengurangi waktu komputasi dari bagian A hingga menjadi sebesar 3,9% (skenario 5) dan 3,8% (skenario 6) skema yang eksisting. Penurunan waktu komunikasi menjadi sebesar 64% (skenario 5) dan 65% (skenario 6) skema yang eksisting. Hasil pengujian dari bagian B menunjukkan bahwa skema SKG SSE mampu mengurangi waktu komputasi menjadi sebesar 38% (skenario 5) dan 40% (skenario 6) skema yang esksisting. Tidak ada perbedaan waktu komunikasi yang signifikan antara skema SKG SSE dengan skema yang eksisting karena *overhead* komunikasi yang dihasilkan hampir sama. Secara keseluruhan terlihat bahwa waktu komputasi dan komunikasi dari skema SKG SSE lebih rendah dari skema SKG yang eksisting. Hal ini terjadi karena pada bagian A, konversi multi bit dari skema SKG SSE didapatkan langsung dari parameter kanal RSS hasil pengukuran tanpa melalui tahap pra proses. Lebih lanjut, tidak ada pembagian blok pada pengolahan parameter kanal RSS sehingga dapat mengurangi waktu komputasi jika dibandingkan dengan skema yang eksisting. Tingginya waktu komputasi dari skema SKG yang eksisting diakibatkan oleh adanya tahap rekonsiliasi informasi. Semakin banyak data yang diolah maka semakin tinggi waktu komputasi, komunikasi serta *overhead* komunikasi yang dibutuhkan.

Tabel 5.25 Perbandingan waktu komputasi dan komunikasi antara skema SKG SSE dengan skema yang eksisting (senario 5)

Skema SKG	Skenario 5			
	Bagian A		Bagian B (s)	
	Waktu komputasi (detik)	Waktu komunikasi (detik)	Waktu komputasi (detik)	Waktu komunikasi (detik)
SSE	24,54	4,23	15,05	4,22
Skema 10	506,03	6,44	28,60	4,23
Skema 11	622,63	6,50	31,79	4,51
Skema 12	496,59	6,35	27,49	4,33
Skema 13	632,43	6,56	39,20	4,97
Skema 14	500,95	6,32	25,33	4,43

Tabel 5.26 Perbandingan waktu komputasi dan komunikasi antara skema SKG SSE dengan skema yang eksisting (skenario 6)

Skema SKG	Skenario 6			
	Bagian A		Bagian B (s)	
	Waktu komputasi (detik)	Waktu komunikasi (detik)	Waktu komputasi (detik)	Waktu komunikasi (detik)
SSE	24.30	4.32	15.42	4.23
Skema 10	509.31	6.55	31.17	4.32
Skema 11	623.25	6.45	29.78	4.30
Skema 12	490.38	6.44	24.79	4.47
Skema 13	633.82	6.45	38.12	4.55
Skema 14	498.18	6.44	26.14	4.33

Tabel 5.27 menunjukkan perbandingan dari *overhead* komunikasi antara skema SKG SSE dengan skema eksisting. *Overhead* komunikasi dihitung dari ukuran *file* yang dikirim untuk sinkronisasi pengguna yang sah. Pada skema SKG SSE, sinkronisasi data dilakukan setelah tahap SQ dan privacy amplification, sedangkan pada skema yang eksisting terjadi setelah tahap rekonsiliasi informasi dan *privacy amplification.* Hasil pengujian yang dilakukan menunjukkan bahwa skema SKG SSE dapat mengurangi *overhead* komunikasi dari bagian A menjadi sebesar 36% (skenario 5) dan 34% (skenario 6) skema yang eksisting. Tidak ada perbedaan *overhead* komunikasi yang signifikan dari bagian B antara skema SKG SSE dengan skema yang eksisting karena *overhead* komunikasi yang dihasilkan hampir sama. Hal ini terjadi karena sinkronisasi setelah tahap SQ hanya dilakukan pada indeks blok data yang terbuang sedangkan sinkronisasi setelah tahap rekonsiliasi informasi dilakukan pada bit *parity* sehingga meningkatkan ukuran dari *overhead* komunikasi. Secara keseluruhan dapat dikatakan bahwa skema SKG SSE mampu mengurangi waktu komputasi, komunikasi serta *overhead* komunikasi jika dibandingkan dengan skema yang eksisting sehingga sesuai jika diimplementasikan pada perangkat IoT dengan keterbatasan sumber daya.

5.6 Matrik Perbandingan Parameter Performansi Hasil Simulasi dan Eksperimen antara Skema SKG SSE dengan Skema yang Eksisting

Pada bagian ini akan dibuat matrik perbandingan parameter performansi hasil simulasi dan eksperimen antara skema SKG SSE dengan skema yang eksisting. Parameter performansi yang dibandingkan meliputi jumlah 128-bit kunci identik yang dihasilkan, KGR, kompleksitas dan durasi waktu. Jumlah 128-bit kunci identik yang dihasilkan skema SKG SSE didapat setelah tahap sinkronisasi pada $a = 0,6$, sedangkan pada skema yang eksisting kunci tersebut didapatkan setelah tahap rekonsiliasi informasi. Parameter KGR digunakan untuk mengetahui banyaknya bit yang dihasilkan dalam satu tahapan skema SKG, sedangkan durasi waktu digunakan untuk mengetahui lamanya waktu yang dibutuhkan untuk menyelesaikan tahapan skema SKG. Semakin

sedikit durasi waktu yang dibutuhkan maka semakin sesuai skema tersebut untuk diimplementasikan pada perangkat dengan keterbatasan sumber daya. Kompleksitas digunakan untuk mengetahui seberapa jauh keefektifan sebuah algoritma dalam meminimumkan waktu dan ruang, dimana waktu dan ruang suatu algoritma ini bergantung pada ukuran masukan (n), yang menyatakan jumlah data yang diproses.

Tabel 5.27 Perbandingan *overhead* komunikasi antara skema SKG SSE dengan skema yang eksisting

Skema SKG	**Skenario 5**		**Skenario 6**	
	***Overhead* komunikasi dari bagian A (byte)**	***Overhead* komunikasi dari bagian B(Byte)**	***Overhead* komunikasi dari bagian A (byte)**	***Overhead* komunikasi dari bagian B(byte)**
SSE	17,962	11,276	16,995	11,276
Skema 10	49,339	11,403	50,133	11,908
Skema 11	49,431	11,276	49,608	11,276
Skema 12	47,289	11,546	47,033	12,100
Skema 13	49,127	11,932	48,582	11,624
Skema 14	48,513	12,005	48,680	11,707

Table 5.29 menunjukkan perbandingan kompleksitas dari skema SKG SSE serta skema yang eksisting. Kami melakukan pengujian kompleksitas di tiap tahapan skema SKG. Skema usulan kami menggunakan 3 tahap yang meliputi channel probing, kuantisasi, dan *privacy amplification*. Skema yang eksisting menggunakan 5 tahap dengan menambahkan tahap pra proses dan rekonsiliasi informasi. Analisa kompleksitas hanya dilakukan pada 4 tahap terakhir karena 4 tahap tersebut kompleksitasnya tergantung dari algoritma yang dibuat. Secara keseluruhan terlihat bahwa skema usulan kami memiliki jumlah tahap yang lebih sedikit dengan kompleksitas yang sama di tahap privacy amplification. Berkurangnya tahap pra proses

dan rekonsiliasi informasi mengurangi durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG secara signifikan. Hal ini terjadi karena pada tahap rekonsiliasi informasi terdapat mekanisme pembangkitan parity yang akan semakin meningkat jika data yang harus dikoreksi semakin banyak.

Tabel 5.29 Perbandingan kompleksitas skema SKG SSE dengan skema yang eksisting

Skema	**Kompleksitas masing-masing tahapan skema SKG**					
	Pra proses		**Kuantisasi**	**Rekonsiliasi informasi**	**Privacy Amplification**	
	Pra proses 1	**Pra proses 2**			**Universal hash**	**SHA-1**
Skema SKG SSE	----	----	$O(pq)$	----	$O(p^2)$	$O(p)$
Skema 10	----	----	$O(n)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 11	$O(pq)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 12	$O(pq)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 13	$O(n^2)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema 14	----	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$

Tabel 5.30 menunjukkan matrik perbandingan parameter performansi skema SKG SSE dengan skema yang eksisting. Dari hasil pengujian terlihat bahwa skema yang eksisting menghasilkan 128-bit kunci yang lebih banyak jika dibandingkan dengan skema SKG SSE. Kondisi ini juga berpengaruh pada KGR yang dihasilkan skema eksisting. Semakin banyak kunci yang dihasilkan maka semakin tinggi KGR yang dihasilkan. Namun peningkatan KGR tersebut juga diikuti oleh peningkatan durasi waktu yang dibutuhkan untuk menyelesaikan satu kali tahapan skema SKG di semua skenario. Skema SKG SSE menghasilkan penurunan durasi waktu hingga 0,10

(simulasi) dan 0,43 (eksperimen) dari skema yang eksisting sehingga lebih sesuai jika diimplementasikan pada perangkat dengan keterbatasan sumber daya.

Tabel 5.31 menunjukkan matrik perbandingan parameter performansi antara skema usulan 1 hingga 4 dan skema SKG SSE. Tujuan dari pembuatan matrik ini adalah untuk mengetahui apakah tujuan dari penelitian ini untuk menghasilkan skema SKG yang efisien dapat tercapai. Hasil pengujian yang dilakukan menunjukkan bahwa skema SKG usulan 1 hingga 3 menghasilkan KGR yang lebih tinggi jika dibandingkan dengan skema usulan lain dengan KGR terendah yang diperoleh adalah 7,10 bps. Skema ini menggunakan 5 tahap dalam pembangkitan *secret key* yaitu *channel probing*, pra proses, kuantisasi multilevel, rekonsiliasi informasi serta *privacy amplification*. Tingginya KGR yang diperoleh disebabkan oleh adanya tahap rekonsiliasi informasi sehingga banyak blok data yang mampu dikoreksi dan tidak dibuang. Namun karena banyaknya tahapan yang harus dilalui maka durasi waktu yang dibutuhkan lebih lama jika dibandingkan dengan skema yang lain. Semakin banyak blok data yang harus dikoreksi maka durasi waktu yang dibutuhkan juga akan meningkat secara signifikan. Skema usulan 4 dan skema SKG SSE menghasilkan KGR yang lebih rendah jika dibandingkan dengan skema usulan yang lain. Namun durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG juga lebih cepat karena tidak digunakannya tahap rekonsiliasi informasi. Skema usulan 4 membutuhkan durasi waktu yang lebih lama jika dibandingkan dengan skema SKG SSE karena adanya penggunaan dua metode pra proses yang menambah waktu komputasi pada tahap pra proses. Peningkatan durasi waktu ini juga berpengaruh pada penurunan KGR yang dihasilkan. Dibandingkan dengan skema usulan yang lain, kami menyarankan penggunaan skema SKG SSE untuk pembangkitan *secret key* karena lebih efisien dan ditunjukkan dengan cepatnya durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG sehingga sesuai untuk perangkat dengan keterbatasan sumber daya. Waktu yang dibutuhkan untuk melakukan *refresh secret key* juga masih memenuhi persyaratan dari IEEE 802.1x yaitu dibawah 1 jam.

Tabel 5.29 Matrik Perbandingan Parameter Performansi Skema SKG SSE dengan Skema yang Eksisting

Skenario	Skema	Simulasi			Eksperimen		
		Jumlah 128-bit kunci yang identik	KGR	Durasi Waktu (menit)	Jumlah 128-bit kunci yang identik	KGR	Durasi Waktu (menit)
5	Skema SKG SSE	4	32,12	0,27	4	1,05	8,13
	Skema 10	61	70,18	1,85	61	7,92	16,42
	Skema 11	61	59,47	2,19	59	6,83	18,42
	Skema 12	46	47,90	2,05	36	4,73	16,25
	Skema 13	61	47,42	2,74	61	6,95	18,72
	Skema 14	36	41,55	1,85	40	5,24	16,28
6	Skema SKG SSE	1	7,99	0,27	4	1,05	8,14
	Skema 10	59	66,77	1,89	61	7,88	16,52
	Skema 11	61	59,65	2,18	52	6,03	18,40
	Skema 12	44	46,34	2,03	43	5,70	16,10
	Skema 13	61	47,45	2,74	61	6,95	18,72
	Skema 14	8	9,22	1,85	27	3,54	16,25

Tabel 5.30 Matrik Perbandingan Parameter Performansi Hasil Eksperimen Skema yang diusulkan

Skema	Skenario	KGR (bps)	Kompleksitas masing-masing tahapan skema SKG					
			Pra proses		Kuantisasi	Rekonsiliasi informasi	Privacy Amplification	
			Pra proses 1	Pra proses 2			Universal hash	SHA-1
Skema usulan 1	1	9,24	$O(pq)$	----	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
	2	9,24						
	3	9,20						
Skema usulan 2	4	7,10	$O(pq)$	$O(n)$	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema usulan 3	3	8,03	$O(pq)$	-	$O(pq)$	$O(pqr)$	$O(p^2)$	$O(p)$
Skema usulan 4	5	0,92	$O(pq)$	$O(pq)$	$O(pq)$	----	$O(p^2)$	$O(p)$
	6	0,45						
Skema SKG SSE	5	1,05	----	----	$O(pq)$	----	$O(p^2)$	$O(p)$
	6	1,05						

--Halaman ini sengaja dikosongkan--

BAB 6

KESIMPULAN DAN SARAN

6.1 Kesimpulan

Beberapa pengembangan skema SKG telah dihasilkan pada disertasi ini dengan performansi yang telah dievaluasi secara simulasi dan eksperimental. Dari pembahasan yang telah dilakukan pada bab-bab sebelumnya, maka disimpulkan beberapa hal sebagai berikut :

1. Telah dihasilkan kombinasi metode pra proses Kalman Filter dengan kuantisasi multilevel *Adaptive* sebagai salah satu mekanisme peningkatan performansi skema SKG yang mampu mengatasi *trade-off* parameter performansi KDR dan KGR. Penurunan KDR menjadi sebesar 58,9 % skema yang eksisting sedangkan peningkatan KGR setelah rekonsiliasi informasi mencapai 2,79 kali skema yang eksisting dengan waktu yang dibutuhkan untuk mendapatkan 256 bit *secret key* adalah 27,71 detik. Dibandingkan dengan mekanisme peningkatan performansi yang lain maka mekanisme ini menghasilkan penurunan KDR dan peningkatan KGR yang lebih tinggi. Penggunaan metode pra proses Kalman Filter memberikan peningkatan *reciprocity* yang lebih signifikan karena banyaknya parameter yang dapat diubah/dimodifikasi sehingga bisa didapatkan peningkatan koefisien korelasi yang lebih optimal jika dibandingkan dengan metode pra proses yang lain. Peningkatan koefisien korelasi ini juga berpengaruh pada lebih rendahnya KDR. Semakin rendah nilai KDR maka semakin besar kemungkinan perbedaan bit di masing-masing blok data dapat dikoreksi saat tahap rekonsiliasi informasi sehingga mengurangi jumlah blok data yang terbuang dan meningkatkan nilai KGR_r dan KGR_{pa}.
2. Telah dihasilkan kombinasi pengembangan metode pra proses *Modified Polynomial Regression* (MPR) dengan kuantisasi multilevel *Adaptive* sebagai salah satu mekanisme peningkatan performansi skema SKG yang mampu mengatasi

trade-off parameter performansi KDR dan KGR. Penurunan KDR menjadi sebesar 53,72 % skema yang eksisting sedangkan KGR setelah rekonsiliasi informasi mengalami peningkatan hingga 81,95% dengan waktu yang dibutuhkan untuk mendapatkan 256 bit *secret key* adalah 36,06 detik. Mekanisme peningkatan performansi ini membutuhkan durasi waktu yang lebih lama untuk menyelesaikan satu tahapan skema SKG dibadingkan dengan mekanisme yang lain. Hal ini terjadi karena mekanisme yang diusulkan merupakan gabungan antara dua metode pra proses yaitu Regresi Polinomial dengan Moving average. Lamanya durasi waktu tersebut juga berpengaruh terhadap KGR_{pa} yang dihasilkan, dimana mekanisme ini menghasilkan KGR_{pa} yang lebih rendah jika dibandingkan dengan mekanisme peningkatan performansi yang lain.

3. Telah dihasilkan kombinasi metode pra proses *Savitzky Golay Filter* dengan kuantisasi multilevel *Adaptive* sebagai salah satu mekanisme peningkatan performansi skema SKG yang mampu mengatasi *trade-off* parameter performansi KDR dan KGR. Penurunan KDR menjadi sebesar 46,13 % dibandingkan dengan skema yang eksisting sedangkan KGR setelah rekonsiliasi informasi mengalami peningkatan hingga 2,29 kali dengan waktu yang dibutuhkan untuk mendapatkan 256 bit *secret key* adalah 31, 89 detik. Mekanisme peningkatan performansi ini memiliki nilai KGR_{pa} yang lebih tinggi jika dibandingkan dengan mekanisme peningkatan performansi dengan kombinasi metode pra proses Kalman Filter dengan kuantisasi multilevel *Adaptive* meskipun KDR yang dihasilkan juga lebih tinggi. Hal ini terjadi karena metode pra proses yang digunakan pada mekanisme ini hanya satu metode sehingga mengurangi durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG. Penurunan durasi ini juga berpengaruh pada peningkatan KGR_{pa} yang diperoleh.
4. Didapatkannya mekanisme penyederhanaan skema SKG dengan kombinasi metode *Modified* Kalman (MK) serta *Combined Multilevel Quantization* (CMQ) dengan menghilangkan tahap rekonsiliasi informasi. Keberhasilan skema SKG ini

ditunjukkan dengan didapatkannya 4 kunci di lingkungan tanpa halangan serta 2 kunci yang memiliki KDR sebesar 0 sehingga tidak memerlukan koreksi untuk mendapatkan *secret key* yang identik. Waktu yang dibutuhkan untuk mendapatkan 128-bit *secret key* adalah 2,32 menit (lingkungan tanpa halangan) serta 4,74 menit (lingkungan dengan halangan). Dibandingkan dengan skema yang eksisting serta mekanisme peningkatan performansi dengan kombinasi pra proses dan kuantisasi multilevel maka skema SKG ini lebih sederhana karena bisa didapatkan *secret key* yang identik tanpa menggunakan tahap rekonsiliasi informasi namun dengan KGR_{pa} yang lebih rendah. Kondisi ini terjadi karena *secret key* yang digunakan adalah *secret key* yang benar-benar identik tanpa melalui tahap rekonsiliasi informasi sehingga *secret key* yang tidak identik akan dibuang. Pemanfaatan tahap rekonsiliasi informasi pada skema yang eksisting serta mekanisme peningkatan performansi dengan kombinasi pra proses dan kuantisasi multilevel memang mampu meningkatkan KGR_{pa} yang dihasilkan, namun dengan semakin banyaknya blok data yang harus dikoreksi juga akan meningkatkan durasi waktu yang dibutuhkan sehingga tidak sesuai jika diimplementasikan pada perangkat dengan keterbatasan sumber daya.

5. Didapatkannya skema SKG yang efisien dalam hal waktu komputasi, komunikasi dan *overhead* komunikasi dengan menggunakan metode *Synchronized Quantization* (SQ) sebagai bagian dari skema SKG *Signal Strength Exchange* (SSE) yang melakukan sinkronisasi blok data pada tahap kuantisasi. Penurunan waktu komputasi dari bagian A menjadi sebesar 3,9% (skenario 5) dan 3,8% (skenario 6) skema yang eksisting sedangkan penurunan waktu komunikasi menjadi sebesar 64% (skenario 5) dan 65% (skenario 6) skema yang eksisting. Hasil pengujian dari bagian B menunjukkan bahwa skema SKG SSE mampu mengurangi waktu komputasi menjadi sebesar 38% (skenario 5) dan 40% (skenario 6) skema yang esksisting sedangkan penurunan *overhead* komunikasi dari bagian A menjadi sebesar 36% (skenario 5) dan 34% (skenario 6) skema yang eksisting. Secara keseluruhan terlihat bahwa waktu komputasi dan komunikasi dari skema

SKG SSE lebih rendah dari skema SKG yang eksisting. Hal ini terjadi karena pada bagian A, konversi multi bit dari skema SKG SSE didapatkan langsung dari parameter kanal RSS hasil pengukuran tanpa melalui tahap pra proses. Lebih lanjut, tidak ada pembagian blok pada pengolahan parameter kanal RSS sehingga dapat mengurangi waktu komputasi jika dibandingkan dengan skema yang eksisting. Tingginya waktu komputasi dari skema SKG yang eksisting diakibatkan oleh adanya tahap rekonsiliasi informasi. Semakin banyak data yang diolah maka semakin tinggi waktu komputasi, komunikasi serta *overhead* komunikasi yang dibutuhkan. Tidak ada perbedaan *overhead* komunikasi yang signifikan dari bagian B antara skema SKG SSE dengan skema yang eksisting karena *overhead* komunikasi yang dihasilkan hampir sama. Hal ini terjadi karena sinkronisasi setelah tahap SQ hanya dilakukan pada indeks blok data yang terbuang sedangkan sinkronisasi setelah tahap rekonsiliasi informasi dilakukan pada bit *parity* sehingga meningkatkan ukuran dari *overhead* komunikasi.

6. Skema SKG dengan kombinasi metode MK dan CMQ serta skema SKG SSE menghasilkan KGR yang lebih rendah jika dibandingkan dengan skema usulan yang lain. Namun durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG juga lebih cepat karena tidak digunakannya tahap rekonsiliasi informasi. Skema kombinasi metode MK dan CMQ membutuhkan durasi waktu yang lebih lama jika dibandingkan dengan skema SKG SSE karena adanya penggunaan dua metode pra proses yang menambah waktu komputasi pada tahap pra proses. Peningkatan durasi waktu ini juga berpengaruh pada penurunan KGR yang dihasilkan. Dibandingkan dengan skema usulan yang lain, skema SKG SSE merupakan skema yang lebih efisien dan ditunjukkan dengan lebih cepatnya durasi waktu yang dibutuhkan untuk menyelesaikan satu tahapan skema SKG sehingga sesuai untuk perangkat dengan keterbatasan sumber daya. Waktu yang dibutuhkan untuk melakukan *refresh secret key* juga masih memenuhi persyaratan dari IEEE 802.1x yaitu dibawah 1 jam.

6.2 Saran

Beberapa hal yang dapat dikembangkan dari disertasi ini antara lain adalah :

1. Pengembangan aspek keamanan skema SKG yang dibangun. Aspek keamanan tidak hanya dilihat dari *passive attack* namun juga dari *active attack* dengan menggunakan berbagai mekanisme serangan
2. Pengembangan lingkungan yang digunakan untuk melakukan validasi eksperimental. Validasi tidak hanya dilakukan di lingkungan *indoor* namun juga dapat dilakukan di lingkungan *outdoor*.
3. Pengembangan jenis parameter kanal yang digunakan sebagai sumber pembangkitan *secret key*. Terdapat beberapa jenis parameter kanal yang dapat digunakan diantaranya CSI, RSS, serta Bluetooth.

--Halaman ini sengaja dikosongkan--

DAFTAR PUSTAKA

Ahlswede, R. and Csiszar, I. (1993) ,"Common randomness in information theory and cryptography – Part I: secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132.

Ali, S.T, Sivaraman, V. and Ostry, D. (2014), "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 12, pp. 2763–2776.

Ali, S.T., Sivaraman, V. and Ostry, D. (2010), "Secret Key Generation Rate vs. Reconciliation Cost Using Wireless Channel Characteristics in Body Area Networks," *in Proc. of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, Hong Kong, China, pp. 644–650.

Ambekar, A. (2015), *Exploiting Radio Channel Aware Physical Layer Concepts,* Ph.D Dissertation, Kaiserslautern University of Technology, Kaiserslautern.

Ambekar, A., Hassan, M. and Schotten, H.D. (2012), " Improving channel reciprocity for effective key management systems, " *In Signals, Systems, and Electronics (ISSSE), 2012 International Symposium on*, Postdam, Germany pages 1–4.

Aono, T., Higuchi, K. , Ohira, T. , Komiyama, B. and Sasaoka, H.(2005), ''Wireless secret key generation exploiting reactance domain scalar response of multipath fading channels, '' *IEEE Trans. Antennas Propag.,* vol. 53, no. 11, pp. 3776-3784.

Bregman, I. (2008), *Public Keys and Private Keys in Quantum Cryptography* , Ph.D Dissertation, Hebrew University, Jerusalem.

Carter, J.L. and Wegman, M.N. (1979), "Universal Classes of Hash Functions," *J. Comput. Syst. Sci.* 18, 143–154.

Chen, L., Ji, J. and Zhang, Z. (2013), Eds., *Wireless Network Security: Theories and Applications*, Springer.

Cheng, L., Zhou, L., Seet, B.-C., Li, W., Ma, D. and Wei, J, "Efficient Physical-Layer Secret Key Generation and Authentication Schemes Based on Wireless Channel-Phase, " *Mob. Inf. Syst.*, *2017*, 7393526.

Edman, M., Kiayias, A. and Yener, B. (2011), ''On passive inference attacks against physical-layer key extraction?'' *in Proc. 4th Eur. Workshop Syst. Secur.*, Salzburg, Austria, pp. 8:1–8:6.

Gene H Golub and Charles F Van Loan. (2012), *Matrix computations*, volume 3, JHU Press.

Guillaume, R., Winzer, F. and Czylwik, A. (2015), "Bringing PHY-based key generation into the field: An evaluation for practical scenarios", *in Proc. 82nd IEEE Veh. Technology Conf. (VTC Fall)*, Boston, USA, pp. 1–5.

He, X. , Dai, H., Huang, Y., Wang, D., Shen, W. and Ning, P. (2014), ''The security of link signature: A view from channel models,'' *in Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, San Francisco, CA, USA, pp. 103–108.

Hershey, J. E., Hassan, A. and Yarlagadda, R. (1995), "Unconventional crypto-

graphic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6.

Jana, S., Premnath, S. N., Clark, M., Kasera, S. K., Patwari, N. and Krishnamurthy, S. V. (2009), "On the effectiveness of secret key extraction from wireless signal strength in real environments," *in Proc. 15th Annu. Int. Conf. Mobile Computing and Networking (MobiCom)*, Beijing, China, pp. 321–332.

Jiang, Y., Hu, A. and Huang, J. A lightweight physical-layer based security strategy for Internet of things. *Clust. Comput*., doi:10.1007/s10586-018-1820-0.

Liu, H., Yang, J., Wang, Y., Chen, Y. and Koksal, C. (2014), "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2820–2835.

Liu, H. , Wang, Y., Yang, J. and Chen, Y. (2013), "Fast and practical secret key extraction by exploiting channel response," *in Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, pp. 3048–3056.

Liu, Y., Draper, S. C. and Sayeed, A. M. (2012), "Exploiting channel diversity in secret key generation from multipath fading randomness," *IEEE Trans. Inf. Forensics Security,* vol. 7, no. 5, pp. 1484–1497.

Lopez, A.B. (2017), *Physical Layer Key Generation for Wireless Communication Security in Automotive Cyber-Physical Systems*. Ph.D. Thesis, University of California, Irvine, CA, USA.

McGuire, M. (2014), "Channel Estimation for Secret Key Generation", *in Proceedings of the International Conference on Advanced Information Networking and Applications*, Victoria, BC, Canada, pp. 490–496.

Margelis, G., Fafoutis, X., Oikonomou, G., Piechocki, R., Tryfonas, R. and Thomas, P. (2018), " Efficient DCT-based secret key generation for the Internet of Things", *Ad Hoc Netw.*, in press.

Marino, F., Paolini, E. and Chiani, M. (2014), "Secret key extraction from a UWB channel: Analysis in a real environment," *in Proc. IEEE Int. Conf. Ultra-WideBand (ICUWB)*, Paris, France, pp. 80–85.

Mathur, S., Reznik, A., Ye, C., Mukherjee, R., Rahman, A., Shah, Y., Trappe, W. and Mandayam, N. (2010), "Exploiting the physical layer for enhanced security," *IEEE Wireless Commun. Mag*., vol. 17, no. 5, pp. 63–70.

Mathur, S., Trappe, W., Mandayam, N., Ye, C. and Reznik, A. (2008), "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel", *in Proc. 14th Annu. Int. Conf. Mobile Computing and Networking (MobiCom)*, San Francisco, California, USA, pp. 128–139.

Maurer, U. M. (1993),"Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory,* vol. 39, no. 3, pp. 733–742.

Menezes, A. J., Van Oorschot, P. C. and Vanstone, S. A. (1996), *Handbook of Applied Cryptography*, CRC press.

Mukherjee, A., Fakoorian, S., Huang, J. and Swindlehurst, A. (2014), "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573.

Moore, T. (2001), *IEEE 802.11-01/610r02: 802.1.x and 802.11 Key Interactions*, Technical Report, Microsoft Research.

Patwari, N., Croft, J., Jana, S. and Kasera, S. K. (2010), "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput*, vol. 9, no. 1, pp. 17–30.

Premnath, S.N. , Jana, S., Croft, J., Gowda, P.L., Clark, M., Kasera, S.K, Patwari, N. and Krishnamurthy, S.V. (2013), "Secret key extraction from wireless signal strength in real environments", *IEEE Transactions on Mobile Computing*, 12(5), pp.917–930.

Ren, K., Su, H. and Wang, Q. (2011), "Secret key generation exploiting channel characteristics in wireless communications", *IEEE Wireless Commun. Mag.*, vol. 18, no. 4, pp. 6–12.

Rukhin, A. L , Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S. (2010), *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. 800-22.

Shehadeh, Y.E.H, Alfandi, O., Tout, K. and Hogrefe, D. (2011), "Intelligent mechanisms for key generation from multipath wireless channels," *in Proc. Wireless Telecommun. Symp. (WTS)*, New York City, New York, USA, pp. 1–6.

Shiu, Y.S., Chang, S. Y., Wu, H.C., Huang, S.H. and Chen, H.H. (2011), "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun. Mag.*, vol. 18, no. 2, pp. 66–74.

Stallings, W. (2013), *Cryptography and Network Security: Principles and Practice*, 6th ed. Prentice Hall.

Sudarsono, A., Yuliana, M., Kristalina, P. and Barakbah, A.R. (2018), "An Implementation of Shared Key Generation Extracted from Received Signal Strength in Vehicular Ad-Hoc Communication, " *In Proceedings of the 2018 Sixth International Symposium on Computing and Networking (CANDAR)*, Takayama, Japan, pp. 57–65.

Vogt, H. , Ramm, K. and Sezgin, A. (2016), "Practical secret-key generation by full-duplex nodes with residual self-interference, " in *Proc. 20th Int. ITG Workshop Smart Antennas*, Munich, Germany, pp. 1-5.

Wang, Q., Wang, X., Lv, Q., You, L., and Yu, W. (2015), "Pre-process Method for Reducing Initial Bit Mismatch Rate in Secret Key Generation based on Wireless Channel Characteristics," *in proc. 2015 IEEE 16th International Conference on Communication Technology (ICCT)*, Hangzhou, China.

Wang, Q, Su, H., Ren, K. and Kim, K. (2011), "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," *in INFOCOM 2011. 30th IEEE International Conference on Computer Communications, Joint Conference of the IEEE Computer and Communications Societies*, Shanghai, China, pages 1422–1430. IEEE, 2011.

Wei, Y., Zeng, K. and Mohapatra, P. (2013), "Adaptive wireless channel probing for shared key generation based on PID controller", *IEEE Transactions on Mobile Computing*, 12(9), pp.1842–1852.

Welch, G. and Bishop, G. (2006) , *An Introduction to the Kalman Filter*, Technical report, University of North Carolina at Chapel Hill.

Wu, B., Chen, J., Wu, J. and Cardei, M. (2007), "A survey of attacks and countermeasures in mobile ad hoc networks," *in Wireless Network Security,* Y. Xiao, X. Shen, and D. Du, Eds. Springer, 2007, pp. 103–135.

Ye, C. and Reznik, A. (2007), "Group secret key generation algorithms," *in Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, pp. 2596–2600.

Yuliana, M.; Wirawan; Suwadi. (2019a), "A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization". *Entropy*, 21, 192.

Yuliana, M., Wirawan and Suwadi. (2019b), "Performance Analysis of Loss Multilevel Quantization on the Secret Key Generation Scheme in Indoor Wireless Environment", *Int. J. Adv. Sci. Eng. Inf. Technol.*, 9, pp. 100–108.

Yuliana, M., Wirawan and Suwadi. (2019c), "An Efficient Key Generation for the Internet of Things Based Synchronized Quantization", *Sensors,* 19*(*12), 2674.

Yuliana, M., Wirawan and Suwadi. (2018a), "Improving performance of secret key generation from wireless channel using filtering techniques", in *Proceedings of the Tenth International Conference on Signal Processing Systems*, Singapore, doi:10.1117/12.2521870.

Yuliana, M., Wirawan and Suwadi. (2018b), "Enhancing Channel Reciprocity of Secret Key Generation Scheme by Using Modified Polynomial Regression Method", ", in *Proceedings of the International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM)*, Surabaya, Indonesia, 10.1109/CENIM.2018.8711332.

Yuliana, M., Wirawan and Suwadi (2017a), " Performance evaluation of the key extraction schemes in wireless indoor environment", *in Proceedings - International Conference on Signals and Systems, ICSigSys 2017*, Sanur, Indonesia, pp.138-144.

Yuliana, M., Wirawan and Suwadi (2017b), "Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment," *International Journal of Communication Networks and Information Security (IJCNIS)*, vol.9,no.3, pp.474-482.

Zeng, K., Wu, D. , Chan, A. and Mohapatra, P. (2010), ''Exploiting multiple- antenna diversity for shared secret key generation in wireless networks,'' in *Proc. 29th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, San Diego, CA, USA, pp. 1–9.

Zenger, C. T., Zimmer, J., Pietersz, M., Posielek, J.-F. and Paar, C. (2015), ''Exploiting the Physical Environment for Securing the Internet of Things'', *Proceedings of the New Security Paradigms Workshop on ZZZ - NSPW '15*, pp. 44–58. doi: 10.1145/2841113.2841117.

Zhan, F., Yao, N., Gao, Z., Lu, Z. and Chen, B. (2019), "Efficient key generation leveraging channel reciprocity and balanced gray code", *Wirel. Netw.*, 25, 611–624, doi:10.1007/s11276-017-1579-x.

Zhan, F., Yao, N., Gao, Z. and Yu, H. (2018), "Efficient key generation leveraging wireless channel reciprocity for MANETs", *J. Netw. Comput. Appl.*, 103, 18–28.

Zhan, F. and Yao, N. (2017), "Efficient key generation leveraging wireless channel reciprocity and discrete cosine transform", *KSII Trans. Internet Inf. Syst.*, 11, 2701–2722.

Zhang, J., Duong, T.Q., Woods, R.and Marshall, A. (2017), "Securing wireless communications of the internet of things from the physical layer, an overview", *Entropy*, 19, 420.

Zhang, J., Duong, T. Q., Marshall, A. and Woods, R. (2016a), "Key Generation from Wireless Channels: A Review", *IEEE Access*, vol. 4, pp. 614–626.

Zhang, J., Woods, R., Marshall, A. and Duong, T. Q. (2015), "Verification of key generation from individual OFDM subcarrier's channel response," *in Proc. IEEE GLOBECOM Workshop Trusted Commun. with Physical Layer Security (TCPLS)*, San Diego, California, USA, pp. 1–6.

Zhang, J., Marshall, A., Woods, R. and Duong, T. Q. (2014), "Secure key generation from OFDM subcarriers' channel responses," *in Proc. IEEE GLOBECOMWorkshop Trusted Commun. with Physical Layer Security (TCPLS)*, Austin, Texas, USA, pp. 1302–1307

--Halaman ini sengaja dikosongkan--

Lampiran 1A. Tes NIST

Frequency (Monobit) Test

Tujuan dari tes ini adalah untuk menentukan apakah jumlah 1 dan 0 pada kunci yang dihasilkan hampir sama seperti yang diharapkan untuk rangkaian kunci yang benar-benar acak.

Block Frequency Test

Tujuan dari tes ini adalah untuk menentukan apakah frekuensi bit 1 dalam sebuah blok dengan sejumlah M bit adalah $M / 2$ agar bisa memenuhi persyaratan keacakan.

Runs Test

Tujuan dari tes ini adalah untuk menentukan apakah osilasi dari 0 dan 1 terlalu cepat atau terlalu lambat.

Longest Run of Ones in a Block Test

Tujuan dari tes ini adalah untuk menentukan apakah banyaknya bit 1 pada rangkaian kunci adalah konsisten dengan panjang bit 1 pada bilangan acak. Ketidakteraturan panjang bit 1 juga akan berakibat pada ketidakteraturan bit 0.

Approximate Entropy Test

Tujuan dari tes ini adalah untuk membandingkan frekuensi dari blok yang *overlapping* dengan panjang yang berurutan..

Cumulative Sums (Cusum) Test

Tujuan dari tes ini adalah untuk menentukan apakah jumlah kumulatif dari bit kunci yang dihasilkan relatif terlalu besar atau terlalu kecil terhadap jumlah kumulatif yang diharapkan dari sebuah bit kunci yang acak.

```
========== PENGUJIAN NIST TEST SUITE ==========

========== KUNCI KE 1 ==========

BIT KUNCI = 10000111110010111010000111100000011100001110000000100101010110011011011
10001100110100011100100010000100110001101011000010110111 1

APPROXIMATE ENTROPY TEST [1]            = 0.411051
FREQUENCY TEST [1]                      = 0.376759
BLOCK FREQUENCY TEST [1]                = 0.414261
CUMULATIVE SUMS (FORWARD) TEST [1]      = 0.369656
CUMULATIVE SUMS (REVERSE) TEST [1]      = 0.499939
RUNS TEST [1]                           = 0.412311
LONGEST RUNS OF ONES TEST [1]           = 0.594441
-----------------------------------------------
```

Gambar A.1 Contoh pengujian NIST 1

```
========== KUNCI KE 2 ==========

BIT KUNCI = 00000000000000111111111111111000000000100110111101100100011111011110001 0
01111010110110001011010110110111001000011110001001100001 0

APPROXIMATE ENTROPY TEST [2]            = 0.017385
FREQUENCY TEST [2]                      = 0.859684
BLOCK FREQUENCY TEST [2]                = 0.004650
CUMULATIVE SUMS (FORWARD) TEST [2]      = 0.431439
CUMULATIVE SUMS (REVERSE) TEST [2]      = 0.574764
RUNS TEST [2]                           = 0.008060
LONGEST RUNS OF ONES TEST [2]           = 0.198306
-----------------------------------------------
```

Gambar A.2 Contoh pengujian NIST 2

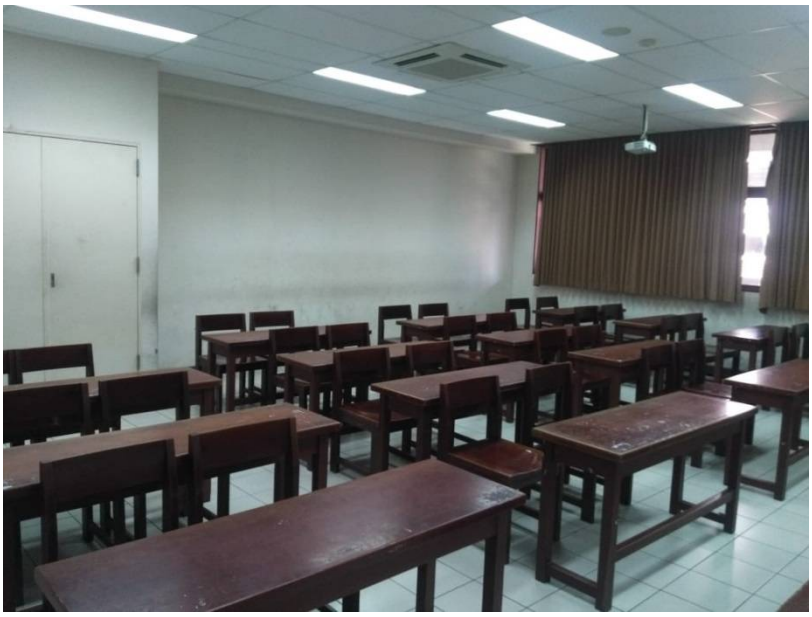
```
========== KUNCI KE 3 ==========

BIT KUNCI = 10000000000000011001000000011001111111111111111111110000000000000000101 0
01110101011111111111111111111111111111111111111111111111111111 1

APPROXIMATE ENTROPY TEST [3]            = 0.000000
FREQUENCY TEST [3]                      = 0.002654
BLOCK FREQUENCY TEST [3]                = 0.000000
CUMULATIVE SUMS (FORWARD) TEST [3]      = 0.005308
CUMULATIVE SUMS (REVERSE) TEST [3]      = 0.000006
RUNS TEST [3]                           = 0.000000
LONGEST RUNS OF ONES TEST [3]           = 0.003101
-----------------------------------------------
```

Gambar A.3 Contoh pengujian NIST 3

Lampiran 1B. Lingkungan Pengukuran

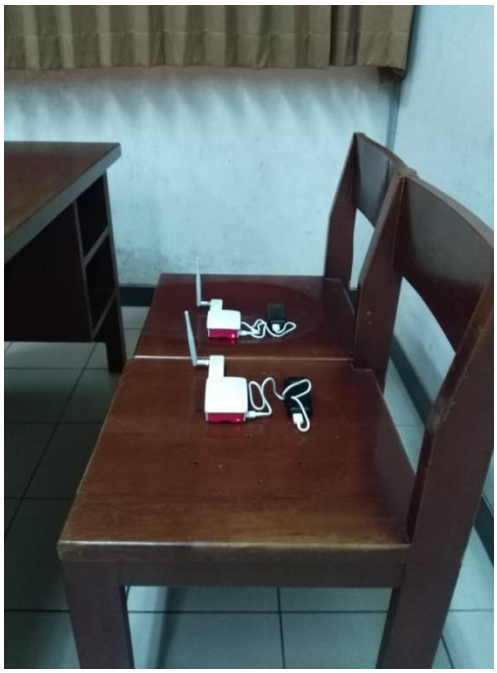


Gambar B.1 Ruangan Pengukuran di lingkungan tanpa halangan

Gambar B.2 Ruangan Pengukuran di lingkungan tanpa halangan tampak belakang

Gambar B.3 Ruangan Pengukuran ke-1 di lingkungan dengan halangan

Gambar B.4 Ruangan Pengukuran ke-2 di lingkungan dengan halangan



Gambar B.5 Contoh mekanisme pengukuran ke-1

Gambar B.6 Contoh mekanisme pengukuran ke-2

--Halaman ini sengaja dikosongkan--

CAPAIAN PUBLIKASI

A. Jurnal Internasional Terindex Scopus

1. Yuliana, M., Wirawan, & Suwadi (2017). Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment. *International Journal of Communication Networks and Information Security (IJCNIS), 9*(3), 474-482. (*Published)*
   ISSN: 2073-607X

2. Yuliana, M., Wirawan, & Suwadi (2019). Performance Analysis of Loss Multilevel Quantization on the Secret Key Generation Scheme in Indoor Wireless Environment. *International Journal on Advanced Science, Engineering and Information Technology, 9*(1), 100-108. (*Published)*
   ISSN: 2088-5334

3. Yuliana, M., Wirawan, & Suwadi (2019). A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization. *Entropy, 21*(2), 192. (*Published)*
   ISSN: 1099-4300

4. Yuliana, M., Wirawan, & Suwadi (2019). An Efficient Key Generation for the Internet of Things Based Synchronized Quantization. *Sensors*, *19*(12), 2674. (*Published)*
   ISSN: 1424-8220

B. Seminar Internasional

1. Yuliana, M., Wirawan, & Suwadi (2017). Performance evaluation of the key extraction schemes in wireless indoor environment. *2017 International Conference on Signals and Systems (ICSigSys)*, Sanur, Indonesia, 16-18 May 2017. Signal Processing Society. doi: 10.1109/ICSIGSYS.2017.7967029.

2. Yuliana, M., Wirawan, & Suwadi (2018). Improving performance of secret key generation from wireless channel using filtering techniques. *Tenth International Conference on Signal Processing Systems*, Singapore, 16-18 November 2018. The International Society for optics and photonics. doi:10.1117/12.2521870.

3. Yuliana, M., Wirawan, & Suwadi (2018). Enhancing Channel Reciprocity of Secret Key Generation Scheme by Using Modified Polynomial Regression Method. *2018 International Conference on Computer Engineering, Network and Intelligent Multimedia (CENIM),* Surabaya, Indonesia, 26-27 Novomber 2018. doi: 10.1109/CENIM.2018.8711332.

entropy

MDPI

Article

A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization

Mike Yuliana [1,2,*], Wirawan [1] and Suwadi [1]

[1] Department of Electrical Engineering, Faculty of Electrical Technology, Institut Teknologi Sepuluh Nopember, Jalan Raya ITS, Keputih, Sukolilo, Surabaya 60111, Indonesia; wirawan@ee.its.ac.id (W.); suwadi@ee.its.ac.id (S.)

[2] Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya (PENS), Jalan Raya ITS, Keputih, Sukolilo, Surabaya 60111, Indonesia

* Correspondence: mieke@pens.ac.id or mike16@mhs.ee.its.ac.id; Tel.: +62-812-1746-4666

Received: 14 January 2019; Accepted: 15 February 2019; Published: 18 February 2019

Abstract: Limitations of the computational and energy capabilities of IoT devices provide new challenges in securing communication between devices. Physical layer security (PHYSEC) is one of the solutions that can be used to solve the communication security challenges. In this paper, we conducted an investigation on PHYSEC which utilizes channel reciprocity in generating a secret key, commonly known as secret key generation (SKG) schemes. Our research focused on the efforts to get a simple SKG scheme by eliminating the information reconciliation stage so as to reduce the high computational and communication cost. We exploited the pre-processing method by proposing a modified Kalman (MK) and performing a combination of the method with a multilevel quantization, i.e., combined multilevel quantization (CMQ). Our approach produces a simple SKG scheme for its significant increase in reciprocity so that an identical secret key between two legitimate users can be obtained without going through the information reconciliation stage.

Keywords: secret key generation; modified Kalman; combined multilevel quantization

1. Introduction

The Internet of Things (IoT) is one of the results of advancing network and telecommunications technology. This technology is expected to connect millions of home devices, vehicles, and industrial environments. Some applications that can be developed from this IoT device include autonomous vehicles [1], health services [2], industrial services [3], and smart homes [4]. It is conceivable that millions of devices will be equipped with various sensors and be connected to the internet through various heterogeneous networks. IoT, therefore, can be said as a system that allows the transfer of data between interconnected devices without human intervention. IoT infrastructure is connected to a communication network to collect and exchange information between devices. Referring to the basic character of wireless media, data aggregation through wireless communication is very vulnerable to eavesdropping [5–7]. This condition is a serious threat to the security of the IoT network, thus demanding the need for research dedicated to the security of wireless communication in collecting/exchanging data [6] and providing a system for hardware security [8].

The conventional symmetrical cryptographic protocol requires the distribution of secret key or certificate management to ensure the security of the data being transmitted [9–12], where the security of this protocol is influenced by the computing capability of the device. With the development of computing capabilities of the eavesdropping device (for example by using quantum computing technology), however, the protocol will be easily solved in the future [13–15]. Besides, the distribution

of a secret key is also very complex to implement on a large scale network because it requires intensive secret key distribution to support the establishment of secret keys between devices. Several studies focus on efforts to obtain cheap and promising solutions from symmetric cryptography and can be used as a lightweight cryptographic solution on IoT devices [16–21]. The SKG scheme is one solution that is often used for several reasons, i.e., it utilizing randomness from wireless channels so it is secure in theory, it can be conducted between a pair of users without the need for third-party assistance, and it is lightweight so it is suitable for IoT devices [5].

There are 3 properties of wireless channels that are often used in the SKG scheme, where the properties include reciprocity, spatial decorrelation, and they are spatial-temporal [22]. Reciprocity indicates that the wireless channel is symmetric, where the channels of legitimate users will be the same [23–25]. Spatial decorrelation can be fulfilled if the distribution is uniformly distributed and there are variations in channels due to scatterer movements, and also sending and receiving nodes. Eavesdroppers that are more than half the wavelength will get uncorrelated channel parameters with the legitimate users. Dynamic environmental conditions will also result in various wave propagation consequences such as scattering, diffraction, and reflection so the spatial-temporal character can be fulfilled. With the fulfillment of the spatial-temporal then the character of the channel parameters obtained are also expected to fulfill the randomness requirements. Besides environmental conditions, other factors that also affect the randomness of channel parameters are the coherence time of the channel.

Several types of channel parameters can be obtained from the communication between wireless devices, i.e., received signal strength (RSS) [26–29], channel impulse response (CIR) [30], and ultra-wideband (UWB) [31]. These parameters are obtained from the average signal strength provided by the physical layer within a certain time period. CIR and CSI parameters are difficult to explore in more detail since most wireless devices are not designed to display all channel information, so some studies have modified wireless card drivers. RSS parameters have their advantages, where the parameters can be obtained from most wireless devices without the need for modification. This is the basis for selecting RSS as a parameter to be extracted as the secret key in the implementation of the SKG scheme that will be built.

Generally, there are four stages used to generate a secret key, i.e., probing channel, quantization, information reconciliation, and privacy amplification [32,33]. The disadvantage of using these four SKG stages is the high mismatch bits that are produced between two users [34,35]. One of the solutions to solve this problem is the utilization of the pre-processing method before the quantization stage. This method performs smoothing or fitting, so it increases reciprocity between the two users and reduces the incompatibility of the bits produced. Some studies in [35–39] show that the utilization of this method can reduce the mismatch of bits produced but still requires an information reconciliation stage to correct the mismatch bits. This condition results in the increasing computational time needed, because of the increasing number of stages that must be passed. In addition, the information reconciliation stage also requires the exchange of parity bit between the two users, increasing the communication cost of the implementation of IoT device communication in real life.

In this paper, we focus on getting a simple SKG scheme by reducing the reconciliation stage, so it can reduce the high computational and communication cost of implementation. This paper has three main contributions. Firstly, a new pre-process method called modified Kalman (MK) is proposed. It combines the polynomial regression method with the modified Kalman filter. The results show that our approach can significantly increase reciprocity, so a high correlation can be obtained. Secondly, we combined MK method with a multilevel quantization called the combined multilevel quantization (CMQ) method. This method produces a simple SKG scheme for its significant increase in reciprocity, so it can obtain an identical secret key between two legitimate users without going through the information reconciliation stage. The stage reduction also resulted in less computational and communication cost. Thirdly, performance evaluation of our proposed SKG scheme was performed by using 802.11 devices in line of sight (LOS) and non-line of sight (NLOS) indoor environments.

The rest of this paper is organized as the following. Section 2 describes the system model used in the SKG scheme. Section 3 explains the detail of each stage from our proposed SKG scheme. Section 4 explains the experimental setup. In Section 5, the performance evaluation of the experiment is discussed. We conclude the paper in Section 6.

2. System Model

This section explains the modeling system used, and the principle of reciprocity as the main basis of the SKG scheme being built.

2.1. System Modelling on the Secret Key Generation (SKG) Scheme

Illustrations of the SKG scheme modeling can be seen in Figure 1. Two legitimate users, Alice and Bob, will generate wireless channel parameters $\left(h^a, h^b\right)$. In this paper, we use RSS as a channel parameter because most IoT devices have the ability to do RSS measurements. Eve, who acts as an eavesdropper, attempts to intercept the communication carried out by Alice and Bob $\left(h^e, h^{e'}\right)$, where Eve is a passive attacker model. Each user works in half-duplex mode. Alice and Bob will get high correlated channel parameters if the measurement is conducted in coherence time, so the principle of channel reciprocity can be fulfilled. Meanwhile, Eve, which is more than half the wavelength, will not get a correlated parameter channel with the legitimate user. In our SKG scheme, we assume that all the procedures and parameters used by the legitimate user are known by Eve.

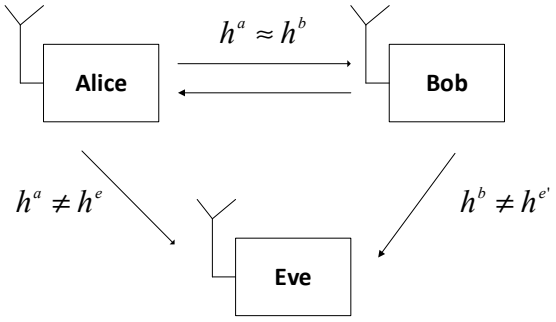


Figure 1. System modeling on the secret key generation (SKG) scheme.

2.2. Channel Reciprocity

Channel reciprocity is symmetrical characteristic of wireless channel parameters that allow for the formation of a secret key as an encryption key between two legitimate users. Wireless channel parameters are obtained by conducting measurements on each user, which is highly influenced by the characteristics of the various phenomena that characterize the wireless channel. Due to the limitations of the device which resulted in half duplex measurements, the SKG scheme sends and receives wireless channel parameters alternately. Two important parameters used in the measurement are the probing rate r_p and sampling rate r_s as shown in Figure 2. The principle of reciprocity can be fulfilled if the measurement of wireless channel parameters is carried out within coherence time T_c where the channel is assumed to be fixed, while randomness requirements can be fulfilled if $r_s^{-1} > T_c$ [40]. Coherence time invite/reply is influenced by various physical phenomena and changes from time to time and space. For example, we use 802.11b standard devices that work on a 2.4 GHz carrier frequency f_c. In dynamic scenarios where user movements occur, variations in wireless channel parameters are influenced by the Doppler effect. If the user speed v is 1.2 m/s, then the Doppler frequency obtained is $f_D = vf_c/c = 1.2x2.4x10^9/(3.10^8) = 9.6$ Hz. Coherence time obtained is $T_c = 1/|f_D| = 1/9.6 = 104.16$ ms. In our proposed SKG scheme, we use a sampling rate r_s^{-1} of 110 ms. The sampling rate value has exceeded coherence time, so the randomness requirements have been

fulfilled. Meanwhile, the probing rate is within coherence time, so the principle of channel reciprocity between two users also can be fulfilled.

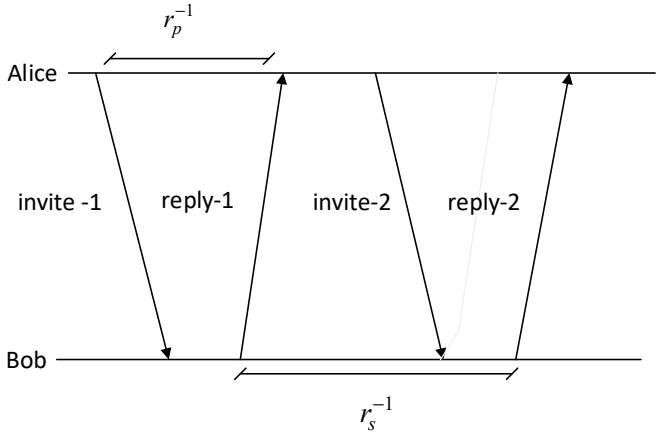


Figure 2. Measurement parameters.

3. Secret Key Generation Scheme

There are 3 parts described in this section, wherein the section includes existing SKG schemes, our proposed SKG schemes, and performance parameters.

3.1. Existing SKG Schemes

The procedure for obtaining a secret key from several previous studies generally consists of four stages. Firstly, by sending probe signals alternately between Alice and Bob to get wireless channel parameters called the probing stage channels. We use RSS channel parameters for ease of implementation, although there are some other channel parameters which have been discussed in several previous studies. Secondly, wireless channel parameters obtained from probing channel stage will be converted into the form of bits to obtain the initial key (quantization stage). Thirdly, information reconciliation stage to correct the mismatched bit in the initial key caused by noise and half duplex mode of the wireless device used. At this stage, the parity bit is exchanged to equalize the initial key, so a synchronized key can be obtained. The exchange of parity bit results in the leakage of the secret key making it easier for Eve to conclude the secret key generated. Fourthly, privacy amplification stage to increase the randomness of the secret key and verify the secret key generated.

The problem arising from the existence of the information reconciliation stage is that the increase in the cost of this stage is greatly influenced by the number of bit mismatches and the success of parity bit exchange. The more bit mismatch, the longer is the time needed to make corrections. The success of parity bit exchange is also strongly influenced by network conditions. If the network condition is poor, the longer is the time needed to exchange parity bit. In addition, parity bit exchanges also trigger the leakage of parity bit information to eavesdroppers, making it easier for eavesdroppers to get the same key. In this paper, we tried to solve these problems by proposing the pre-processing stage before quantization, so it can increase the reciprocity of RSS measurement results significantly. The combination of our proposed pre-process method with multilevel quantization is also able to reduce bit mismatches, so the identical secret keys can be obtained without requiring an information reconciliation stage.

3.2. Proposed SKG Schemes

Our proposed SKG scheme is shown in Figure 3 with the following four stages, i.e., channel probing, pre-process, multilevel quantization, and privacy amplification. To simplify the secret key generation procedure Alice was set as an initiator. Instead of directly changing the RSS measurement results into bits, we chose to add the pre-process stage using the MK

method. Several studies [35,38] expose that the addition of the pre-processing method before the quantization will reduce the incompatibility of the resulting bits. Our proposed pre-process method i.e., modified Kalman is a combination of the polynomial regression and modified Kalman filter. At this stage, the RSS measurement results divide into several data blocks and our proposed method is used to increase the reciprocity of each block of data. The advantage of this mechanism is the pre-processing method, which is able to work more effectively so there is a significant increase in reciprocity for several blocks of data. This increase is indicated by an increase in the value of the correlation coefficient close to 1. The next stage is a combination of the MK method with the CMQ. Quantization is used to change the RSS pre-process results into bits. We use multilevel quantization to avoid too few bits being generated. At this stage, the quantization process is carried out on each pre-process data block. Several blocks of data from the pre-process have a very high similarity with a correlation coefficient close to 1. Thus, this increases the probability of acquisition of an identical secret key between two legitimate users without going through the information reconciliation stage. Compared to other studies that also add a pre-processing stage [35–38], we can show that our proposed SKG scheme is simpler because it can reduce the information reconciliation stage. The advantage of losing this stage is the reduced difficulty of implementation because there is no exchange of parity bits. Another advantage is the increased security of the SKG scheme that was built because it reduces the possibility of leaking information to the eavesdropper. In the privacy amplification stage, we add a universal hash [41] to increase the randomness of the generated key so as to meet the requirements of randomness and SHA-1 [42] in order to guarantee that the generated key between two legitimate users is the same.

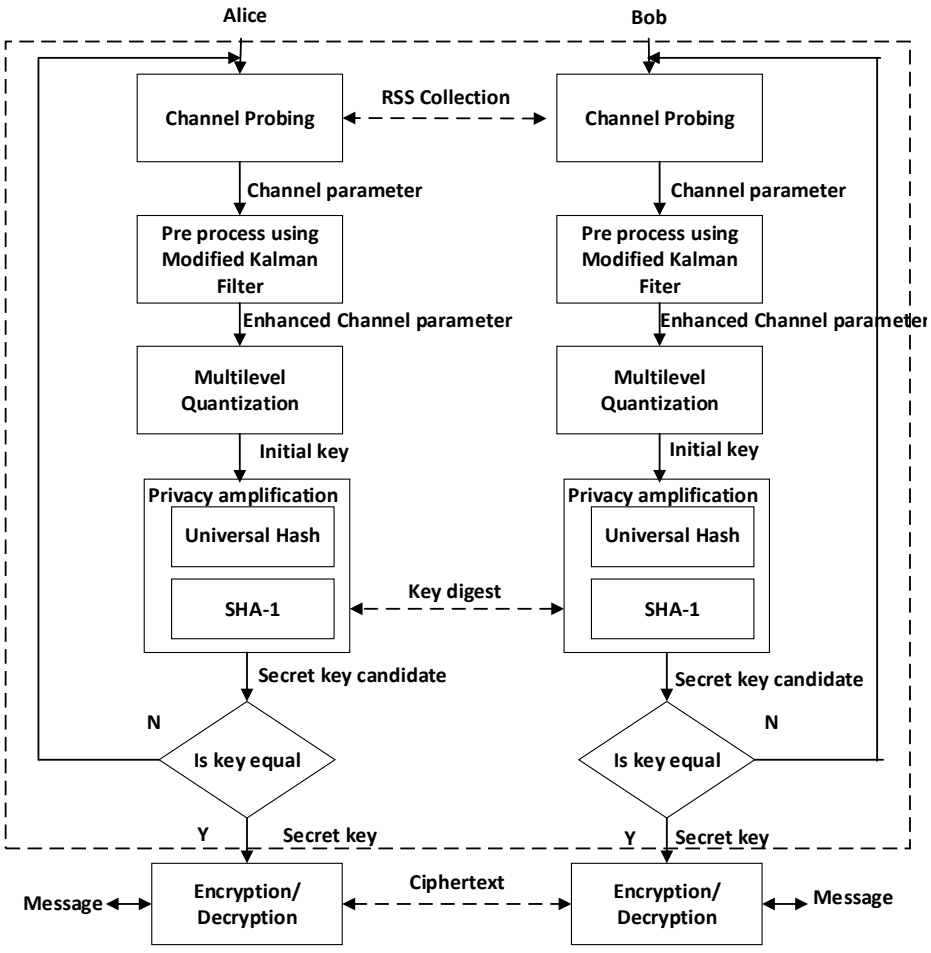


Figure 3. Our proposed SKG scheme.

In the probing channel stage, Alice and Bob measure the RSS channel parameters h^u, where the super-script u is replaced by a for Alice and b for Bob. However, because the wireless device used has a half-duplex mode, the two users cannot send and receive RSS simultaneously. We used the ping command to ensure that the invite and reply times from the channel parameter measurements do not exceed coherence time. At the completion of the channel probing stage, Two legitimate users will create sets of n RSS channel parameters which are expressed by Equations (1) and (2).

$$h^a = \{h^a(t_1), h^a(t_2), \ldots, h^a(t_n)\} \tag{1}$$

$$h^b = \left\{h^b(t'_1), h^b(t'_2), \ldots, h^b(t'_n)\right. \tag{2}$$

where h^a is the RSS channel parameter measured by Alice and h^b is the RSS channel parameter measured by Bob. In its implementation, although h^a is not exactly the same as h^b because of non-simultaneous measurements and noise, they will have a high correlation if bi-directional probing (for example $t'_1 - t_1$) is smaller than coherence time. During coherence time the channel is assumed to be stable, so $h^a \approx h^b$. Channel parameters received by the eavesdropper are defined by Equations (3) and (4):

$$h^e = \left\{h^e(t''_1), h^e(t''_2), \ldots, h^e(t''_n)\right. \tag{3}$$

$$h^{e\prime} = \left\{h^{e\prime}(t'''_1), h^{e\prime}(t'''_2), \ldots, h^{e\prime}(t'''_n)\right. \tag{4}$$

where h^e is channel parameter measured by Eve from Alice, while $h^{e\prime}$ is channel parameter measured by Eve from Bob. It was assumed that Eve was more than $\frac{1}{2}$ the wavelength from two legitimate users so it was difficult for Eve to generate the same key because h^e and $h^{e\prime}$ did not correlate with h^a and h^b.

The next stage is the pre-processed method which aims to increase the reciprocity of RSS channel parameters as measured by the two users. Our proposed pre-process method is the MK that combines the adopted polynomial regression (Algorithm 1) and modified the Kalman filter (Algorithm 2). In Algorithm 1, the RSS data measurement results h^u are then divided into several blocks N to reach a number of blocks N_B written as Equation (5).

$$h_N = [h_N^T \ldots h_{N-N_B+1}^T] \tag{5}$$

Each h_N contains a number of RSS data S_B. In this paper, we use the 2nd order polynomial regression, known as the quadratic for each RSS data block as shown in Equation (6).

$$h_\ell = a_0 + a_1 x_\ell + a_2 {x_\ell}^2 + e \tag{6}$$

where h_ℓ is the RSS data at a time x_ℓ with $\ell = (1, 2, \ldots, S_B)$, while e is RSS data discrepancy between Alice and Bob. The sum of the square of the residual S_r is expressed by Equation (7).

$$S_r = \sum_{\ell=1}^{S_B} (h_\ell - a_0 - a_1 x_\ell - a_2 x_\ell^2)^2 \tag{7}$$

The derivative of the equation is indicated by Equation (8).

$$\begin{array}{l} \frac{\partial S_r}{\partial a_0} = -2\sum (h_\ell - a_0 - a_1 x_\ell - a_2 x_\ell^2) \\ \frac{\partial S_r}{\partial a_1} = -2\sum x_\ell (h_\ell - a_0 - a_1 x_\ell - a_2 x_\ell^2) \\ \frac{\partial S_r}{\partial a_1} = -2\sum x_\ell^2 (h_\ell - a_0 - a_1 x_\ell - a_2 x_\ell^2) \end{array} \tag{8}$$

If the derivative of the Polynomial equation is made equal to zero then the normal equation is obtained as shown in Equation (9).

$$\begin{array}{c}(S_B)a_0 + (\sum x_\ell)a_1 + (\sum x_\ell^2)a_2 = \sum h_\ell \\ (\sum x_\ell)a_0 + (\sum x_\ell^2)a_1 + (\sum x_\ell^3)a_2 = \sum x_\ell h_\ell \\ (\sum x_\ell^2)a_0 + (\sum x_\ell^3)a_1 + (\sum x_\ell^4)a_2 = \sum x_\ell^2 h_\ell\end{array} \tag{9}$$

where a_0, a_1 and a_2 are 3 unknown Polynomial coefficient. We explain the detailed mechanism of the adopted polynomial algorithm that is run in each user in Algorithm 1. The way to calculate the element of normal equations in the form of an augmented matrix is shown on Lines 1–15 (Equation (9)), and the way for solving the augmented matrix to get 3 unknown polynomial coefficients by using elimination methods is shown on Lines 16–17. Finally, the output of pre-processing results by using adopted polynomial regression is shown on Line 20.

Algorithm 1: Adopted Polynomial Regression.

Input: Channel measurement h^u at the time x_ℓ.
Input: Block Number N_B, the size of each block S_B.
Input: Polynomial coefficient a, order polynomial m.
Output: Enhanced Polynomial Regression y^u

```
1:  for i ← 1 to N_B do
2:      for j ← 1 to m+1 do
3:          for k ← 1 to j do
4:              d = j + k − 2
5:              sum = 0
6:              for ℓ ← 1 to S_B
7:                  sum = sum + x_ℓ^d
8:              end for
9:              c_{j,k} = sum
10:             c_{k,j} = sum
11:         end for
12:         sum = 0
13:         for ℓ ← 1 to S_B
14:             sum = sum + x_ℓ^{j−1} . h^u_{ℓ,i}
15:         end for
16:         b_{j,1} = sum
17:         a_{j,1} = c \ b
18:     end for
19:     for ℓ ← 1 to S_B
20:         y^u_{ℓ,i} = a_{1,i} + a_{2,i} . x_ℓ + a_{3,i} . x_ℓ^2
21:     end for
22: end for
```

The MK method (Algorithm 2) works recursively to estimate status by using a priori and a posteriori estimation, where the estimation is carried out for each data block (the same as Algorithm 1). The initial estimation is carried out by the time update equation, while the correction of the estimation is carried out with the measurement update equation. The input of the time update equation is a priori estimation $\hat{x}_{k-1}$, a priori covariance error P_{k-1}, and covariance noise process Q. The equation of the time update is shown in Equation (10).

$$\begin{aligned} \hat{x}_k^- &= A.\hat{x}_{k-1} \\ P_k^- &= A.P_{k-1}.A + Q \end{aligned} \tag{10}$$

where A is a status of measurement at a time $k-1$. There are five inputs of the measurement update equation, i.e., $\hat{x}_k^-$, P_k^-, y_k^u, measurement noise covariance R and the variance of each data block v. We modified the correction process in the measurement update as shown in Equation (11).

$$\begin{aligned} K_k &= (P_k^- / (P_k^- + R) \\ P_k &= P_k^- (1 - K_k) \\ \hat{x}_k &= \hat{x}_k^- + K_k(y_k^u - H\hat{x}_k^-) \\ z_k &= \hat{x}_k \\ z_k &= z_k + 0.2v \end{aligned} \tag{11}$$

where H is a status of measurement at a time k, $\hat{x}_k$ is a posteriori estimation, P_k is a posteriori covariance error, K_k is Kalman gain, while z_k is RSS data as a result of the pre-processing stage with the MK method. We modified the a posteriori estimation results by adding 0.2 times the variance of each block of data and eliminate the parameter H with the aim of improving the reciprocity of pre-processing data z_k. The detailed mechanism of the MK method is explained in Algorithm 2. We initialize several parameters that provide the best configuration and shown on Lines 1–2. The time update process can be seen on Lines 4–5 and Lines 12–13 (Equation (10)), while the modified measurement update process can be seen on Lines 6–10 and Lines 14–18 (Equation (11)).

After the pre-processing stage, enhanced modified Kalman z^u will be converted into bit by using multilevel quantization, so the initial key can be obtained. Like the previous stage, in this stage, RSS data will also be divided into several data blocks. Algorithm 3 shows our proposed method, i.e., CMQ, wherein this algorithm combines the MK method with multilevel quantization. Inputs from this algorithm are z^u, mean of each block μ^u, and variance of each block v^u. The determination of the initial key bit is based on the Gray Code b_k at each level, and the levels' determinants are mean and variance for each block. Data outside the levels will be discarded. We select RSS amount of data per block to be quantized $S_B = 128$ because it produces the best performance parameters when compared to the other number. The significance of reciprocity improvement from the pre-process stage results in several identical initial keys, so it does not require the information reconciliation stage. This stage requires synchronization in the communication and requires a good network connection. If the network connection is poor, the synchronization process will be repeated, resulting in the system being built inefficiently.

The initial key obtained as output from the quantization stage does not necessarily fulfill the randomness requirements. In the privacy amplification stage, we add a universal hash [41] to ensure a small number of crashes in expectancy by using specific arithmetical properties. The addition of this function will increase the randomness of the initial key so that it is expected to be able to fulfill the minimum approximate entropy requirements. To test the randomness of the initial key we conducted randomization testing using the National Institute of Standards and Technology (NIST) statistical suite. The initial key that fulfills the requirements will be processed further so that it can be used as a key to the cryptosystem. We use SHA-1 [42] to guarantee that the initial key generated by two legitimate users is the same. Alice as the initiator sends a key digest from several initial keys to Bob. Bob also generates a key digest and compares the results with Alice. The same key digest shows the same initial

key bit. The same block of initial keys will be used as a candidate secret key, while different blocks will be discarded. SHA-1 produces a 160-bit message digest, so sending the entire message will result in high communication costs. In this paper, we only sent 6 bits from each block to obtain 98% correctness during the verification process [43].

Algorithm 2: Modified Kalman (MK).

Input: Enhanced Polynomial Regression y^u
Input: Status of measurement at a time $k-1$ A, status of measurement at the time k H
Input: co-variance of process noise Q, co-variance of measurement noise R
Input: A priori estimation $\hat{x}_k^-$, a priori covariance error P_k^-
Input: A posteriori estimation $\hat{x}_k$, a posteriori covariance error P_k
Input: Initial guesses $\hat{x}_0$, P_0
Input: Block number N_B, the size of each block S_B, the variance for each block v^u
Output: Enhanced modified Kalman z^u

$A = 2.13$, $H = 2.13$, $Q = 0.0001$, $R = 4.6$
$\hat{x}_0 = 0$, $P_0 = 1$
for $i \leftarrow 1$ **to** N_B **do**
  $\hat{x}_{k_{1,i}}^- = A.\hat{x}_0$
  $P_{k_{1,i}}^- = A.A.P_0 + Q$
  $K_{k_{1,i}} = P_{k_{1,i}}^- / (P_0 + R)$
  $P_{k_{1,i}} = P_{k_{1,i}}^- (1 - K_{k_{1,i}})$
  $\hat{x}_{k_{1,i}} = \hat{x}_{k_{1,i}}^- + K_{k_{1,i}} (y_{k_{1,i}}^u - H.\hat{x}_{k_{1.i}}^-)$
  $z_{k_{1,i}}^u = \hat{x}_{k_{1,i}}$
  $z_{k_{1,i}}^u = z_{k_{1,i}}^u + 0.2.\mathrm{v}_i^u$
  for $j \leftarrow 2$ **to** S_B **do**
    $\hat{x}_{k_{j,i}}^- = A.\hat{x}_{j-1,i}$
    $P_{k_{j,i}}^- = A.A.P_{j-1,i} + Q$
    $K_{k_{j,i}} = P_{k_{j,i}}^- / (P_{j,i} + R)$
    $P_{k_{j,i}} = P_{k_{j,i}}^- (1 - K_{k_{j,i}})$
    $\hat{x}_{k_{j,i}} = \hat{x}_{k_{j,i}}^- + K_{k_{j,i}} (y_{k_{j,i}}^u - H.\hat{x}_{k_{j,i}}^-)$
    $z_{k_{j,i}}^u = \hat{x}_{k_{j,i}}$
    $z_{k_{j,i}}^u = z_{k_{j,i}}^u + 0.2.\mathrm{v}_i^u$
  end for
end for

Algorithm 3: Combined Multilevel Quantization (CMQ).

Input: Enhanced channel parameter z^u
Input: Block Number N_B, the size of each block S_B
Input: The variance for each block v^u, means of each block u^u, quantization level Q
Output: Initial key K^u

$Q = 2$
Construct Gray code b_k ($k \leftarrow 1$ **to** $2^Q - 1$)
Assign them to a different level [level 1, level 4]
for $i \leftarrow 1$ **to** N_B **do**
  for $j \leftarrow 1$ **to** S_B **do**
    if $z^u_{j,i} < \mu^u_i - \mathrm{v}^u_i$ %level 1
      $K^u_{j,i} = b_1$
    else if $\mu^u_i - \mathrm{v}^u_i < z^u_{j,i} < \mu^u_i$ %level 2
      $K^u_{j,i} = b_2$
    else if $\mu^u_i < z^u_{j,i} < \mu^u_i - \mathrm{v}^u_i$ %level 3
      $K^u_{j,i} = b_3$
    else if $z^u_{j,i} > \mu^u_i - \mathrm{v}^u_i$ %level 4
      $K^u_{j,i} = b_4$
    else
      $z^u_{j,i}$ dropped
    end if
  end for
end for

3.3. Performance Parameter

There are four parameters used to determine the performance of our proposed SKG scheme as follows:

1. Pearson correlation coefficient: calculates linear dependency between two RSS data. The resulting value ranges within -1 to 1, where -1 specifies a negative correlation, 0 specifies no correlation, while 1 specifies an absolute correlation [44]. In this paper, we use this parameter to determine the success of the MK method. This success is indicated by an increase in the correlation coefficient of legitimate users. Detailed testing is conducted by comparing the correlation coefficient of the RSS data block measurement results with the pre-process results by using the MK method. From the test results, there will be an increase in the correlation coefficient close to 1 from several data blocks. The closer to 1 the greater the probability of obtaining an identical secret key.
2. Bit disagreement rate (BDR): bit incompatibility of total bits in one RSS data block. This parameter is the first parameter used to determine the success of the CMQ method. In this paper, we make effort to build a simple SKG scheme by eliminating the information reconciliation stage. One of the requirements that must be fulfilled to eliminate this stage is that the obtained BDR must have a value of 0, where the value means the secret key produced is perfectly identical. Therefore, the SKG scheme does not require a correction process. Detailed testing is conducted by comparing the bits from multilevel quantization between two legitimate users. Quantization is carried out on each block of the pre-process RSS data.

3. Key generation rate (KGR): the number of produced bits at one time in the SKG scheme. This parameter is the second parameter used to determine the success of the CMQ method. KGR is obtained by calculating the number of secret key bits that have been successfully generated in a certain period of time. Thus, it can be said that the purpose of these parameters is to determine the speed of the built SKG scheme to acquire the secret key. In accordance with the 802.1x recommendation, the secret key must be refreshed every 1 h [45]. KGR value will meet the requirements if the secret key can be obtained within that time period.
4. Randomness: utilized to determine the randomness of the produced secret key. Testing of the p values of several parameters is conducted using the NIST statistical suite [46]. A secret key will pass the randomness requirements if $p \geq 0.01$. In this paper, we conducted 6 randomness tests out of a total of 15 tests that can be conducted using NIST. This test is selected because the secret key length only meets the requirements of the 6 tests. The remaining tests require very long bits. Even some tests need a bit length $\approx 10^6$. Because we performed randomness testing in each 128-bit secret key (used for AES-128), we merely had to undertake the testing with the 6 tests.

4. Experimental Setup

The SKG scheme is built on 3 Raspberry Pi 3 Type B devices. There are 2 devices that become legitimate users, i.e., Alice and Bob, while the other devices become eavesdroppers (Eve). Each device is equipped with TL-WN722N 802.11 b/g/n wireless card. The operating system used is Linux Raspbian Stretch with the kernel version 4.14.74. RSS data aggregation in the probing channel stage is conducted using Wireshark software. The amount of RSS data collected in both legitimate users and eavesdropper is 4000. In studies on the SKG scheme, Raspberry Pi is often used as a tool for processing RSS measurements so a shared secret key can be obtained [23,47]. The selection of this equipment is based on the ease of programming used because it uses high-level programming, i.e., Phyton, and expansion slots to facilitate connectivity. The ease of connectivity is needed in various IoT applications. Besides the SKG scheme, Raspberry Pi can also be used as part of a chaotic cryptosystem [17]. However, its use is different from the utilization of Raspberry Pi in the SKG scheme which processes all key generation processes. In this research, Raspberry Pi is only used as one of the subsystems that are connected to other devices, namely the digital camera, monitor, and Field-Programmable Gate Array (FPGA). FPGA is a digital IC that is often used to implement digital circuits. The selection of Raspberry Pi is based on the ability to develop graphical interfaces through python, so the mechanism of capture and display of images that will be encrypted/decrypted can be done.

4.1. Experimental Scenarios

There are two experiments to be performed at this paper, i.e., experiment 1 and 2. As seen in Figure 4, experiment 1 was carried out in the line-of-sight (LOS) environment, while Figure 5 shows that experiment 2 was carried out in a non-line-of-sight (NLOS) environment. In the LOS environment, testing was carried out in a room measuring 8.68 $\times$ 6.946 m with a table, chairs, and blackboard in it. Alice moved along the track, while Eve and Bob were motionless with a very close distance of 10 cm. There was no barrier between Alice and Bob. In the NLOS environment, testing was carried out in a sized room measuring 14.72 $\times$ 8 m with tables, chairs and glass cabinets inside. Alice moved along the track with a barrier in the form of a glass cabinet. Eve and Bob were also motionless with a distance of 10 cm. The distance had exceeded half the wavelength of 6.25 cm ($\lambda = c/f = 3.10^8/2.4.10^9 = 12.5$ cm), so Eve would not get the same RSS data.

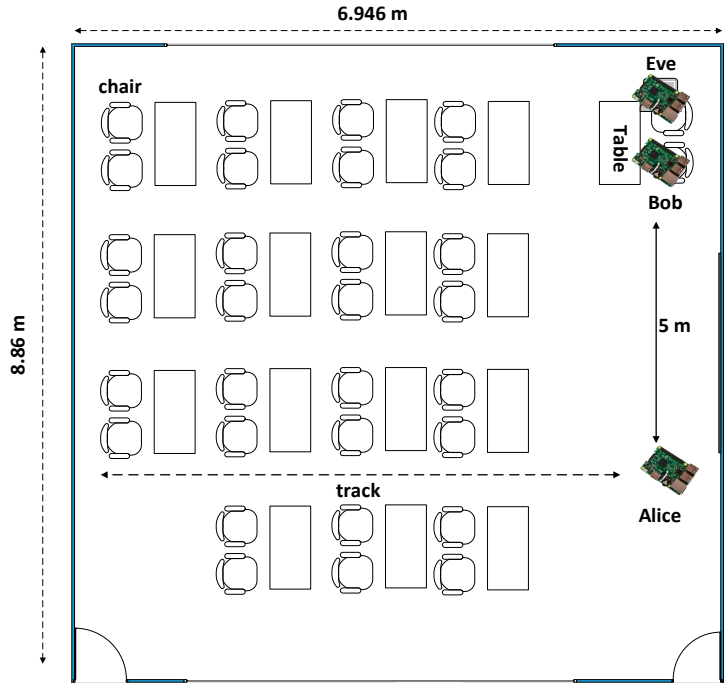


Figure 4. The experimental scenario in the line-of-sight (LOS) environment.

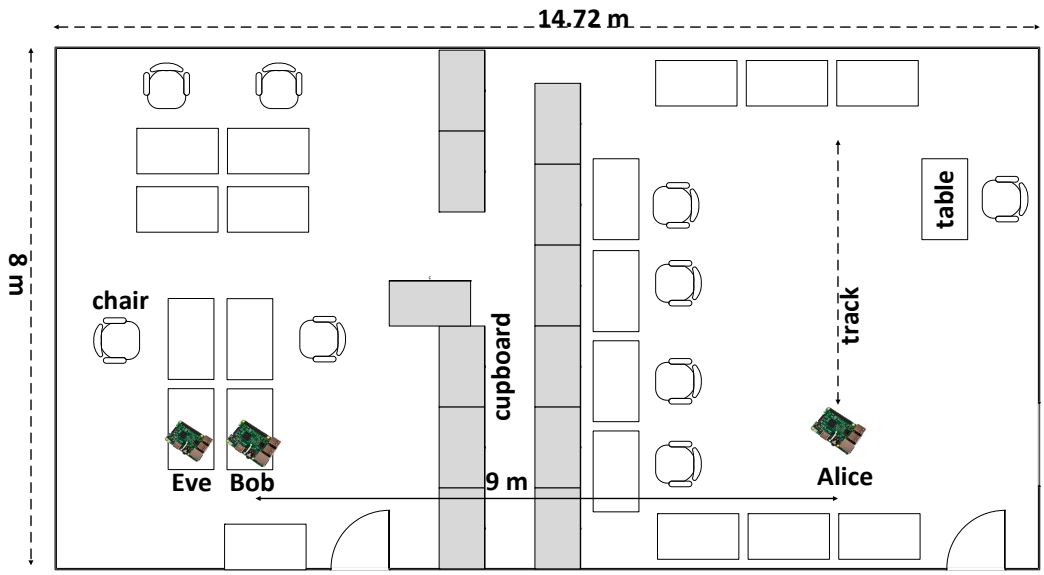


Figure 5. The experimental scenario in the non-line of sight (NLOS) environment.

4.2. Measurement Results

The measurement results show a high correlation coefficient of the RSS data between legitimate users as seen in Table 1. In the LOS environment (Experiment 1) the correlation coefficient of 0.7573 was obtained. Meanwhile, in the NLOS environment (Experiment 2) the correlation coefficient of 0.6988 was obtained. The smaller correlation of RSS data in the NLOS environment indicates that the multipath component found in this environment causes an increase in the difference of the RSS data. The existence of a barrier in the form of cupboard between Alice and Bob causes the RSS data received to come from several paths (multipath), so the signal was weakened. These conditions led to the increasing differences in the RSS data of each user. The correlation coefficient obtained by eavesdroppers is very low (uncorrelated), so we can say that the built SKG scheme has fulfilled the

spatial decorrelation principles, and it is difficult for an eavesdropper to obtain the same secret key as the legitimate user.

Table 1. The correlation coefficient of the measurement result.

Experiment	User	Correlation coefficient
1	Alice and Bob	0.7573
	Alice and Eve	0.0216
	Bob and Eve	0.0153
2	Alice and Bob	0.6988
	Alice and Eve	0.0100
	Bob and Eve	0.0282

Figures 6 and 7 show variations of RSS data in the LOS and NLOS environment. The measurement results in the LOS environment tend to show a better strength signal variation compared to the NLOS environment which is between −25 dBm to −60 dBm. Meanwhile, the strength signal variation in the NLOS environment is between −50 to −75. This occurs because in the LOS environment there is no barrier between Alice and Bob, so the possibility of getting a stronger signal is greater than in the NLOS environment. Therefore, it can be said that the barrier and scatterer in the NLOS environment, cause the weakening of the received signal.

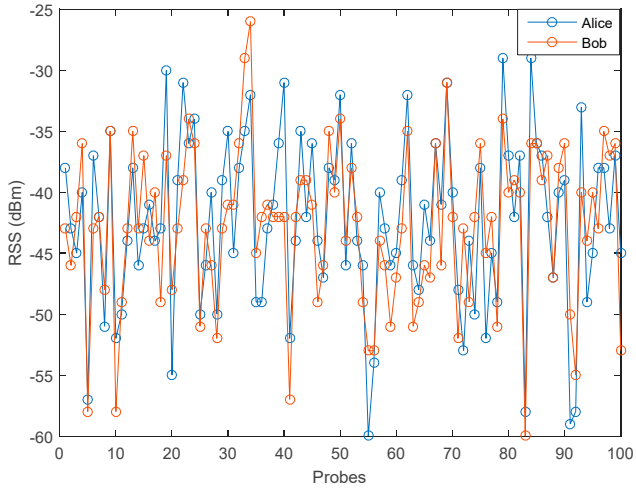


Figure 6. Measurement results in the LOS environment.

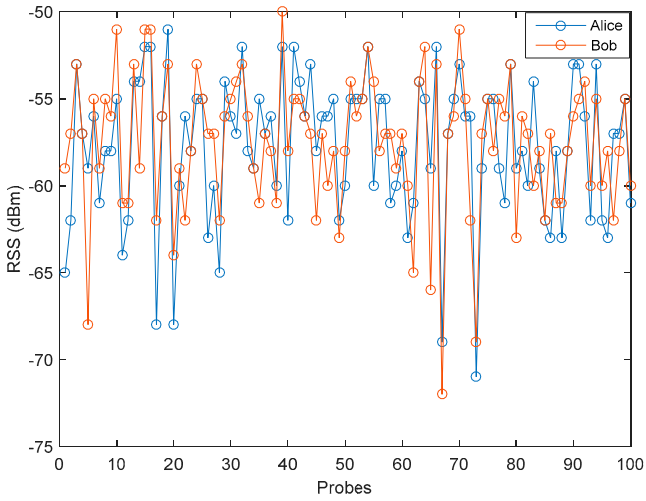


Figure 7. Measurement results in the NLOS environment.

5. Performance Evaluation

In this segment, we assess the achievement of the built SKG scheme by using several predetermined parameters. This evaluation was used to determine the success of the proposed method, namely MK and CMQ. Experimental validation was carried out in two test environments, i.e., the LOS and NLOS environments. The success of the MK method is indicated by the increasing correlation coefficient of a legitimate user. Evaluation is conducted by comparing the correlation coefficient of the RSS data block of the measurement with the pre-process results using the MK method. The more blocks of data with a correlation coefficient of close to 1, the more likely it is to get an identical secret key. The success of the CMQ method is shown by the success of obtaining identical secret keys without requiring an information reconciliation stage. This stage can be omitted if there is a block of RSS data that has BDR with a value of 0 and the success of getting a secret key within the recommended time span of 802.1x [45]. The speed of the SKG scheme to get the secret key in that time period is indicated by the KGR parameter. In addition, we also carry out the NIST test to ensure that the generated secret key has $p \geq 0.01$ to meet randomness requirements.

5.1. Performance Evaluation of the Modified Kalman (MK) Method

In this test, we divided the RSS data into several data blocks, i.e., 64 and 128. The purpose of this data block distribution is to ensure an improvement in the correlation of each data block so as to increase the similarity of the secret key produced. The selection of the amount of RSS data on each block is based on the quantization method used. We used a multilevel quantization method that converts 1 RSS data into 2 bits, so if 1 block contains 64 RSS data, then it will be converted to 128 bits. If 1 block contains 128 RSS data, then it will be converted to 256 bits. Because the length of the secret key used is 128 bits, the data block will be divided into 2 so each block contains 128 bits.

Table 2 demonstrates the achievement of the MK algorithm as opposed to the existing measurement results for all RSS data. The correlation coefficient obtained is the value of the entire RSS data after processing the RSS data for each block by using the MK method. The results of the experiment show that the RSS data distribution into several data blocks gives an increase in a correlation coefficient of the legitimate user in both LOS and NLOS environments. In the NLOS environment, blocks of data containing 64 RSS data resulted in a higher significant improvement in the correlation coefficient compared to the blocks of data containing 128 RSS data. However, there is a decrease in the correlation coefficient in the LOS environment. This condition occurs because of a decrease in the correlation coefficient when processing data using the adopted polynomial regression (Algorithm 1), so when the data were processed using the Modified Kalman Filter (Algorithm 2) there is no improvement in the correlation coefficient even tends to decline. In this paper, we select blocks of data containing 128 RSS data because of the improvement in the correlation coefficient in all environments. Eavesdropper's correlation coefficients also increase, but the results obtained are still far below the correlation coefficient obtained by legitimate users. Therefore, it is still difficult for eavesdroppers to get an identical secret key as legitimate users.

Table 2. Improvement of correlation coefficient by using the modified Kalman (MK) method.

Experiment	User	Measurement Correlation Coefficient	Improvement of the Correlation Coefficient for the Data Block	
			64	128
1	Alice and Bob	0.7573	0.7500	0.8196
	Alice and Eve	0.0216	−0.0062	0.2017
	Bob and Eve	0.0153	0.1657	0.1995
2	Alice and Bob	0.6988	0.7782	0.7667
	Alice and Eve	0.0100	0.3016	0.2922
	Bob and Eve	0.0282	0.3682	0.3876

We conducted a detailed analysis of the improvement in the correlation coefficient of the legitimate user with each block of data containing 128 RSS data as seen in Figure 8. Testing is conducted by comparing the correlation coefficients of each measured block of data with the pre-process results by using the MK method. The results of an experiment in the LOS environment indicate that most measurement data blocks have a correlation coefficient of 0.7. After the pre-process stage, there is a significant increase in the number of data blocks that have a correlation coefficient of 0.9 with a range value between 0.9016 to 0.9996. There are 2 blocks of data that have the correlation coefficients of 0.9993 and 0.9996, so it is possible to obtain an identical secret key from the two blocks of data without requiring the information reconciliation stage.

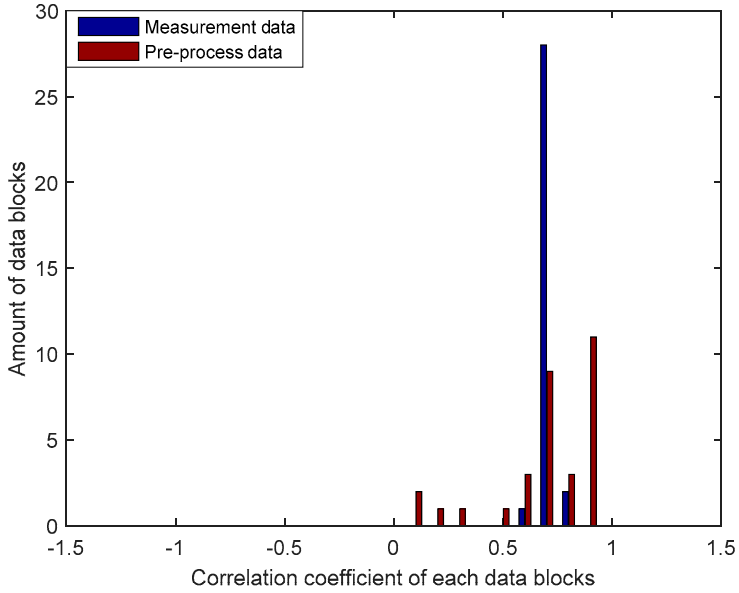


Figure 8. Improvement of the correlation coefficient for each block of data in the LOS environment.

The test results of RSS data for each block in the NLOS environment as seen in Figure 9 also showed an improvement in the correlation coefficient of the pre-processes results when compared with the measured data. From the pre-process results, there are 9 blocks of data that have a correlation coefficient of 0.9 with a range of values between 0.9053 to 0.9976. One block has a correlation coefficient of 0.9976 so it is possible to obtain an identical secret key without requiring an information reconciliation stage. Generally, the MK method produces a better improvement in the correlation coefficient of the pre-process results in the LOS environment. This can be seen from the increasing number of data blocks that have a correlation coefficient of 0.9 when compared to the NLOS environment, so it has a greater probability of producing identical secret keys.

From the overall tests that have been conducted, it can be concluded that our proposed pre-process method, i.e., the MK method, is able to increase the significant correlation coefficient in some data blocks to 0.9. This increase has an effect on the greater the possibility of getting an identical secret key because of the increased similarity of the RSS data block resulting from the pre-processing stage. The increased number of data blocks with the correlation coefficient can reach up to 35.48% in the LOS environment and 29.03% in the NLOS environment. This shows the success of the addition of the MK method in the built SKG scheme since the method was able to increase the reciprocity of measured RSS data.

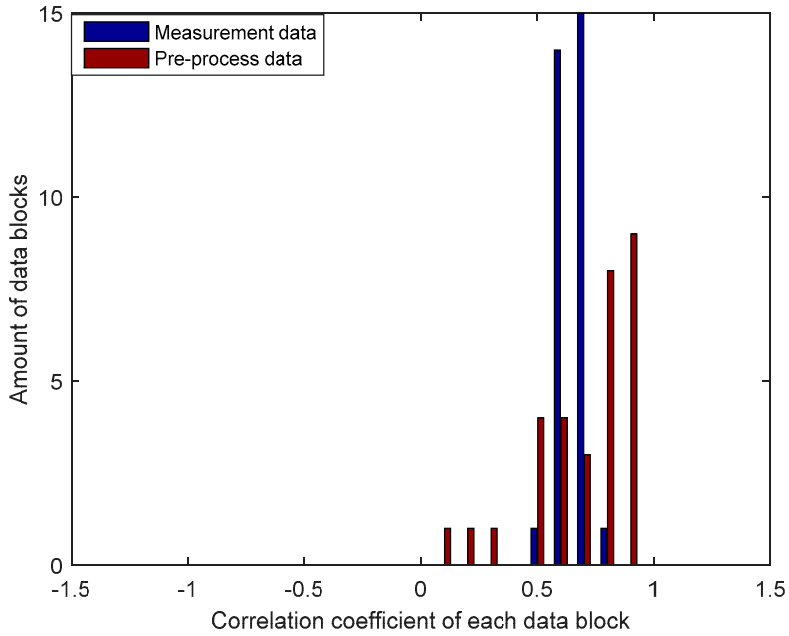


Figure 9. Improvement of the correlation coefficient for each block of data in the NLOS environment.

5.2. Performance Evaluation of the Combined Multilevel Quantization (CMQ) Method

In this segment, we oppose the achievement evaluation between our proposed method, i.e., CMQ and several existing methods/schemes. In our proposed method we utilize RSS data from the pre-process using the MK method z^u as the input to be processed into the initial key K^u. The quantization method used is a multilevel quantization [48] that uses mean μ^u and variance v^u to determine the level of each RSS data. There are 4 existing schemes used as a comparison, i.e., schemes [36,48–50]. Scheme [48] also uses mean and variance to determine the level of each RSS data, but the mean and variance are obtained from blocks of data containing 10 RSS data. The scheme uses RSS data from the pre-process using the existing Kalman as the input to be processed into the initial key. Scheme [49] uses intervals from sorted RSS data, where this scheme uses $N = 2$ values as the number of bits to be extracted at each interval. Scheme [50] uses guard bands in each RSS data interval with values α as guard band comparison ratios with the total RSS data. We select α value of 0.1. The last existing scheme is [36], wherein this scheme is an enrichment of the scheme [48]. Compared to scheme [48] which uses 2 parameters, scheme [36] uses 3 parameters, namely the mean, standard deviation and α as a parameter that will be multiplied by the standard deviation. The α value used in this scheme is 0.01.

Performance evaluation of the SKG scheme is seen from several parameters, namely BDR, KGR, and randomness. BDR testing aims to determine bit incompatibility of total bits in one RSS data block. Since the built SKG scheme does not use the information reconciliation stage, the candidate secret key can be obtained if the BDR value is 0. KGR shows the number of bits produced at one time in the SKG scheme stage. The higher the KGR value is, the faster is the time needed to get the secret key. The randomness parameter aims to determine the level of randomness of the secret key generated. The level of randomness generated can be seen from the significance level α. The higher is the value α generated, the more random the secret key value is. In cryptographic systems, the minimum α value that must be fulfilled is 0.01 ($p \geq \alpha$).

Figure 10 shows the results of the comparison of BDR between our proposed scheme, i.e., CMQ and several existing schemes in the LOS environment. BDR test results of the legitimate user indicate that our proposed scheme is capable of producing 4 identical candidate secret keys without requiring an information reconciliation stage since the BDR value is 0. This condition occurs because of an improvement in the correlation coefficient up to 0.9999 in several data blocks using

the MK method. Increasing the correlation coefficient also increases the similarity of the pre-process RSS data results, thus improving the possibility to obtain an identical secret key without requiring an information reconciliation stage. The test outcomes also present that all of the existing schemes produce the non-identical secret key because all data blocks generate BDR values that exceed 0. Therefore, error correcting techniques are still needed to reconcile information. Figures 11 and 12 show the BDR value between eavesdroppers and legitimate users. Many eavesdropper's blocks of data have different bits with the legitimate user, so there is no BDR value that is worth 0. This shows that the eavesdropper does not get an identical secret key with the legitimate user.

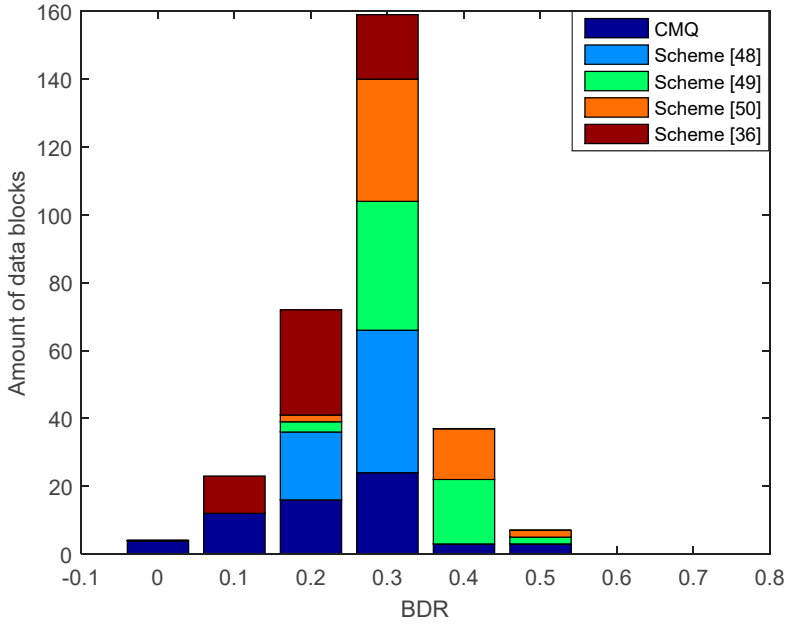


Figure 10. Bit disagreement rate (BDR) of the legitimate user between combined multilevel quantization (CMQ) and several existing schemes in the LOS environment.

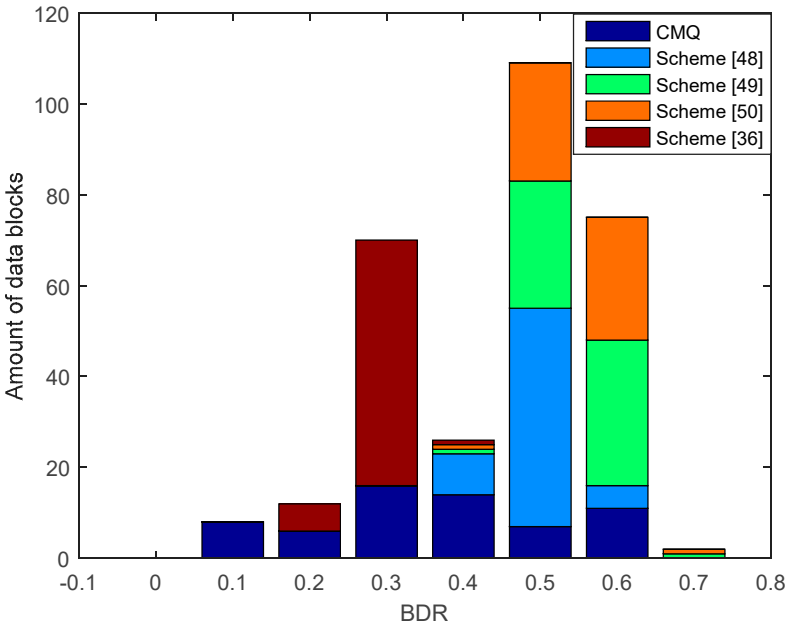


Figure 11. BDR of eavesdropper (Alice–Eve) between CMQ and several existing schemes in the LOS environment.

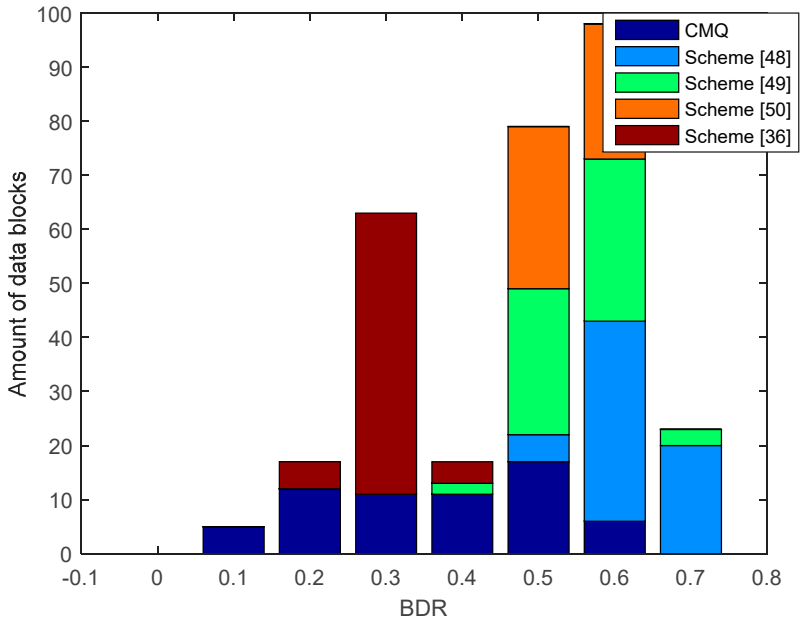


Figure 12. BDR of eavesdropper (Bob–Eve) between CMQ and several existing schemes in the LOS environment.

Figure 13 presents the results of the comparison of BDR between our proposed scheme i.e., CMQ and several existing schemes in the LOS environment. BDR test results of the legitimate user indicate that our proposed scheme is capable of producing 2 identical candidate secret keys without requiring an information reconciliation stage because the BDR value is 0. The number of identical secret keys produced is still less when compared to testing in the LOS environment. This occurs because the overall correlation coefficient in the NLOS environment is still smaller when compared to the LOS environment. Besides, the number of data blocks that have increased the correlation coefficient up to 0.9 is also less when compared to the LOS environment. The test outcomes also show that all of the existing schemes produce the non-identical secret key because all data blocks generate BDR values that exceed 0. Therefore, error correcting techniques are still needed to reconcile the information. Overall, it can be appreciated that our scheme is able to produce a simpler SKG scheme compared to the existing scheme. This is indicated by the ability to obtain identical secret keys without going through the information reconciliation stage. Figures 14 and 15 show BDR between legitimate users and eavesdroppers. The results of the tests indicate that there is no BDR that has a value of 0, so the eavesdropper does not get an identical secret key with the legitimate user. It shows that our proposed scheme is also able to warrant the security of the secret key generated by the legitimate user. The same with the testing in the LOS environment, the BDR values obtained by eavesdropper in the NLOS environment range between 0.5 and 0.7.

The next tested parameter is randomness by using the NIST statistical suite. There are 6 tests are carried out to ensure the randomness of a candidate secret key, which is generated from the privacy amplification stage. We provide a brief explanation of the objectives of each test as follows [46]. The approximate entropy test is used to determine the frequency of all possible overlapping bit patterns in a key sequence. The purpose of the frequency (monobit) test is to determine whether the proportions of 0 and 1 in a key sequence are the same. A frequency test within a block is used to determine whether the proportion of 1 in one block is around half a block. A run test is used to determine whether the oscillations of 1 and 0 of a key sequence are too fast or slow compared to a random sequence. A longest-run-of-ones in a block test determines whether the length of the 1 from the test sequence is consistent with the expected length of 1 from the random sequence. Cumulative sums test is used to determine whether the cumulative number of parts of the sequence is too large or too small for the

expected cumulative number of a random sequence. Cumulative sums (forward) test use mode 0 by changing 0 to −1, while cumulative sums (reverse) test use mode 1 by changing 1 to +1.

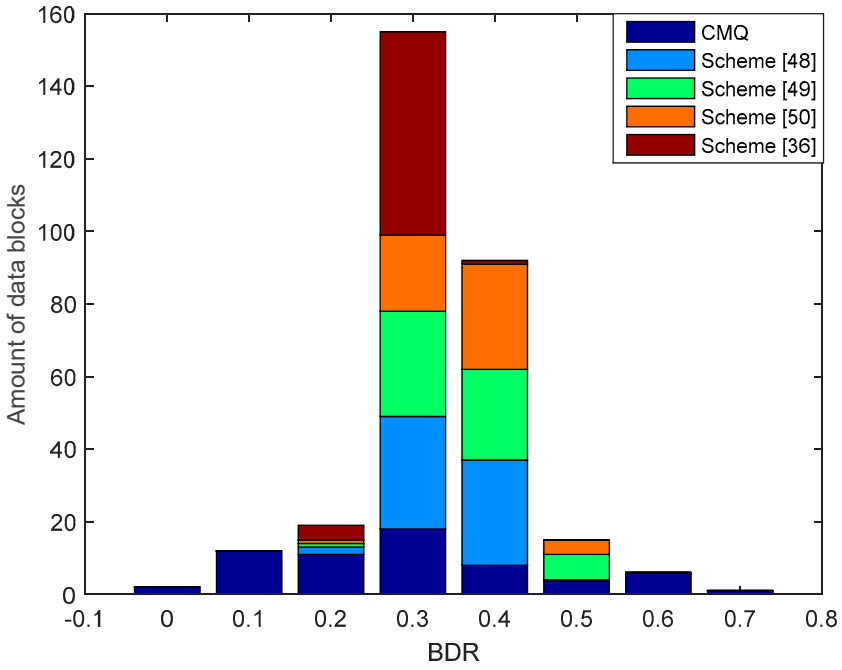


Figure 13. BDR of the legitimate user between CMQ and several existing schemes in the NLOS environment.

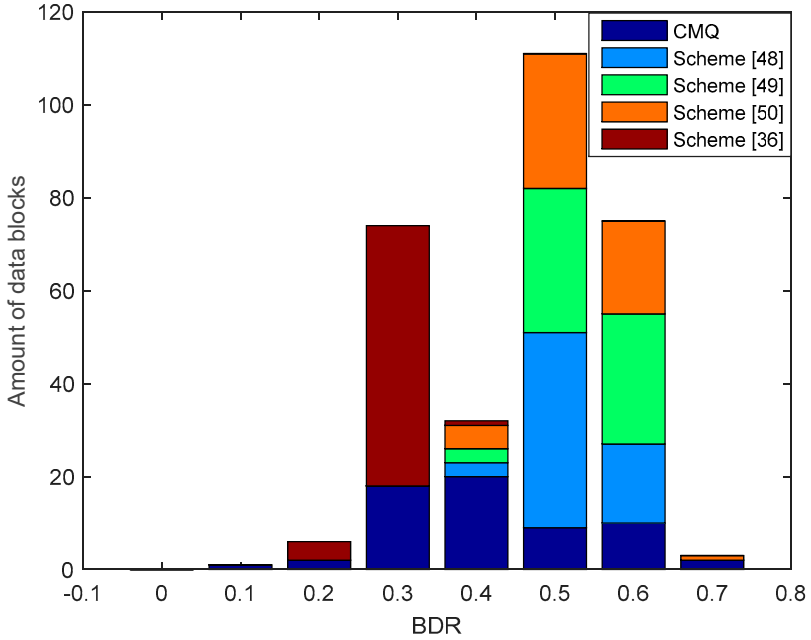


Figure 14. BDR of eavesdropper (Alice–Eve) between CMQ and several existing schemes in the NLOS environment.

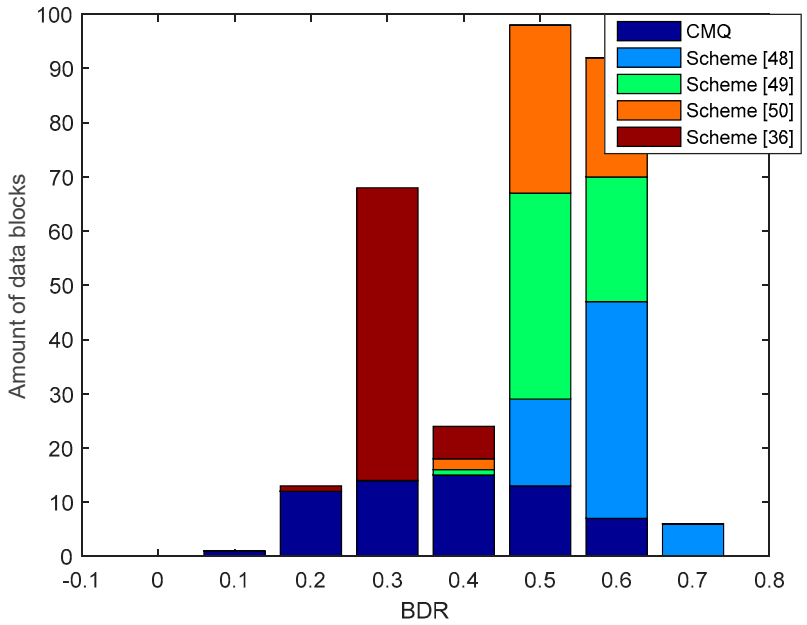


Figure 15. BDR of eavesdropper (Bob–Eve) between CMQ and several existing schemes in the NLOS environment.

From the test outcomes presented in Table 3, it can be ensured that all secret keys fulfill the randomness requirements with p value exceeding 0.01 for all types of tests. The priority of the selected key sequence as the shared secret key is key 4, key 3, key 1, and key 2. This selection is based on the approximate value of each key. If the first priority key failed in the verification stage, then the next key utilized as the secret key is the second priority, i.e., key 3. Generally, key 4 has a greater value for each type of test when compared to the other key. The approximate entropy test results show p values up to 0.980078. The higher the value of the test shows the higher the irregularity of the resulting bit so the resulting key sequence is more random. The highest p value of the frequency (monobit) test is 0.859684. The higher the test results show the proportions of 1 and 0 are almost the same or close to $\frac{1}{2}$, so the distribution can be obtained in accordance with the requirements of randomness. On the frequency test within a block, the highest value is obtained on key 1 which is equal to 0.529508. This shows that key 1 has a proportion of 1, which is closer to half the block, so it is as expected on the randomness assumption. The results of the key 1 run test also show a greater p value compared to the other keys which are equal to 0.920091. These results indicate that the oscillations occurring in the key are faster when compared to other keys. The longest-run-of-ones in a block test shows that key 4 has a length of 1 that is more invariant with the expected length of 1 from a random key set. The results of cumulative sums testing (forward and backward) indicate that the cumulative number of produced keys corresponds to the expected cumulative number of a random sequence. Too many 1 or 0 at the beginning of the key sequence (mode 0) and at the end of the key sequence (mode 1) will result in the p value being too small, so it does not meet the randomness requirements.

The results of the NIST statistical suite randomization test in the NLOS environment are shown in Table 4. There are 2 keys with the first priority as a shared secret key, i.e., key 1 with an approximate entropy value of 0.916730. If the verification stage fails, key 2 can be used as an alternative key. Overall, it can be seen that the produced secret keys have fulfilled the randomness requirements because the p value has exceeded 0.01. Key 1 shows a higher irregularity compared to key 2. This is indicated by a higher p value of key 1 when compared to key 2 in the approximate entropy test. To fulfill randomization requirements, the key obtained must have a proportion of 1 and 0 that are close to $\frac{1}{2}$. The results of testing frequency (monobit) indicate that key 1 has a proportion of 1 and 0 that are closer to $\frac{1}{2}$, so it has a higher p value than key 2. The same results were also obtained in testing the frequency test within a block, where key 1 has a proportion of 1 which is closer to half the block so it has a higher

value than key 2. In run testing it appears that key 2 oscillates faster than key 1, besides that key 2 also has a length of 1 which is more consistent with the expected length of 1 from a random key sequence. The same results were also obtained in the frequency test within a block, where key 1 has a proportion of 1 which is closer to half the block so it has a higher p value than key 2. In run testing it appears that key 2 oscillates faster than key 1, besides that key 2 also has a length of 1 which is more invariant with the expected length of 1 from the random key sequence. In cumulative sums testing it appears that key 2 has too many 1 or 0 at the beginning and at the end of the key sequence, so the resulting p value is smaller than key 1. Overall, the results of the NIST testing in the LOS and NLOS environment show p values that have exceeded 0.01. It means that the generated secret keys have meets the randomness requirements with confidence level reaching up to 99%.

Table 3. National Institute of Standards and Technology (NIST) test in the LOS environment.

NIST Test	p Value			
	Key 1	**Key 2**	**Key 3**	**Key 4**
Approximate Entropy	0.594945	0.012247	0.841149	0.980078
Frequency (Monobit)	0.288844	0.376759	0.723674	0.859684
Frequency Test within a Block	0.529508	0.079139	0.323897	0.418642
Runs	0.920091	0.188673	0.382288	0.721539
Longest-Run-of-Ones in a Block	0.390869	0.508286	0.495995	0.876990
Cumulative Sums (forward)	0.314554	0.737518	0.654761	0.892023
Cumulative Sums (backward)	0.431439	0.431439	0.949266	0.818770

Table 4. NIST test in the NLOS environment.

NIST Test	p Value	
	Key 1	**Key 2**
Approximate Entropy	0.916730	0.182499
Frequency (Monobit)	0.595883	0.021556
Frequency Test within a Block	0.756805	0.635908
Runs	0.463206	0.502046
Longest-Run-of-Ones in a Block	0.151703	0.202941
Cumulative Sums (forward)	0.892023	0.026657
Cumulative Sums (backward)	0.431439	0.034021

KGR is a performance parameter that aims to determine the speed of the SKG scheme built to obtain the secret key. The KGR test results as shown in Table 5 showed a higher KGR result in the LOS environment, i.e., 0.92 bps so that it took approximately 2.32 min to get a 128-bit secret key that would be utilized to encrypt the message using the AES-128 method. In accordance with the recommendations of 802.1x, the secret key must be refreshed every 1 h so that the SKG scheme built has fulfilled the recommendation [45]. This is because the secret key generated is still less than 1 h, which is 2.32 min. The test results in the NLOS environment also still fulfill the requirements for the refresh key, because the time needed to obtain the 128-bit secret key is 4.74 min. The average of approximate entropy in both test environments ranges from 0.5 to 0.6, with a lower average of approximate entropy obtained in the NLOS environment. In the built SKG scheme, we eliminate the information reconciliation stage. The total computation time needed is 18.3 s (LOS) and 18.6 s (NLOS), while the information reconciliation stage using BCH (31.6) requires computing time up to 7.139 s (LOS) and 7.068 s (NLOS). We assume that the scheme was tested in good network conditions. The elimination of these stages can reduce computational time to 39.1% (LOS) and 38% (NLOS). If network conditions are poor, then the possibility of decreasing computational time is also greater than good network conditions because of the longer time needed to exchange parity bits.

Table 5. Key generation rate (KGR) in the LOS and NLOS environment.

Experiment	KGR (bps)	Average of Approximate Entropy
1	0.92	0.607105
2	0.45	0.5496145

From the overall test to determine the success of the CMQ method, it can be concluded that our proposed method is able to produce a simple SKG scheme by eliminating information reconciliation stage. This condition is indicated by the production of several blocks of data that have a BDR value of 0. The results of tests carried out in the LOS and NLOS environments also show that the time required to obtain the secret key is far below 1 h which is 2.32 min (LOS) and 4.74 min (NLOS) with KGR values reaching 0.92 bps (LOS) and 0.45 bps (NLOS). Therefore, it can be said that the built SKG scheme has been able to meet the recommendations of 802.1x because the secret key could be refreshed under 1 h. Reducing the stage of information reconciliation also affects the decrease in computational and communication cost.

6. Conclusions

In this paper, we offer a new pre-process method, i.e., modified Kalman (MK), and perform a combination of the method with a multilevel quantization, i.e., combined multilevel quantization (CMQ). We also carried out experimental validation in two test environments i.e., LOS and NLOS. The results of the tests conducted indicate that the addition of the MK method to the built SKG scheme was able to increase the number of data blocks that have a correlation coefficient above 0.9 to 35.48% in the LOS environment and 29.03% in the NLOS environment. Therefore, the probability of getting an identical secret key is also increasing. Furthermore, the CMQ method was able to simplify the stages of the built SKG scheme because the scheme was able to produce several identical secret keys without requiring an information reconciliation stage with KGR reaching 0.92 bps in the LOS environment and 0.45 bps in the NLOS environment. The results of the tests conducted also showed that reducing the information reconciliation stage could reduce computational and communication time to 39.1% in the LOS environment and 38% in the NLOS environment. In addition, the secret key produced has passed 6 randomness tests with p values exceeding 0.01 so it can fulfill the requirements for randomization of cryptosystems with confidence levels reaching up to 99%.

Author Contributions: Conceptualization, M.Y., W. and S.; Methodology, M.Y., W. and S.; Software, M.Y., W. and S.; Validation, M.Y., W. and S.; Formal Analysis, M.Y, W. and S.; Investigation, M.Y and W.; Resources, M.Y.; Data curation, M.Y.; Writing—original draft preparation, M.Y.; Writing—review and editing, M.Y., W. and S.; Visualization, M.Y, W. and S.; Supervision, W. and S.; Project Administration, M.Y, W. and S.; Funding Acquisition, M.Y, W. and S.

Funding: This research was funded by the Ministry of Research, Technology, and Higher Education through the scholarship program BUDI-DN by the LPDP of the Ministry of Finance of the Republic of Indonesia to Mike Yuliana.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Lee, E.; Gerla, M.; Pau, G.; Lee, U. Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. *Int. J. Distrib. Sens. Netw.* **2016**, *12*, 1–13. [CrossRef]
2. Mora, H.; Gil, D.; Szymanski, J. An IoT-Based Computational Framework for Healthcare Monitoring in Mobile Environments. *Sensors* **2017**, *17*, 2302. [CrossRef]
3. Diaz-cacho, M.; Delgado, E.; Falcon, P.; Barreiro, A. IoT integration on Industrial Environments. In Proceedings of the IEEE World Conference on Factory Communication Systems (WFCS), Palma de Mallorca, Spain, 27–29 May 2015.
4. Yadav, V.; Borate, S. Smart Home Automation using Virtue of IoT. In Proceedings of the International Conference for Convergence in Technology (I2CT), Mumbai, India, 7–9 April 2017; pp. 313–317.

5. Zhang, J.; Duong, T.Q.; Woods, R.; Marshall, A. Securing wireless communications of the internet of things from the physical layer, an overview. *Entropy* **2017**, *19*, 420. [CrossRef]
6. Margelis, G.; Fafoutis, X.; Oikonomou, G.; Piechocki, R.; Tryfonas, R.; Thomas, P. Efficient DCT-based secret key generation for the Internet of Things. *Ad Hoc Netw.* **2018**, 1–11. [CrossRef]
7. Yener, A.; Ulukus, S. Wireless Physical-Layer Security: Lessons Learned from Information Theory. *Proc. IEEE* **2015**, *103*, 1814–1825. [CrossRef]
8. Carbajal-gomez, V.H.; Tlelo-cuautle, E.; Mu, J.M.; Gerardo, L.; Fraga, D.; Sanchez-lopez, C.; Fernandez-fernandez, F.V. Optimization and CMOS design of chaotic oscillators robust to PVT variations: INVITED. *Integration* **2018**. [CrossRef]
9. Lee, C. A simple key agreement scheme based on chaotic maps for VSAT satellite communications. *Int. J. Satell. Commun. Netw.* **2013**, *31*, 177–186. [CrossRef]
10. Lin, C.L.T.; Tsai, C. A new authenticated group key agreement in a mobile environment. *Ann. Telecommun.* **2009**, *64*, 735–744.
11. Menezes, A.J.; Oorschot, P.C.V.; Vanstone, S.A. *Handbook of Applied Cryptography*, 1st ed.; CRC Press: Boca Raton, FL, USA, 1996.
12. Stallings, W. *Cryptography and Network Security: Principles and Practice*, 6th ed.; Prentice Hall Press: Upper Saddle River, NJ, USA, 2013.
13. Cheng, C.; Lu, R.; Petzoldt, A.; Takagi, T. Securing the Internet of Things in a Quantum World. *IEEE Commun. Mag.* **2017**, *55*, 116–120. [CrossRef]
14. Padamvathi, V.; Vardhan, B.V.; Krishna, A.V.N. Quantum Cryptography and Quantum Key Distribution Protocols: A Survey. In Proceedings of the 6th International Conference on Advanced Computing (IACC), Bhimavaram, India, 27–28 February 2016; pp. 556–562.
15. Wang, Y.; She, K.A. practical quantum public-key encryption model. In Proceedings of the 3rd International Conference on Information Management (ICIM), Chengdu, China, 21–23 April 2017; pp. 367–372.
16. Zhang, J.; Duong, T.Q.; Marshall, A.; Woods, R. Key Generation from Wireless Channels: A Review. *IEEE Access* **2016**, *4*, 614–626. [CrossRef]
17. Rodríguez-orozco, E.; Garcí-guerrero, E.; Inzunza-gonzalez, E.; López-bonilla, O.R.; Flores-vergara, A.; Cádenas-valdez, J.R.; Tlelo-Cuautle, E. FPGA-based Chaotic Cryptosystem by Using Voice Recognition as Access Key. *Electronics* **2018**, *7*, 414.
18. Sun, L.; Du, Q.A. Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy* **2018**, *20*, 730. [CrossRef]
19. Zenger, C.T.; Zimmer, J.; Pietersz, M.; Posielek, J.-F.; Paar, C. Exploiting the Physical Environment for Securing the Internet of Things. In Proceedings of the New Secur. Paradig, Work (NSPW), Twente, The Netherlands, 8–11 September 2015; pp. 44–58.
20. Pecorella, T.; Brilli, L.; Mucchi, L. The Role of Physical Layer Security in IoT: A Novel Perspective. *Indormation* **2016**, *7*, 49. [CrossRef]
21. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
22. Zhang, J.; Woods, R.; Duong, T.Q.; Marshall, A.; Ding, Y.; Huang, Y.; Xu, Q. Experimental Study on Key Generation for Physical Layer Security in Wireless Communications. *IEEE Access* **2016**, *4*, 4464–4477. [CrossRef]
23. Guillaume, R.; Winzer, F.; Zenger, C.T.; Paar, C.; Czylwik, A. Bringing PHY-based key generation into the field: An evaluation for practical scenarios. In Proceedings of the 82nd 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, USA, 6–9 September 2015.
24. Li, G.; Hu, A.; Sun, C.; Zhang, J. Constructing Reciprocal Channel Coefficients for Secret Key Generation in FDD Systems. *IEEE Commun. Lett.* **2018**. [CrossRef]
25. Peng, L.; Li, G.; Zhang, J.; Woods, R.; Liu, M.; Hu, A. An Investigation of Using Loop-back Mechanism for Channel Reciprocity Enhancement in Secret Key Generation. *IEEE Trans. Mob. Comput.* **2018**. [CrossRef]
26. Kreiser, D.; Dyka, Z.; Kornemann, S.; Wittke, C.; Kabin, I.; Stecklina, O.; Langendoerfer, P. On Wireless Channel Parameters for Key Generation in Industrial Environments. *IEEE Access* **2017**. [CrossRef]
27. Van Torre, P. Channel-Based Key Generation for Encrypted Body-Worn Wireless Sensor Networks. *Sensors* **2016**, *16*, 1453. [CrossRef]

28. Yuliana, M.; Wirawan; Suwadi. Performance evaluation of the key extraction schemes in wireless indoor environment. In Proceedings of the International Conference on Signals and Systems (ICSigSys), Sanur, Indonesia, 16–18 May 2017; pp. 138–144.
29. Castel, T.; Van Torre, P.; Rogier, H. RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes. In Proceedings of the International Conference on Military Communications and Information Systems (ICMCIS), Brussels, Belgium, 23–24 May 2016.
30. Liu, Y.; Draper, S.C.; Sayeed, A.M. Exploiting Channel Diversity in Secret Key Generation from Multipath Fading Randomness. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1484–1497. [CrossRef]
31. Marino, F.; Paolini, E.; Chiani, M. Secret key extraction from a UWB channel: Analysis in a real environment. In Proceedings of the IEEE International Conference on Ultra-WideBand (ICUWB), Paris, France, 1–3 September 2014; pp. 80–85.
32. Cheng, L.; Zhou, L.; Seet, B.-C.; Li, W.; Ma, D.; Wei, J. Efficient Physical-Layer Secret Key Generation and Authentication Schemes Based on Wireless Channel-Phase. *Mob. Inf. Syst.* **2017**, *2017*, 1–13. [CrossRef]
33. Jiang, Y.; Hu, A.; Huang, J. A lightweight physical-layer based security strategy for Internet of things. *Clust. Comput.* **2018**. [CrossRef]
34. Ambekar, A.; Hassan, M.; Schotten, H.D. Improving channel reciprocity for effective key management systems. In Proceedings of the International Symposium on Signals, Systems and Electronics (ISSSE), Postdam, Germany, 3–5 October 2012; pp. 1–4.
35. Zhan, F.; Yao, N. Efficient key generation leveraging wireless channel reciprocity and discrete cosine transform. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 2701–2722.
36. Yuliana, M.; Wirawan; Suwadi. Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment. *Int. J. Comm. Netw. Inf. Secur.* **2017**, *9*, 474–483.
37. Ambekar, A.; Kuruvatti, N.; Schotten, H.D. Improved method of secret key generation based on variations in wireless channel. In Proceedings of the International Conference on Systems, Signals and Image Processing (IWSSIP), Vienna, Austria, 11–13 April 2012; pp. 60–63.
38. Zhan, F.; Yao, N.; Gao, Z.; Yu, H. Efficient key generation leveraging wireless channel reciprocity for MANETs. *J. Netw. Comput. Appl.* **2018**, *103*, 18–28. [CrossRef]
39. McGuire, M. Channel Estimation for Secret Key Generation. In Proceedings of the International Conference on Advanced Information Networking and Applications, Victoria, BC, Canada, 13–16 May 2014; pp. 490–496.
40. Zenger, C.T. Physical–Layer Security for the Internet of Things. Ph.D. Thesis, Ruhr-University Bochum, Bochum, Germany, 30 January 2017.
41. Carter, J.L.; Wegman, M.N. Universal Classes of Hash Functions. *J. Comput. Syst. Sci.* **1979**, *18*, 143–154. [CrossRef]
42. Publication, F. Archived Publication Secure Hash Standard. *Public Law* **1987**, *2*, 100–235.
43. Zhao, J.; Xi, W.; Han, J.; Tang, S.; Li, X.; Liu, Y.; Gong, Y.; Zhou, Z. Efficient and Secure Key Extraction using CSI without Chasing down Errors. *arXiv* **2012**, arXiv:1208.0688.
44. Ali, S.T.; Sivaraman, V.; Ostry, D. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2763–2776. [CrossRef]
45. Moore, T. *IEEE 802.11-01/610r02: 802.1.x and 802.11 Key Interactions*; Technical Report; Microsoft Research, 2001.
46. NIST. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Available online: http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501 (accessed on 8 January 2019).
47. Lopez, A.B. Physical Layer Key Generation for Wireless Communication Security in Automotive Cyber-Physical Systems. Ph.D. Thesis, University of California, Irvine, CA, USA, 2017.
48. Ambekar, A. Exploiting Radio Channel Aware Physical Layer Concepts. Ph.D. Thesis, Ruhr-University Bochum, Bochum, Germany, 5 October 2015.
49. Kai, Z.; Wu, D.; An, C.; Mohapatra, P. Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks. In Proceedings of the International Conference on IEEE INFOCOM, San Diego, CA, USA, 14–19 March 2010; pp. 1–9.

50. Premnath, S.N.; Jana, S.; Croft, J.; Gowda, P.L.; Clark, M.; Kasera, K.S.; Patwari, N.; Krishnamurthy, S.V. Secret key extraction from wireless signal strength in real environments. *IEEE Trans. Mob. Comput.* **2013**, *12*, 917–930. [CrossRef]

sensors

MDPI

Article

An Efficient Key Generation for the Internet of Things Based Synchronized Quantization

Mike Yuliana [1,2,*], Wirawan [1] and Suwadi [1]

[1] Department of Electrical Engineering, Faculty of Electrical Technology, Institut Teknologi Sepuluh Nopember, Jalan Raya ITS, Keputih, Sukolilo, Surabaya 60111, Indonesia; wirawan@ee.its.ac.id (W.); suwadi@ee.its.ac.id (S.)

[2] Department of Electrical Engineering, Politeknik Elektronika Negeri Surabaya (PENS), Jalan Raya ITS, Keputih, Sukolilo, Surabaya 60111, Indonesia

* Correspondence: mieke@pens.ac.id or mike16@mhs.ee.its.ac.id; Tel.: +62-812-1746-4666

Received: 9 May 2019; Accepted: 11 June 2019; Published: 13 June 2019

Abstract: One solution to ensure secrecy in the Internet of Things (IoT) is cryptography. However, classical cryptographic systems require high computational complexity that is not appropriate for IoT devices with restricted computing resources, energy, and memory. Physical layer security that utilizes channel characteristics is an often used solution because it is simpler and more efficient than classical cryptographic systems. In this paper, we propose a signal strength exchange (SSE) system as an efficient key generation system and a synchronized quantization (SQ) method as a part of the SSE system that synchronizes data blocks in the quantization phase. The SQ method eliminates the signal pre-processing phase by performing a multi-bit conversion directly from the channel characteristics of the measurement results. Synchronization is carried out between the two authorized nodes to ensure sameness of the produced keys so it can eliminate the error-correcting phase. The test results at the IoT devices equipped with IEEE 802.11 radio show that SSE system is more efficient in terms of computing time and communication overhead than existing systems.

Keywords: Internet of Things; signal strength exchange system; synchronized quantization

1. Introduction

Today the Internet of Things (IoT) has become a part of our activities with many interconnected things that can be controlled by the internet [1–5]. This condition results in the emergence of new security threats that opens opportunities for third parties to access and obtain confidential information. Most of these things are connected using radio technology which creates communication become susceptible to tapping [6–9]. Many classic security services are realized in the upper Open System Interconnection (OSI) layers, for example, encryption schemes based on key distribution and computational complexity [10,11]. The scheme requires high computational complexity so it is not suitable for IoT devices that have limited computing resources, energy, and memory.

Several studies have focused on security systems from devices with restricted resources and lightweight cryptographic to resolve this issue. One solution is to propose chaotic cryptosystem by optimizing and designing complementary metal-oxide-semiconductor (CMOS) that is connected with chaotic oscillators so that it can be developed in various communication security applications of IoT devices [12,13]. The other interesting solution of lightweight cryptographic is a key generation system that generates an encryption key by using the channel characteristics of the measurement results [14–18]. The system utilizes the principle of reciprocity from electromagnetic propagation which shows that the channel characteristics obtained by the sender and receiver will be the same if the measurement is carried out within coherence time. Some studies use the received signal strength

(RSS) as one of the characteristics of radio channels [19–23]. These channel characteristics are the most available characteristics in wireless devices with various standards, i.e., Bluetooth, IEEE 802.15.4, and IEEE 802.11.

The principle of channel reciprocity as the basis of key generation shows the similarity of the produced channel characteristics from both users. In reality, however, most wireless devices work by alternating measurements of channel characteristics. This condition results in a decrease similarity of channel characteristics due to non-simultaneous measurements and wireless devices noise. Several studies have attempted to improve the similarity of produced channel characteristics by appending the signal pre-processing phase after the measurement process [24–29]. The addition of this phase is proven to be able to raise the similarity of the channel characteristics as indicated by an increase in the correlation coefficient value. The higher the correlation coefficient value of the channel characteristics, the more likely it is to get the same key between the two users. The weakness of the research is that there is still a possibility of different key between the two users so the error-correcting phase is needed to create an equal key. The more the key bits to be corrected then the longer the computing time is needed to make corrections. This phase also increases the communication time between two users due to the exchange of parity bits.

Some studies [30,31] seek to overcome this problem by modifying the existing signal pre-processing phase. The phase is modified by dividing the measurement data into several blocks of data. Each data block will be pre-processed using the existing signal pre-processing method. Another study [32] modified the signal pre-processing phase by combining the Polynomial Regression method with the modified Kalman Filter. The phase is also carried out in each block of measurement data. The results of the performed tests indicate that the use of modified signal pre-process phase is able to produce the same key bits without going through the error correcting phase. However, the signal pre-processing phase requires high computing time because it is conducted for each data block. The more the data amount is, then higher computing time is needed. The frequently parameters for determining the success of the built key generation system are the correlation coefficient, key discrepancy rate, key synchronized rate, and irregularity. The correlation coefficient is used to determine the increasing similarity of the produced channel characteristics. The key synchronized rate is used to specify the number of key bits produced during the duration of the key generation system communication. The duration time of key generation includes the measurement time of channel characteristics, the computation time of each phase and the communication/synchronization time between the two users. Communication/synchronization time obtained if there is an exchange of information between the two users. Phases that often require synchronization are error correcting and privacy amplification phases. The more information sent, the higher the synchronization time needed so the duration of the key generation will also be longer. The higher the duration of communication, the lower the key synchronized rate obtained. The key discrepancy rate is used to specify the number of key bits that are different from the two users. The irregularity is used to determine randomness of key bits generated using the National Institute of Standards and Technology (NIST) test. Some studies on the key generation system for IoT devices [6,33,34] also focus on using these parameters to determine the performance of the built key generation system. The parameters of performance in IoT devices shall be added with computing time and communication overhead that will show the efficiency of the system. The lower the computing time and communication overhead the more efficient the system is, so it is suitable to be implemented on devices with limited resources.

In this paper, we propose an efficient key generation design without the signal pre-processing and error-correcting phase so it can reduce computing time and communication overhead. The details on the two contributions made in this paper will be abbreviated as follows. Firstly, we propose a new quantization method i.e., synchronized quantization (SQ) as a part of the signal strength exchange (SSE) system. The method utilizes the mean, standard deviation and a parameter as the standard deviation dividing parameter. The bits conversion results of the SQ method are then divided into several blocks, each containing 3 bits. The bits taken as key extraction are the three bits totaling 0

or 3. In this paper, we synchronize key bits between the two users by sending the wasted index of blocks. The synchronization system is able to produce the same key bits without going through the signal pre-processing and error-correcting phases. Compared to the previous system, the performance evaluations of the proposed system show faster computing time and lower communication overhead. Secondly, we validate the performance of the SSE system in two real indoor environment scenarios, i.e., unobstructed and obstacles scenarios. Performance validation is conducted by using several performance parameters, i.e., key synchronized rate (KSR), key discrepancy rate (KDIR), irregularity, computing time, and communication overhead.

The rest of this paper is arranged as follows. Section 2 describes in detail about the introduction of key generation models and principle. Section 3 provides an overview of existing key generation system. Section 4 explains in detail about the proposed key generation system, i.e., the SSE System. Section 5 discusses the implementation and performance evaluation of the SSE key generation system. Section 6 summarizes the performance of the built key generation system.

2. Key Generation Model and Principle

In this section, we explain the key generation model and principle. The key generation model is used to indicate the involved node/user and the type of attack from the attacker. The principle key generation explains the three principles used in key generation systems.

2.1. Key Generation Model

There are three nodes involved in this paper Alice (A), Bob (B) and Eve (E) as seen in Figure 1. Authorized nodes are A and B, while an unauthorized node is E. A and B conduct the measurement process to get the channel characteristics y_A dan y_B. Based on the principle of channel reciprocity, authorized nodes will get almost the same or identical channel characteristics measurement results $(y_A \approx y_B)$ if the measurement were performed within coherence time [35]. E as an unauthorized node listens to all the probing processes so it will get the channel characteristics from A and B such as y_E and $y_{E'}$. In this paper, there are three assumptions that will be used for the node E. The first assumption E can listen to all communications made by authorized nodes. In addition, the distance of E is also more than $\frac{1}{2}$ wavelength from the authorized nodes so the received channel characteristics will not correlate with the produced channel characteristics from the authorized nodes $(y_E \neq y_A, y_{E'} \neq y_B)$. The second assumption E is a passive tapper, so it will not attack the communications made by authorized nodes. The third assumption E knows all the algorithms used by authorized nodes.

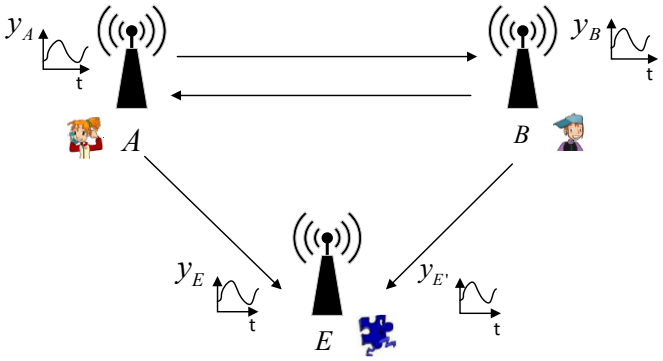


Figure 1. Key generation model.

2.2. Key Generation Principle

The three principles used in key generation systems include channel reciprocity, temporal variation, and spatial decorrelation [36]. The principle of channel reciprocity shows that channel characteristics are measured by authorized nodes and they will be the same if measured simultaneously. However, most wireless devices have limited capabilities so they are not able to take measurements simultaneously.

This condition results in the nonidentical channel characteristics between the two authorized nodes. The value of the channel reciprocity of both authorized nodes can be measured by Equation (1). The principle of temporal variation can be obtained if there is a movement of the sender or recipient node and other things in the observation area. The movement of objects and nodes can affect the level of randomness of the produced channel characteristics. The higher the level of randomization, the more difficult it is for tappers to get the same key as the authorized nodes. The last principle the spatial decorrelation is very important to determine the security of the built key generation system. In this principle, the distance of the unauthorized node that is more than $\frac{1}{2}$ wavelengths will get uncorrelated channel characteristics with the authorized nodes [37].

$$r_{y_A y_B} = \frac{\sum_{i=1}^{n} (y_{A_i} - \mu_A)(y_{B_i} - \mu_B)}{\sqrt{\sum_{i=1}^{n} (y_{A_i} - \mu_A)^2} \sqrt{\sum_{i=1}^{n} (y_{B_i} - \mu_B)^2}} \quad (1)$$

where $r_{y_A y_B}$ is the correlation coefficient of characteristics of the channel measurement results between the two authorized nodes, n states the number of channel characteristics, whereas μ_A and μ_B is the average of the channel characteristics measurement results of A and B. μ_A is obtained by $\mu_A = \frac{1}{n} \sum_{i=1}^{n} y_{A_i}$ and μ_B is obtained by $\mu_B = \frac{1}{n} \sum_{i=1}^{n} y_{B_i}$.

3. Key Generation System Overview

Some existing studies [24–29] use a key generation system consisting of five phases as shown in Figure 2. The first phase is to alternately measure channel characteristics between two authorized nodes. Non-simultaneous measurements can lead to high differences in the generated key bits. To overcome these problems, the signal pre-processing phase is carried out on measured channel characteristics using smoothing [24] and filtering [28]. The third phase is quantization which aims to change the channel characteristics of the signal pre-processing results in the form of a single bit [38] and multi-bit [39]. The fourth phase is the error-correcting that is used to correct the different bits due to nonsimultaneous measurements. The last phase is privacy amplification which aims to obscure the part of the leaked key to the tapper by increasing the randomness of the produced key. At this step, verification is also carried out which aims to ensure that the produced keys from the authorized nodes are the same.

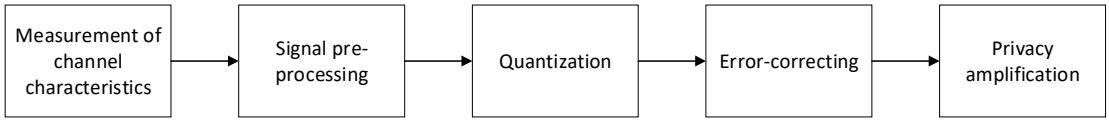


Figure 2. The Existing of the key generation system.

The other studies use a key generation system consisting of four phases [40–42]. These phases include the measurement of channel characteristics, quantization, error-correcting, and privacy amplification. The performance evaluation shows that direct quantization can result in high bit mismatches at the quantization phase. The addition of the signal pre-processing phase at [24–29] aims to reduce the incompatibility of the resulting bits. However, compared with [32], the studies that use five phases tend to be less efficient due to the addition of the signal pre-processing and error-correcting phases, which increases computing time. The higher the difference bit that occurs, the higher the produced computing time is because more data blocks must be corrected. The study [32] modified the signal pre-processing phase to increase the similarity of channel characteristics in each block of measurement data and eliminate error-correcting phase. However, the signal pre-processing phase requires high computing time because it is conducted for each data block. The more data the higher computing time needed. In this paper, we try to overcome this problem by proposing a simpler key

generation system, i.e., signal strength exchange (SSE) system because it only consists of 3 phases. Elimination of signal pre-processing and error-correcting phases significantly reduced computing time so it is suitable for IoT devices with limited computing resources.

4. SSE System

We propose the SSE system as a key generation system that consists of three phases, i.e., measurement of channel characteristics, quantization, and privacy amplification as shown in Figure 3. The system is simpler when compared to existing systems [24–29,32,40–42], so it is expected to be able to reduce computing time, communication overhead and suitable for IoT devices with limited computing resources. We claim that our proposed key generation system is simpler in terms of the number of phases that must be passed. The more phases that must be passed will affect the produced computing time. The amount of communication/synchronization between two nodes will affect communication overhead and the produced communication/synchronization time. Table 1 shows the comparison of the phases that must be passed on the key generation. Overall, it can be said that SSE systems have fewer phases compared to existing systems. The measurement of channel characteristics was carried out in two different scenarios i.e., unobstructed and obstacles scenarios. In this paper, we use RSS as channel characteristics to be measured due to the most easily acquired on a variety of wireless devices. A is one of the authorized nodes selected as the initiator. The channel characteristics of measurement results will be converted into multi-bit using the quantization phase. As part of the SSE system, we also propose a new quantization method i.e., synchronized quantization (SQ) which synchronizes data blocks in the quantization phase. Synchronization is carried out between the two authorized nodes by exchanging wasted index of blocks to ensure that the produced key is absolutely the same so it can eliminate the error-correcting phase. Another advantage of the SQ method is the elimination of the signal pre-processing phase. This occurs because the SQ method is able to produce absolutely the same key bits directly from the channel characteristics of the measurement results. In the privacy amplification phase, we use the universal hash [43] to obfuscate the leaked key parts to the unauthorized node and SHA-1 [44] to ensure that the produced keys by the two authorized nodes are the same.

The first phase of the SSE system is the mechanism for measuring RSS channel characteristics y_u between nodes as shown in Figure 4. Subscript u can be replaced with A for Alice, B for Bob, E for Eve (RSS channel characteristics from A), and E' for Eve (RSS channel characteristics from B). A sends pings to B with each time interval t_m. B measures and stores the RSS channel characteristics of the ping conducted by A before giving response with delay τ. In the same way, A also conducts measurement and stores the RSS channel characteristics of response conducted by B. To ensure the reciprocity of the produced channel characteristics τ must be made as small as possible so it is smaller than coherence time. From the measurement phase, A and B collect a number of RSS channel characteristics n as shown by Equations (2) and (3). E as an unauthorized node listens to all the measurement processes and collects a number of RSS channel characteristics from A and B as seen in Equations (4) and (5).

$$y_A = [y_A(1), y_A(2), \ldots, y_A(n)]^T \tag{2}$$

$$y_B = [y_B(1), y_B(2), \ldots, y_B(n)]^T \tag{3}$$

$$y_E = [y_E(1), y_E(2), \ldots, y_E(n)]^T \tag{4}$$

$$y_{E'} = [y_{E'}(1), y_{E'}(2), \ldots, y_{E'}(n)]^T \tag{5}$$

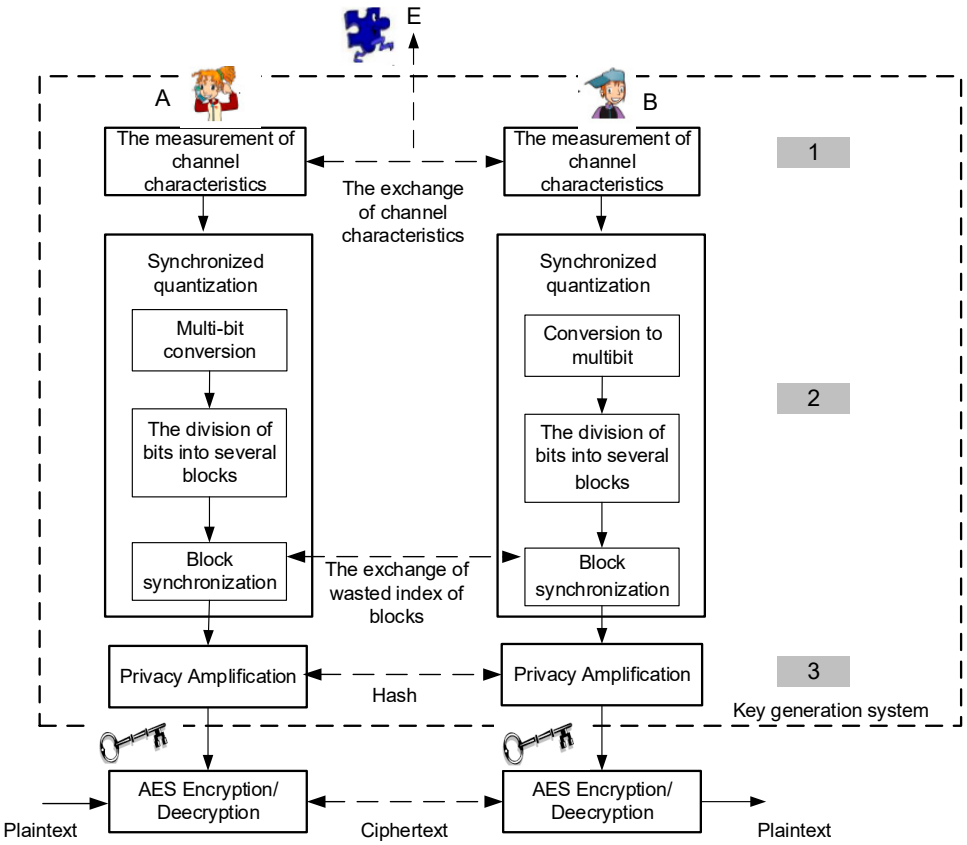


Figure 3. SSE key generation system.

Table 1. Comparison of the key generation phases.

Key Generation System	Key Generation Phases				
	Measuring Channel Characteristics	Signal Pre-Processing	Quantization	Error Correcting	Privacy Amplification
[22–27]	V	V	V	V	V
[30]	V	V	V	-	V
[38–40]	V	-	V	V	V
SSE System	V	-	V	-	V

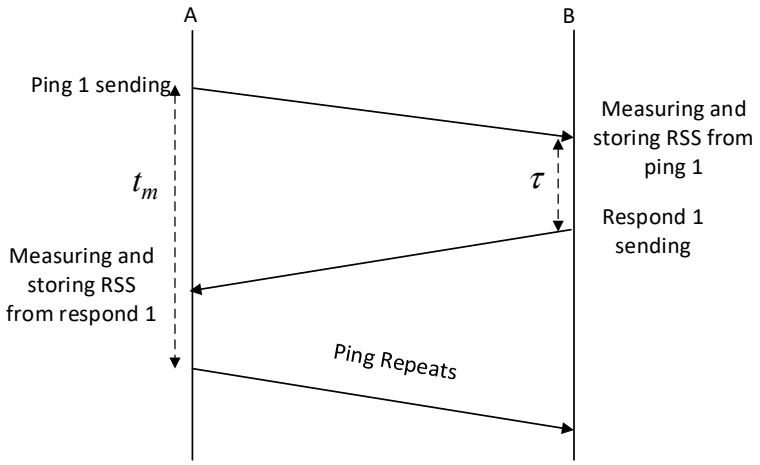


Figure 4. The mechanism of RSS channel characteristics measurement.

The second phase is to convert the RSS channel characteristics y_u into multi-bit using the SQ method. This method utilizes three parameters, i.e., standard deviation σ_u, mean μ_u and a to determine the produced bits in each area. In this paper standard deviation and mean are calculated from the overall RSS channel characteristics, while a is used as dividers from the standard deviation. These parameters are used to determine the area of each channel characteristics. Bit conversion Q_u from each area determined using Gray code as shown by Equation (6). All the RSS channel characteristics will be converted into multi-bit and no waste channel characteristics. The resulting multi-bit sequence K_u is seen in Equation (7).

$$Q_u = \begin{cases} y_u \leq \mu_u - (\sigma_u/a) & ,00 \\ \mu_u - (\sigma_u/a) < y_u < \mu_u & ,01 \\ \mu_u \leq y_u < \mu_u + (\sigma_u/a) & ,11 \\ y_u \geq \mu_u + (\sigma_u/a) & ,10 \end{cases} \tag{6}$$

$$K_u = [Q_u(1), Q_u(2), \ldots Q_u(n)]^T \tag{7}$$

There are no wasted channel characteristics so the length of K_u is N, where $N = 2xn$. The sequence of K_u will be divided into a few blocks B_N wherein each block contains 3 bits so $K_B = [K_B^T \ldots K_{B-B_N+1}^T]$ is obtained. The next step is the synchronization of bit blocks K_B. The bit blocks will be saved if there are three sequential bits (i.e., 000 or 111) and convert it to 1 or 0. Synchronization is conducted by exchanging wasted index of blocks between the authorized nodes. After synchronization is complete, the remaining block bits will be converted back into bit sequences Key_u. A detailed description of the SQ method that is run on each node can be seen in Algorithm 1. We initialize 2 parameters i.e., a and k which is able to provide the most optimal configuration as shown in Line 1. Determining the number of areas and bit conversion of each channel characteristic is shown in Line 2–3. The conversion mechanism of channel characteristics measurement results into a multi-bit is shown in Lines 4–14 (Equation (6) and (7)), while the division of bits into several blocks and synchronization of each of the blocks are shown in Lines 15–26.

Algorithm 1: Synchronized Quantization (SQ)

Input : RSS Channel characteristics y_u
Input : The standard deviation of the overall RSS channel characteristics σ_u, mean of the overall RSS channel characteristics μ_u
Input : The number of bit conversion of each RSS channel characteristics k
Input : The bit length of the conversion result N
Input : Number of block bits conversion B_N
Output : The synchronization bit sequence Key_u

$a = 0.6 - 0.85$, $k = 2$
Determination of the number of areas 2^k
Determination k bit in each area with Gray Code $[Q_1, Q_{2^k}]$
for $i \leftarrow 1$ **to** n **do**
  if $y_{u_i} \le \mu_{u_i} - (\sigma_{u_i} / a)$ %area 1
    $K_{u_i} = Q_1$
  else if $\mu_{u_i} - (\sigma_{u_i} / a) < y_{u_i} < \mu_{u_i}$ %area 2
    $K_{u_i} = Q_2$
  else if $\mu_{u_i} \le y_{u_i} < \mu_{u_i} + (\sigma_{u_i} / a)$ %area 3
    $K_{u_i} = Q_3$
  else if $y_{u_i} \ge \mu_{u_i} + (\sigma_{u_i} / a)$ %area 4
    $K_{u_i} = Q_4$
  end if
end for
for $i \leftarrow 1$ **to** B_N
  $K_{B_i} = 0$
  for $j \leftarrow 1$ **to** 3
    $K_{B_i} = K_{B_i} + K_{u_{j,i}}$
  end for
  if $K_{B_i} == 3$
    $Key_{u_i} = 1$
  else if $K_{B_i} == 0$
    $Key_{u_i} = 0$
  else
    Key_{u_i} dropped
  end if
end for

The latter is a privacy amplification phase that consisted of an increased randomness and verification mechanism. Increased randomness mechanism is used to increase the randomization of key synchronization results and remove the possibility of information obtained by the unauthorized node during the block synchronization phase and is used to guess the part of the key [38]. Bit synchronization Key_u will be improved for its randomness by using a Universal Hash. The method works by randomly selecting a hash function with certain mathematical properties that can ensure the randomness of produced data. The advantage of this method is the small possibility of obtaining the same data even though the data is selected by the unauthorized node. In this paper, increased randomness was carried out on Key_u that had been divided into several blocks of key bits. Each block contains a 128-bit key

and will be tested by using NIST software [45]. Blocks that fulfill the requirements will be used as a key to encrypt the plaintext. The verification mechanism is carried out to ensure that the keys used by authorized nodes are the same. In this paper, a block of the 128-bit key that has met the randomness requirements will be hashed using SHA-1. We chose this method because of the high security of the produced hash and it is widely used for one-way functions so key constancy could be seen without revealing information to the tapper. SHA-1 generates hash up to 160 bits long so it will increase the time communications between authorized nodes if all bits are transmitted. Since SHA-1 has the ability to detect bit differences even though it is very small, then only 6 bits of hashes will be sent with a correction capability of up to 98%. The relationship between the length of the bit ℓ and the correction ability c is expressed by Equation (8).

$$\begin{aligned} 1-\left(\tfrac{1}{2}\right)^{\ell} &\geq c \\ \ell &= \left\lceil \log_{1/2}(1-c) \right\rceil \end{aligned} \tag{8}$$

5. Implementation and Performance Evaluation

This section discusses in detail the implementation and performance evaluation of the SSE system. The implementation section provides a detailed description of the devices and software used, as well as the topology measurement scenarios. The performance evaluation section discusses the parameters of performance of the built SSE system, analysis of test results and comparison with several existing systems.

5.1. Implementation

We implemented the SSE system on three Raspberry Pi 3 Model B devices with the operating system Raspbian Stretch and kernel version 4.14.74-v7 +. Two devices become authorized nodes A and B while another becomes an unauthorized node E. One of the reasons why we chose this device is because of the open source operating system used i.e., Linux so there are many possibilities for application development. The number of high-level programming languages that can be used such as Python and the existence of additional slots for various connectivities is also the reason for choosing this device. RSS channel characteristics measurements conducted using the wireless USB Adapter (TL-WN722N) that operates at a carrier frequency of 2.45 GHz. This device works in the half-duplex mode so the measurements must be made alternately. Figure 5 shows the devices that used to build the SSE system. The measurement mechanism is conducted by equipping each node with Wireshark software so that it can capture the received RSS channel characteristics. As an initiator A pings to B at any time interval $t_m = 110$ ms. The time interval is based on the speed of movement of the authorized nodes which is equal to 1.2 m/s. The Doppler Frequency f obtained is 9.6 GHz (the speed of movement multiplied by the carrier frequency divided by the speed of light) so the coherence time obtained is 104.2 ms $(1/|f|)$. Randomness requirements can be fulfilled if the time interval t_m exceeds coherence time [46] so we select time interval 110 ms. In this paper, there are 4000 RSS channel characteristics captured by each node.

There are two topology measurement scenarios used in this paper, i.e., unobstructed and obstacles scenarios. In unobstructed scenarios as shown in Figure 6, we measure in classroom measures 8.8 m and 6.9 m. The barrier to the left and right of the classroom is glass, while the front and rear borders are walls. The objects in the classroom include tables, chairs, and blackboards. A is a mobile node and moves straight along the yellow path. B and E are static with a distance of approximately 10 cm. In obstacles scenario, as seen in Figure 7, we measure in two rooms, the laboratory room, and the final project. The room is bounded by closets. Both rooms measure 8 and 14.7 m. The two rooms also contain tables, chairs, blackboards, and closets as a barrier. The same as the previous scenarios A is a mobile node and moves to the yellow path. B and E static with a distance of approximately 10 cm, and separated by closets with A. There were no people passing at the time of measurement in both scenarios.

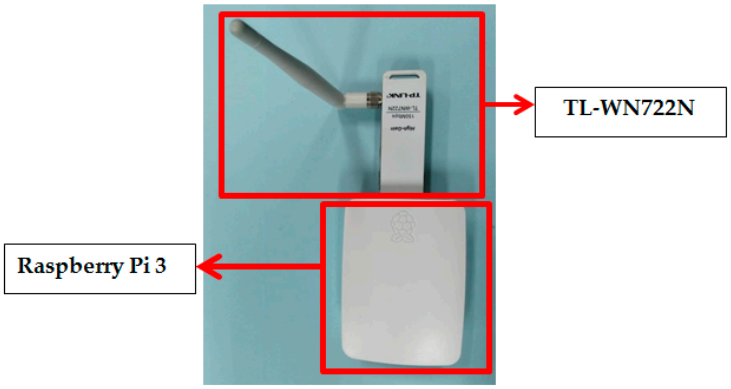


Figure 5. The device used to build the SSE system.

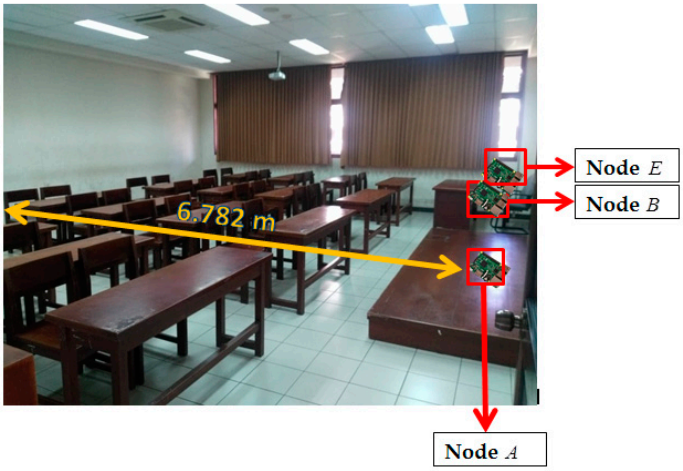


Figure 6. Unobstructed scenario.

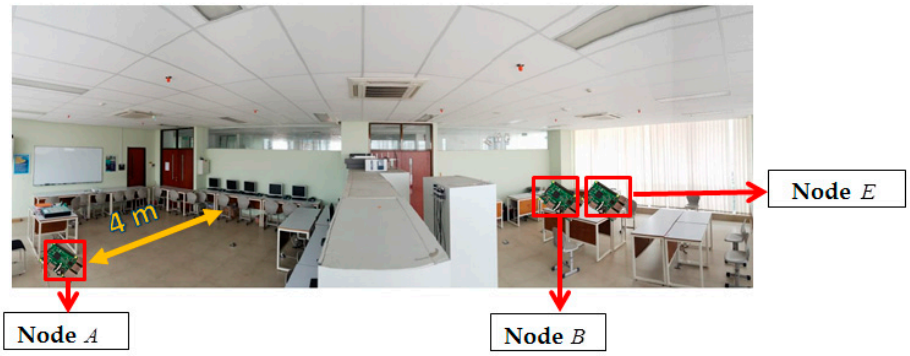


Figure 7. Obstacles scenario.

5.2. Performance Evaluation

This section discusses in detail the performance parameters and the performance analysis of test results. The used performance parameters are aimed at determining the success rate of the SSE key generation system. Performance analysis discusses in detail the measurement results performed in two types of scenarios and the advantages of the SSE system compared with previous key generation systems.

5.2.1. Performance Parameter

We evaluate the built SSE key generation system by using several parameters i.e., key synchronized rate (KSR), key discrepancy rate (KDR), irregularity, computing time and communication overhead.

KSR, computing time and communication overhead are implementational dependent parameters because it is strongly influenced by the computing resources used. KDIR and irregularity are implementational independent parameters because it is influenced by the method used in each key generation phase. So there is no result difference if the key generation system is run in different computing resources. A summary of each parameter is explained as follows.

1. Key synchronized rate (KSR): the number of identical bits during the duration of the key generation system communication. The aim of this proposed key generation system is to conduct key updates every 15 minutes. This time has met the requirements proposed by [47] because the key update time is less than 1 hour.
2. Key discrepancy rate (KDIR): the number of discrepancy bits from the obtained 128-bit key after the quantization phase. The aim of this proposed key generation system is yielding KDIR values of 0 for channel characteristics obtained from authorized nodes and KDIR above 0 for channel characteristics obtained from an unauthorized node.
3. Irregularity: the randomness of the produced key evaluated using 6 tests from the National Institute of Standards and Technology (NIST) [45]. The tests included frequency test (F), frequency block test (BF), runs test (R), a long run of ones in the block (LROB), approximate entropy test (AP), and cumulative sums test (CS). Each test result will produce P value. If P value is at least 0.01 then the produced key has met the randomness requirements.
4. Computing time: the length of time required to complete each key generation phase. The lower the complexity of the phases performed, the faster the resulted in computing time is, so it is suitable for IoT devices that have limited computing resources.
5. Communication overhead: the number of bytes transmitted for two-node communication. In the SSE system, communication overhead is greatly influenced by the number of wasted index of blocks in the quantization phase and the number of hashes transmitted during privacy amplification.

5.2.2. Performance Analysis of the SSE System

Figures 8 and 9 show box plots of the correlation coefficients measurement results between nodes in the unobstructed and obstacles scenarios. In this paper, the box plots were obtained from the calculation of data block correlation coefficients with Equation (1), each of which contained 128 RSS channel characteristics. The smaller the value of the correlation coefficient, the more different RSS channel characteristic values are obtained from the measurement results, so it is difficult to get the same keys. The correlation coefficients value range from 1 to −1. There are three pieces of information that will be retrieved from the box plots i.e., the median, the lower and upper quartile of the correlation coefficient. The correlation coefficient results between nodes $A - B$ in the unobstructed scenario obtained a median value of 0.7547, lower quartile of 0.7303, and the upper quartile of 0.7809. The correlation coefficient results between nodes $A - E$ show a median value of 0.0007, lower quartile of −0.0462 and upper quartile of 0.0825. Meanwhile, the correlation coefficient obtained between nodes $B - E$ indicates similar results with correlation coefficient obtained from the node $A - E$ with the median value of 0.0323, the lower quartile and the upper quartile of −0.0575 at 0.0718. The results of testing in an unobstructed scenario indicate the difficulty of the unauthorized node to get the same key because of the significant difference of the correlation coefficient between the authorized nodes ($A - B$) and the unauthorized node ($A - E$ and $B - E$). The correlation coefficient results between nodes $A - B$ in the obstacles scenario obtained a median value of 0.7021, lower quartile of 0.6645, and the upper quartile of 0.7326. The correlation coefficient results between nodes $A - E$ show a median value of 0.0143, lower quartile of −0.0687 and the upper quartile of 0.0631. Whereas the correlation coefficient obtained between nodes $B - E$ indicate similar results with correlation coefficient obtained from the node $A - E$ with the median value of 0.0430, lower quartile of −0.0220 and upper quartile of 0.0772. Generally, it can be seen that the correlation coefficient value of authorized nodes in the obstacles scenario is lower than the unobstructed scenario. There is a barrier between authorized nodes so that

the RSS channel characteristics obtained is also worse and decreases the correlation coefficient of the measurement results. Similar to the testing conducted in an unobstructed scenario, the correlation coefficients obtained also indicate the difficulty of the unauthorized node to get the same key because of the significant difference of the correlation coefficient between the authorized nodes ($A - B$) and the unauthorized node ($A - E$ and $B - E$).

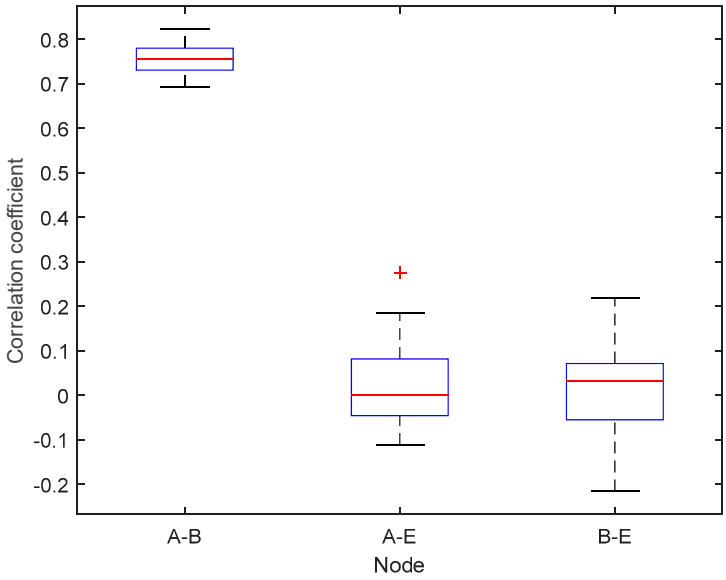


Figure 8. Box plots of the correlation coefficient value in the unobstructed scenario.

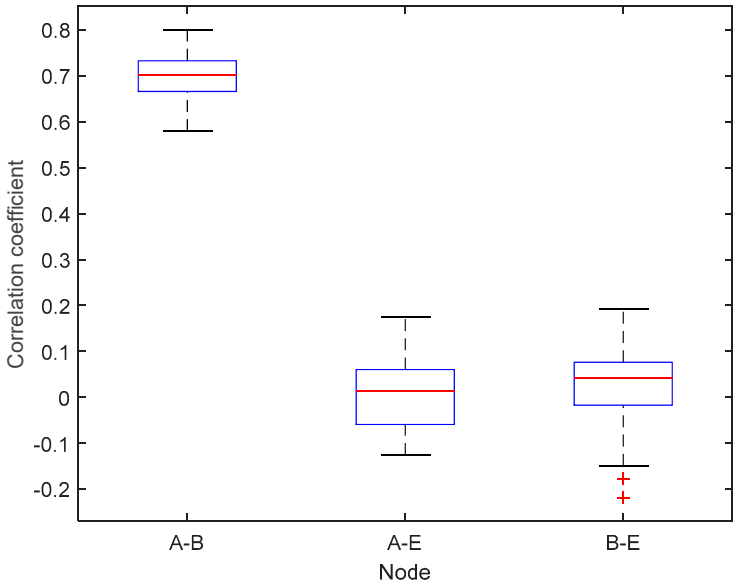


Figure 9. Box plots of the correlation coefficient value in the obstacles scenario.

The SQ method performs the multi-bit conversion by dividing the RSS channel characteristics into several areas. The number of RSS channel characteristics in each area is strongly influenced by the selection of a as a standard deviation dividing parameter. Figures 10 and 11 show the number of RSS channel characteristics from the node A and B in each area on the unobstructed and obstacles scenarios. The performed tests indicate that in all of the value of a the highest amount of RSS is in area 2 and 3. These conditions resulted in increasing the probability of getting three sequential bits i.e., 111 and convert it to 1. The resulting key bit will be dominated by 1. The higher the a value, the higher the possibility to get variations 1 and 0 of the produced keys is. This happens because of the growing

number of RSS channel characteristics that are in area 1 and 4 thus increasing the probability of getting three sequential bits i.e., 000 and converting them to 0. The higher variations 1 and 0 in the resulting key, the higher the likelihood of different key bits being produced between the two nodes. Table 2 shows the number of equal keys with lengths of 128, 192 and 256 that were successfully produced from two scenarios. Equal keys are obtained if the resulting KDIR between authorized nodes is 0. The test results in unobstructed scenario show that the higher the value of a the less equal key is successfully produced. This happens because of the higher variations of the 1 and 0 thus reducing the possibility of getting an equal key. The highest number of equal keys is obtained when $a = 0.6$ and $a = 0.65$. In these parameters, most RSS channel characteristics are in areas 2 and 3 so that the resulting key bits are dominated by 1. The low variation in the resulting bits increases the possibility to get an equal key. The test results in obstacles scenario show that the equal key is only obtained when $a = 0.6$ and $a = 0.65$. The high difference in the amount of RSS channel characteristics in each area and also the higher variations of 1 and 0 triggering more difficulties to get the equal key. The encryption method used to randomize the messages is Advanced Encryption Standard (AES) with key lengths of 128, 192, and 256. In this study, we focus on 128-bit keys because our proposed key generation system produces more keys at the key length of 128. The more keys produced, the higher the KSR value is generated so it can improve the performance of the built key generation system.

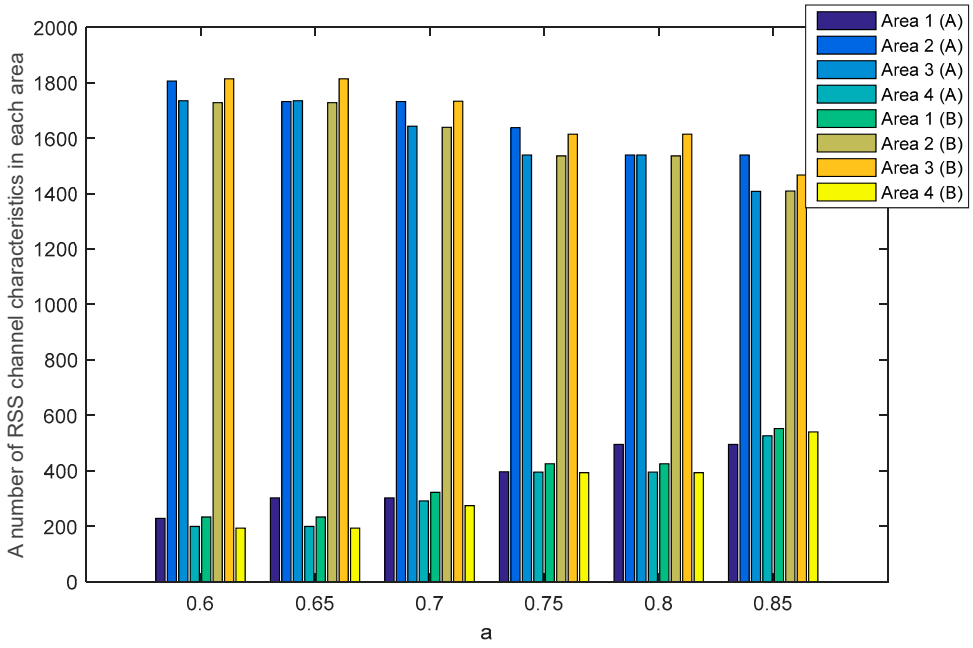


Figure 10. A number of RSS channel characteristics (node $A - B$) in each area in the unobstructed scenario.

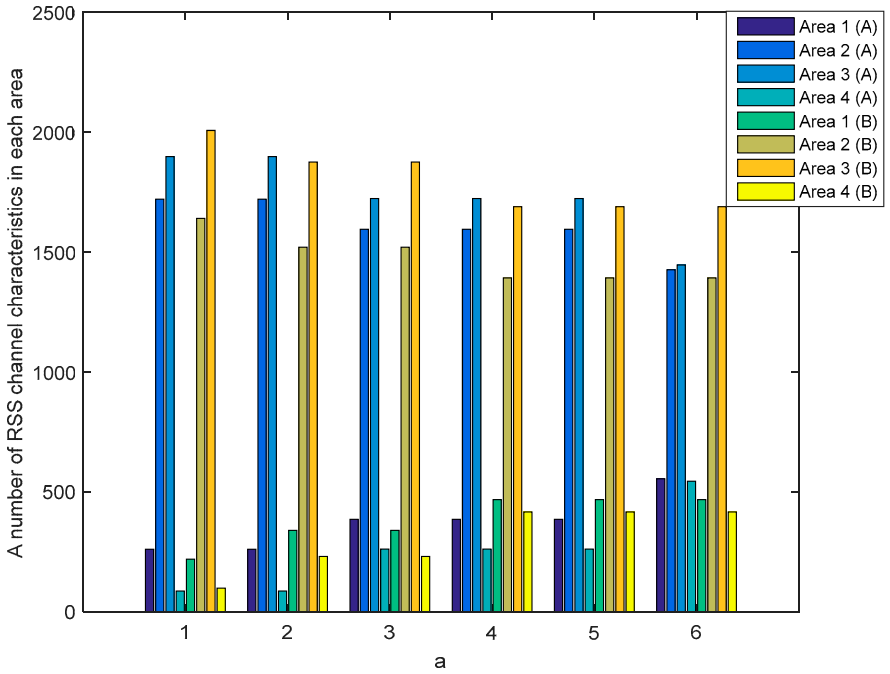


Figure 11. A number of RSS channel characteristics (node $A - B$) in each area in the obstacles scenario.

Table 2. A number of equal keys (node $A - B$).

Number of Bit Keys	a	Number of Equal Keys	
		Unobstructed Scenario	Obstacles Scenario
128	0.6	4	4
	0.65	4	1
	0.7	3	-
	0.75	2	-
	0.8	2	-
	0.85	1	-
192	0.6	2	3
	0.65	2	-
	0.7	2	-
	0.75	1	-
	0.8	1	-
	0.85	-	-
256	0.6	2	2
	0.65	2	-
	0.7	1	-
	0.75	1	-
	0.8	1	-
	0.85	-	-

Figures 12 and 13 show the number of RSS channel characteristics from nodes A and E (node $A - E$) and nodes B and E (node $B - E$) in each area in the unobstructed scenario. Meanwhile, Figures 14 and 15 show the number of RSS channel characteristics from nodes A and E (node $A - E$) and nodes B and E (node $B - E$) in each area in the obstacles scenario. At the node $A - E$, RSS channel characteristics that are processed by the node E is RSS channel characteristics received from the node A. At the node $B - E$, RSS channel characteristics that are processed by the node E is RSS received from the node B. From all scenarios, it can be seen that the number of RSS channel characteristics from a node $A - E$ is mostly in areas 2 and 3 for all values of a. These conditions result in the higher probability of getting three sequential bits i.e., 111 and convert it to 1. However, testing in obstacles scenario results in the

possibility of obtaining three sequential bits, i.e., 111 which are higher when compared to unobstructed scenarios because there are more numbers of RSS channel characteristics in areas 2 and 3. These results in the higher keys are produced. The number of RSS channel characteristics from a node $B-E$ is also mostly in areas 2 and 3 for all values a, but there are significant differences in the number of RSS channel characteristics from area 2 and 3. These results in the lower probability of getting three sequential bits i.e., 111 so fewer keys are produced.

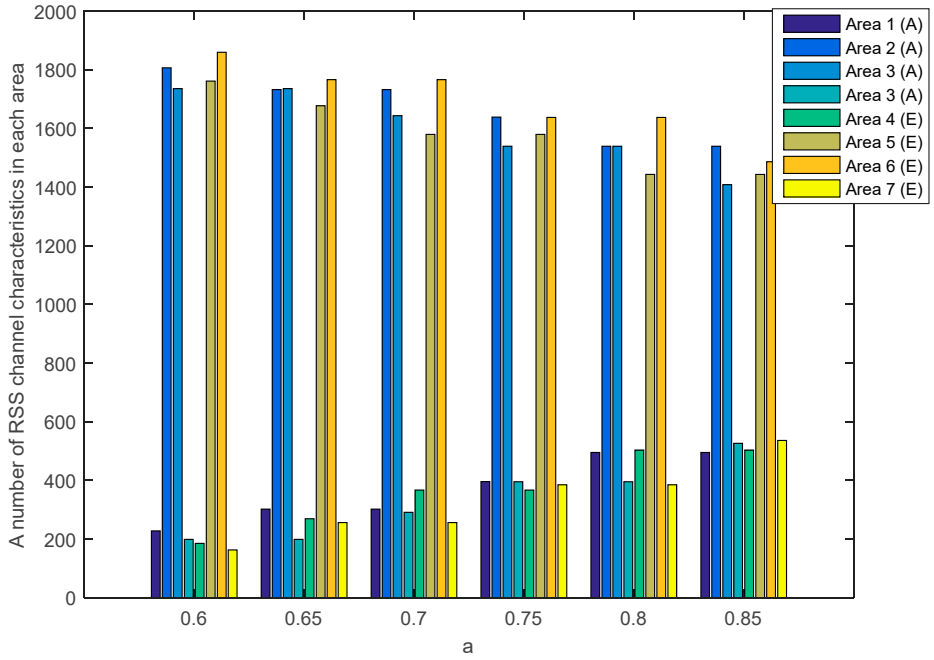


Figure 12. A number of RSS channel characteristics (node $A-E$) in each area in the unobstructed scenario.

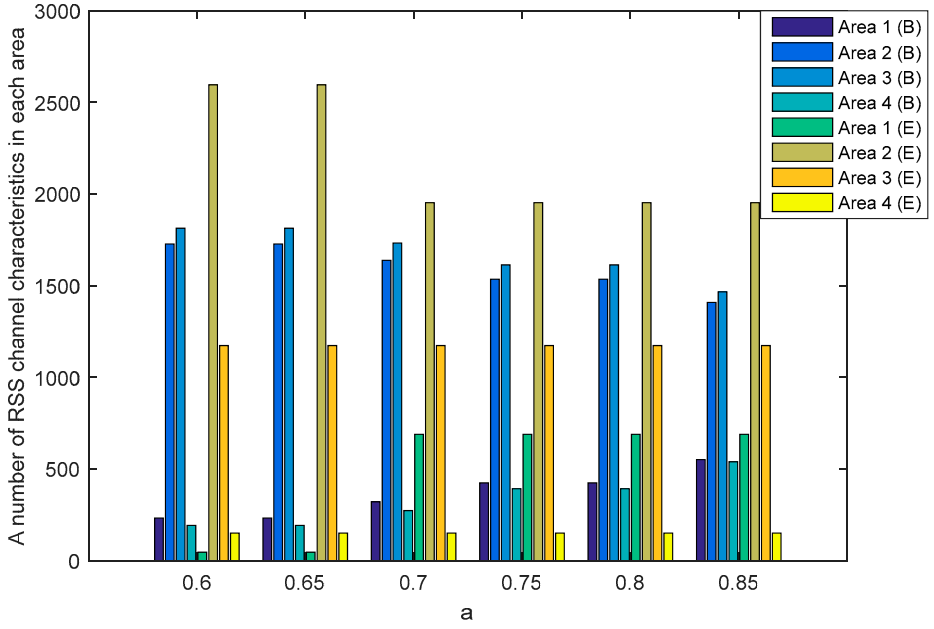


Figure 13. A number of RSS channel characteristics (node $B-E$) in each area in the unobstructed scenario.

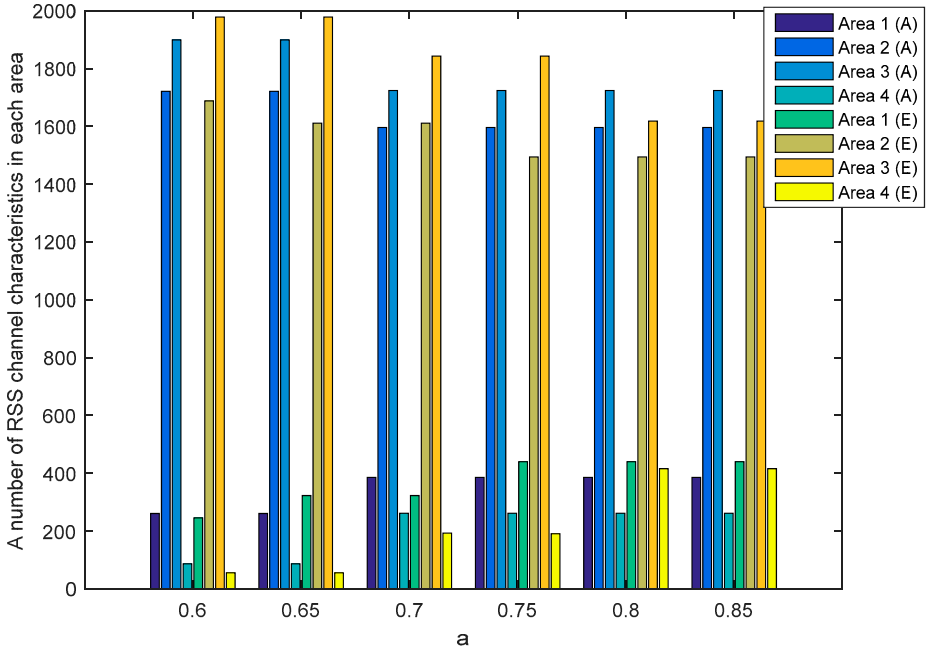


Figure 14. A number of RSS channel characteristics (node $A - E$) in each area in the obstacles scenario.

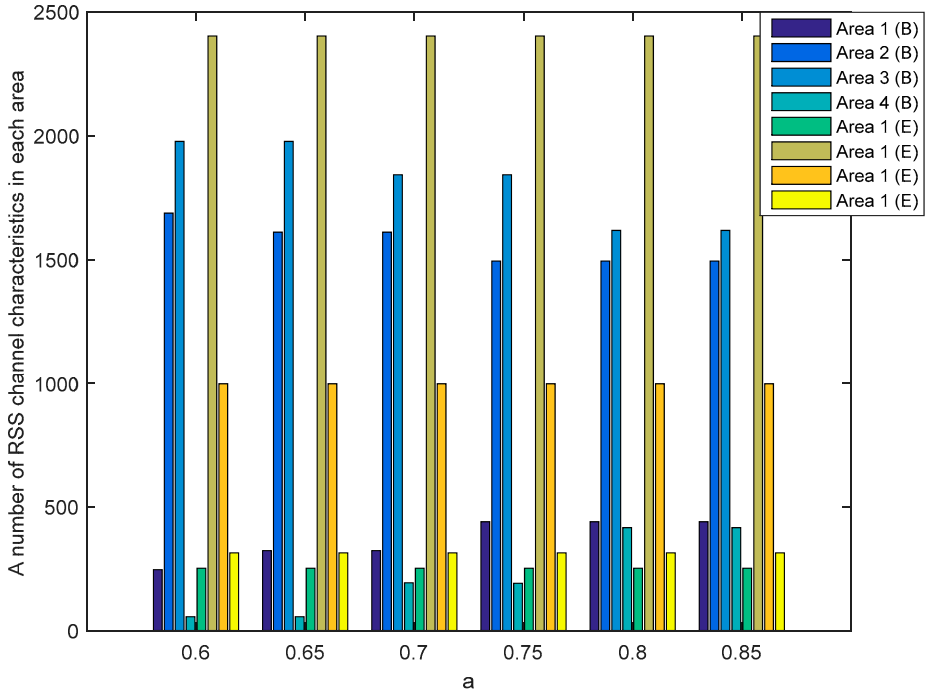


Figure 15. A number of RSS channel characteristics (node $B - E$) in each area in the obstacles scenario.

The number of produced 128-bit keys by the unauthorized node and key discrepancy rate (KDIR) between the unauthorized and authorized nodes is shown in Tables 3–7. The produced 128-bit keys by the authorized nodes are expressed as Ka (node $A - B$) while the produced 128-bit keys by the unauthorized node are expressed as Ke (node $A - E$) and Kb (node $B - E$). The KDIR value was obtained from the number of discrepancy bits between Ka and Ke with Ka and Kb. To meet security requirements, it is expected that there is no equal 128-bit key obtained by the unauthorized node indicated by the KDIR value above 0. The performed test results in both scenarios indicate less number of produced 128-bit keys by node $B - E$ compared to the node $A - E$. This happens because of the low probability of getting three sequential bits i.e., 111 because of the significant difference in the number

of RSS in areas 2 and 3. The fewer three sequential bits produced, the fewer 128-bit keys that can be produced. The test results in unobstructed scenarios also indicate that the higher the value of a, the higher KDIR value between unauthorized and authorized nodes. The high KDIR is caused by the higher variations of the 1 and 0 so as to increase the difference in the produced bits. From the results of testing in the obstacles scenario, there is no significant difference in the KDIR value between the values of $a = 0.6$ and $a = 0.65$. This happens because the number of RSS is almost the same in each area for both a values. Overall, it can be said that the built SSE system has met the security requirements because all KDIR values have exceeded 0. There are no equal keys that were successfully produced by the unauthorized node.

Table 3. A number of keys (node $A - E$ and $B - E$).

Scenarios	Number of Keys Ke for Each a Value						Number of Keys Kb for Each a Value					
	0.6	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**	**0.6**	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**
Unobstructed scenario	2	2	2	2	1	1	1	1	1	1	1	1
Obstacles scenario	3	1	-	-	-	-	3	1	-	-	-	-

Table 4. The key discrepancy rate of unauthorized nodes in the unobstructed scenario ($a = 0.6$ and $a = 0.65$).

KDIR for Each a Value									
a	**Ka**	**Ke-1**	**Ke-2**	**Kb-1**	a	**Ka**	**Ke-1**	**Ke-2**	**Kb-1**
0.6	Ka-1	0.0391	0.0469	0.0234	0.65	Ka-1	0.0547	0.0703	0.0234
	Ka-2	0.0703	0.0781	0.0547		Ka-2	0.0938	0.1094	0.0625
	Ka-3	0.0703	0.0781	0.0547		Ka-3	0.0703	0.1016	0.0547
	Ka- 4	0.0703	0.0781	0.0547		Ka- 4	0.0859	0.1016	0.0703

Table 5. The key discrepancy rate of unauthorized nodes in the unobstructed scenario ($a = 0.7$ and $a = 0.75$).

KDIR for Each a Value								
a	**Ka**	**Ke-1**	**Ke-2**	**Kb-1**	a	**Ka**	**Ke-1**	**Kb-1**
0.7	Ka-1	0.1172	0.1172	0.2891	0.75	Ka-1	0.1406	0.2969
	Ka-2	0.1406	0.1406	0.3125		Ka-2	0.1875	0.2969
	Ka-3	0.1484	0.1328	0.2734		-	-	-

Table 6. The key discrepancy rate of unauthorized nodes in the unobstructed scenario ($a = 0.8$ and $a = 0.85$).

KDIR for Each a Value							
a	**Ka**	**Ke-1**	**Kb-1**	a	**Ka**	**Ke-1**	**Kb-1**
0.8	Ka-1	0.2109	0.3047	0.85	Ka-1	0.2969	0.4063
	Ka-2	0.2344	0.3281		-	-	-

Table 7. The key discrepancy rate of unauthorized nodes in the obstacles scenario ($a = 0.6$ and $a = 0.65$).

KDIR for Each a Value											
a	Ka	Ke-1	Ke-2	Ke-3	Kb-1	a	Ka	Ke-1	Ke-2	Ke-3	Kb-1
0.6	Ka-1	0.0625	0.0703	0.0547	0.0547	0.65	Ka-1	0.0547	0.0781	0.0547	0.0391
	Ka-2	0.0391	0.0469	0.0313	0.0313		-	-	-	-	-
	Ka-3	0.0547	0.0625	0.0469	0.0469		-	-	-	-	-
	Ka-4	0.0469	0.0547	0.0391	0.0391		-	-	-	-	-

The computation of time testing is conducted by calculating the time needed in the SQ and privacy amplification phase. In the SQ phase, there are two calculated times, i.e., computing time (CT) of multi-bit conversion and the division of bits into several blocks, as well as communication/synchronization time (C/ST) of exchanges of wasted index of blocks to ensure the produced key is absolutely the same as it can eliminate the error-correcting phase. In the privacy amplification phase, there are also two calculated times, i.e., computing time (CT) of increased randomness and the verification mechanism, as well as communication/synchronization time (C/ST) of hash exchanges between the two authorized nodes. Communication overhead testing is conducted by calculating the size of the files sent for synchronization between 2 authorized nodes. Synchronization is conducted after the SQ and the privacy amplification phase. Tables 8 and 9 show the computing time testing to get equal 128-bit keys for each a value in two scenarios while communication overhead testing is shown in Tables 10 and 11. The results of the tests showed no significant computing time differences for each a value in both scenarios, even in the SQ or privacy amplification phases. Computing time differences actually occur between SQ and privacy amplification phases. This happens because the processed data in the SQ phase for each a value is the same channel characteristics measurement data. The processed data in the privacy amplification phase is the remaining of the SQ phase data. Communication/synchronization time testing also showed no significant time difference for each a value in both the SQ and privacy amplification phases. This happens because there is no significant difference between the produced communication overhead.

Table 8. Testing of computing time for each a value in the SQ phase.

Scenarios	Computing Time (CT) (s)						Communication/Synchronization Time (C/ST) (s)					
	0.6	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**	**0.6**	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**
Unobstructed scenario	24.54	24.35	24.41	24.45	24.42	24.51	4.23	4.33	4.41	4.40	4.39	4.48
Obstacles scenario	24.30	24.32	-	-	-	-	4.32	4.33	-	-	-	-

Table 9. Testing of computing time for each a value in the privacy amplification phase.

Scenarios	Computing Time (CT) (s)						Communication/Synchronization Time (C/ST) (s)					
	0.6	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**	**0.6**	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**
Unobstructed scenario	15.05	15.19	15.28	15.12	15.23	15.17	4.22	4.25	4.31	4.27	4.33	4.35
Obstacles scenario	15.42	15.42	-	-	-	-	4.23	4.24	-	-	-	-

Table 10. Testing of communication overhead for each a value in the SQ phase.

Scenarios	Communication Overhead (byte)					
	0.6	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**
Unobstructed scenario	17962	17904	18381	18852	18791	19460
Obstacles scenario	16995	17361	-	-	-	-

Table 11. Testing of communication overhead for each a value in the privacy amplification phase.

Scenarios	Communication Overhead (byte)					
	0.6	**0.65**	**0.7**	**0.75**	**0.8**	**0.85**
Unobstructed scenario	11276	11276	11270	11270	11270	11270
Obstacles scenario	11276	11276	-	-	-	-

In this paper, the KSR parameter is obtained by calculating the number of equal key bits during the duration of the SSE system communication. The duration of this system communication includes the measurement of channel characteristics, computing and communication/synchronization time at the synchronized quantization (SQ) phase, as well as computing and communication/synchronization time at the privacy amplification phase. This study carried out testing by varying the parameter of a within 0.6 to 0.85. The varied selection of the value of a is based on the attempt to get the equal 128-bit keys between authorized nodes and ensuring that there are no equal 128-bit keys of the unauthorized node. Figure 16 shows that the higher the value of a, the lower the generated KSR as there are fewer number of equal 128-bit keys. This happens because there is an increase of 1 and 0 of the produced key bits, thus minimizing the possibility of obtaining an equal key. The results of the performed tests in unobstructed scenarios showed that the highest KSR was obtained at $a = 0.6$ and $a = 0.65$, i.e., 1.05 bps, while the lowest KSR was obtained at $a = 0.85$ i.e., 0.26 bps. The obtained values indicate that the computing time to get 128-bit keys ranges from 2.03 min to 8.21 min. Meanwhile, the results of the testing carried out in unobstructed scenarios showed that the highest KSR was obtained at $a = 0.6$, i.e., 1.05 bps, while the lowest KSR was obtained at $a = 0.65$, i.e., 0.26 bps. The obtained values indicate that the computing time to get 128-bit keys ranges from 2.03 min to 8.21 min. Overall, it can be said that the SSE system is able to produce keys below 1 hour to meet the requirements of the update key maximum time proposed by [44].

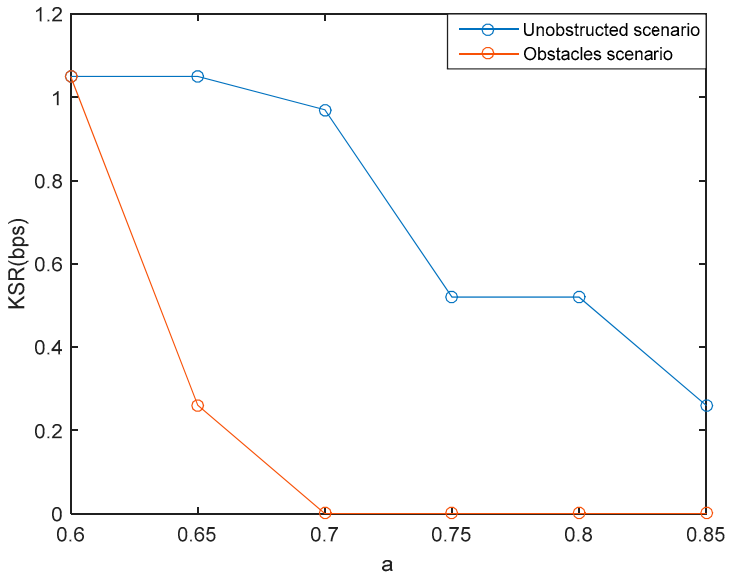


Figure 16. Key synchronized rate (KSR) for several variations of a value.

Irregularity testing was carried out to ensure that the 128-bit keys of universal hash results met the randomness requirements. In this paper, the authors used the 128-bit keys produced by $a = 0.6$. This value is selected because of the higher number of the produced 128-bit keys than the other value in both scenarios. In addition, the security requirements have also been met because there are no equal 128-bit keys produced by the unauthorized nodes. There were 6 randomization tests performed, i.e., frequency test (F), frequency block test (BF), runs test (R), a long run of ones in the block (LROB), approximate entropy test (AP), and cumulative sums test (CS). Each test result will produce a P value which is the randomness probability value of 128-bit keys ($0 \leq P$ value ≤ 1). The closer to 1, the more random the 128-bit keys are produced. In order to fulfill the randomization requirements, the minimum P value of the 128-bit keys is 0.01. The details of the usability of each test are explained as follows. The F test is used to determine the ratio of 0 and 1 of 128 key bits. The BF test aims to discover the ratio of 1 of each block in the 128-bit keys. The determination of whether fluctuations 0 or 1 in a 128-bit key is too fast or slow can be known by R tests, while the determination of whether fluctuations of 0 or 1 of each block in a 128-bit key is too fast or slow can be known with the LROB test. The AP test is used to determine the frequency of all possible intersection bits of each block in the 128-bit keys. Meanwhile, the CS test is used to specify that the accumulative number of the 128 key bits tested is too large or too small for the accumulative sum of the random sequence. Table 12 shows the results of the NIST test in the unobstructed and obstacles scenario. In both scenarios, it appears that all the produced keys have met the randomness requirements for 6 tests because the resulting P value has exceeded the specified standard, i.e., 0.01. The ranking of keys to be selected on the SSE system is Ka-4, Ka-1, Ka-2, and Ka-3. The selection of this ranking is based on the results of the AP test. If Ka-4 fails to be used as a key in the verification phase, then Ka-1 will be used as such a key. The highest P value of the AP tests is 0.9484 (unobstructed scenarios) and 0.9403 (obstacles scenario). This shows that K-4 obtained during the obstacles scenario has a higher persistence bit compared to K-4 obtained when in the unobstructed scenario.

Table 12. NIST Test.

Tes	*P* Value of Unobstructed Scenario				*P* Value of Obstacles Scenario			
	Ka-1 (A-B)	**Ka-2 (A-B)**	**Ka-3 (A-B)**	**Ka-4 (A-B)**	**Ka-1 (A-B)**	**Ka-2 (A-B)**	**Ka-3 (A-B)**	**Ka-4 (A-B)**
F	0.4795	1.0000	0.2159	1.0000	0.3768	0.8597	1.0000	1.0000
BF	0.1532	0.0239	0.3540	0.2202	0.9170	0.9326	0.4530	0.8666
R	0.8941	0.5959	0.2260	0.4795	0.1356	0.2900	0.5959	0.4795
LROB	0.4098	0.9404	0.7529	0.4203	0.1806	0.0359	0.8893	0.5788
AP	0.4540	0.3491	0.0863	0.9484	0.2941	0.4552	0.2806	0.9403
CS (fwd)	0.5748	0.6547	0.3697	0.7375	0.6548	0.8188	0.9842	0.3697
CS (rvs)	0.1542	0.6547	0.3697	0.7375	0.6548	0.9493	0.9842	0.3697

5.2.3. Comparison of Performance between SSE Systems and Existing Key Generation Systems

There are two performance parameters, i.e., computing time and the communication overhead, that are used to compare SSE systems with previous key generation systems that are also implemented on IoT devices with limited power and computing. The selection of these parameters is based on the consideration of obtaining an efficient key generation system in terms of computing time and the communication overhead. The lower the computing time and the communication overhead required, the more efficient the built key generation system. There are 4 existing key generation systems that will be used for comparison, i.e., system [9,31,33,46,48]. The system [9] uses four phases where the RSS channel characteristics will be quantized using the cumulative distribution function (CDF) method. The system [31] uses five phases where the RSS channel characteristics will be divided into several blocks, each containing 50 data. Each block will be pre-processed using the Kalman method and the results will be converted into multi-bits with the quantization method proposed by [24]. The system [33] uses five phases in building a key generation system. The RSS channel

characteristics will be pre-processed using a third order polynomial regression. The results of the signal pre-process phase will be divided into several blocks, each containing 250 bits. Each block will be converted into multi-bit with the quantization method proposed by [24]. The system [47] works by signal pre-processing the RSS channel characteristics using the discrete cosine transform (DCT) method. The results of the pre-process will be quantized using several parameters which include the mean and standard deviation. The system [48] works using 4 phases where the RSS channel characteristics will be divided into several blocks, each containing 128 bits. Each block will be converted into multi-bit with the quantization method proposed by [38]. All of the existing key generation systems still require an error-correcting phase to correct the different bits produced by the authorized nodes. In this paper, the error-correcting method used is BCH (255, 87), while privacy amplification uses the Universal Hash and SHA-1 methods.

Computing time system testing in both scenarios is divided into two parts, i.e., parts A and B. In the SSE system, part A consists of the SQ phase while part B consists of the privacy amplification phase. In the existing key generation system, part A consists of a signal pre-processing phase to the error-correcting phase, while part B consists of privacy amplification. Each part will be divided into two, i.e., computing time (CT) and communication/synchronization time (C/ST). Table 13 shows a comparison of computing time between the SSE and the existing system. The results of the performed tests indicate that the SSE system is able to reduce computing time (CT) of part A to 25.77 times (unobstructed scenarios) and 26.08 times (obstacles scenario) compared to existing systems. The decrease in communication/synchronization time (C/ST) reaches 1.55 times (unobstructed scenarios) and 1.52 times (obstacles scenario). The test results of part B also show that SSE systems are able to reduce computing time (CT) to 2.60 times (unobstructed scenario) and 2.47 times (obstacles scenario) compared to existing systems. There is no significant communication/synchronization (C/ST) time difference of part B between SSE and the existing systems because the produced communication overhead is almost the same. Overall, it can be seen that the computing time (CT) and communication/synchronization (C/ST) time of the SSE system are lower than the existing system. This happens because, in part A, the multi-bit conversion of the SSE system is conducted directly from the RSS channel characteristics without going through the signal pre-processing phase. Further, there is no blocking division in processing RSS channel characteristics so it speeds up computing time compared to existing systems. The high computing time of existing systems is due to the error-correcting phase. The more data proceeded at this phase, the higher the computing time, communication/synchronization time and communication overhead required. Table 14 shows a comparison of the communication overhead between the SSE system and existing systems. The communication overhead is calculated from the size of the file sent for synchronizing the authorized nodes. In the SSE system, the data synchronization occurs after the SQ and privacy amplification phase, whereas in existing systems, the data synchronization occurs after the error-correcting and privacy amplification phase. The results of the performed tests indicate that the SSE systems can reduce the communication overhead from part A to 2.75 times (unobstructed scenario) and 2.92 times (obstacles scenario) compared to existing systems. There is no significant communication overhead difference of part B between SSE and the existing systems because of produced the communication overhead is almost the same. This happens because synchronization after the SQ phase is only conducted on the index of the wasted data block, while synchronization after the error-correcting phase is carried out on the parity bit to increase the size of the communication overhead. Overall, the results of the tests conducted indicate that SSE systems are able to reduce computing time, communication/synchronization time and the communication overhead compared to existing systems. Therefore, it can be said that the SSE system is more efficient for implementation of IoT devices with limited resources compared to existing systems.

Table 13. Comparison of computing time between the SSE and the existing system.

Key Generation System	Unobstructed Scenario				Obstacles Scenario			
	Part A		Part B (s)		Part A (s)		Part B (s)	
	CT(s)	C/ST(s)	CT(s)	C/ST(s)	CT(s)	C/ST(s)	CT(s)	C/ST(s)
SSE system	24.54	4.23	15.05	4.22	24.30	4.32	15.42	4.23
System [9]	506.03	6.44	28.60	4.23	509.31	6.55	31.17	4.32
System [31]	622.63	6.50	31.79	4.51	623.25	6.45	29.78	4.30
System [33]	496.59	6.35	27.49	4.33	490.38	6.44	24.79	4.47
System [46]	632.43	6.56	39.20	4.97	633.82	6.45	38.12	4.55
System [48]	500.95	6.32	25.33	4.43	498.18	6.44	26.14	4.33

Table 14. Comparison of communication overhead between the SSE and the existing system.

Key Generation System	Unobstructed Scenario		Obstacles Scenario (Byte)	
	Communication Overhead of Part A (Byte)	Communication Overhead of Part B (Byte)	Communication Overhead of Part A (Byte)	Communication Overhead of Part B (Byte)
SSE system	17,962	11,276	16,995	11,276
System [9]	49,339	11,403	50,133	11,908
System [31]	49,431	11,276	49,608	11,276
System [33]	47,289	11,546	47,033	12,100
System [46]	49,127	11,932	48,582	11,624
System [48]	48,513	12,005	48,680	11,707

6. Conclusions

This paper proposes the SSE system as an efficient key generation system and synchronized quantization (SQ) as a part of the SSE system that synchronizes data blocks in the quantization phase in order to eliminate the signal pre-processing and error-correcting phase. The efficiency of the system is indicated by lower computing time and the communication overhead between authorized nodes compared to existing systems. Validation of the SSE system performance is carried out in two real indoor environment scenarios, i.e., unobstructed and the obstacles scenarios. The test results showed that the SQ method was able to produce equal 128-bit keys without going through the signal pre-processing and error-correcting phase with KSR values reaching 1.05 bps (unobstructed and obstacles scenario). Testing of computing time and the communication overhead in two scenarios also show the efficiency of the SSE system compared to the existing system. This is indicated by a decrease in computing time up to 25.77 times (unobstructed scenarios) and 26.08 times (obstacles scenario), and decreased communication/synchronization time up to 1.55 times (unobstructed scenarios) and 1.52 times (obstacles scenario) of part A. Part B also shows that SSE systems are able to reduce computing time to 2.60 times (unobstructed scenario) and 2.47 times (obstacles scenario). The communication overhead of part A also decreased by 2.75 times (unobstructed scenario) and 2.92 times (obstacles scenario). In addition, the built SSE system has met the security requirements because there is no equal key that was successfully produced by the unauthorized node.

Author Contributions: Conceptualization, M.Y., W. and S.; methodology, M.Y., W. and S.; software, validation, M.Y., W. and S.; formal analysis, M.Y. and W.; resources, M.Y.; data curation, M.Y., W. and S.; writing—original draft preparation, M.Y.; writing—review and editing, M.Y., W. and S.; visualization, M.Y., W. and S.; supervision, W. and S.; project administration, M.Y., W. and S.; funding acquisition, M.Y., W. and S.

Funding: A part of this research was funded by the Ministry of Research, Technology, and Higher Education through the scholarship program BUDI-DN by the LPDP of the Ministry of Finance of the Republic of Indonesia to Mike Yuliana.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Ammar, M.; Russello, G.; Crispo, B. Internet of Things: A survey on the security of IoT frameworks. *J. Inf. Secur. Appl.* **2017**, *38*, 8–27. [CrossRef]
2. Ray, P.P. A survey on Internet of Things architectures. *J. King Saud Univ. Comput. Inf. Sci.* **2018**, *30*, 291–319.
3. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A Survey of Internet of Things (IoT) Authentication Schemes. *Sensors* **2019**, *19*, 1141. [CrossRef] [PubMed]
4. Liu, R.; Wang, J. Internet of Things: Application and Prospect. In *MATEC Web of Conferences*; Zhao, L., Xavior, A., Cai, J., You, L., Eds.; EDP Sciences France: Les Ulis, France, 2017; Volume 100, p. 02034.
5. Rajakumari, S.; Azhagumeena, S.; Devi, A.B.; Ananthi, M. Upgraded living think-IoT and big data. In Proceedings of the 2017 2nd International Conference on Computing and Communications Technologies (ICCCT), Chennai, India, 23–24 February 2017.
6. Zhang, J.; Duong, T.Q.; Woods, R.; Marshall, A. Securing wireless communications of the internet of things from the physical layer, an overview. *Entropy* **2017**, *19*, 420. [CrossRef]
7. Yener, A.; Ulukus, S. Wireless Physical-Layer Security: Lessons Learned from Information Theory. *Proc. IEEE* **2015**, *103*, 1814–1825. [CrossRef]
8. Burg, A.; Chattopadhyay, A.; Lam, K.-Y. Wireless Communication and Security Issues for Cyber–Physical Systems and the Internet-of-Things. *Proc. IEEE* **2017**, *106*, 38–60. [CrossRef]
9. Zhang, Y.; Shen, Y.; Wang, H.; Yong, J.; Jiang, X. On Secure Wireless Communications for IoT Under Eavesdropper Collusion. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 1281–1293. [CrossRef]
10. Katz, J.; Menezes, A.J.; Van Oorschot, P.C.; Vanstone, S.A. *Handbook of Applied Cryptography*, 1st ed.; CRC Press: Boca Raton, FL, USA, 1996.
11. Stallings, W. *Cryptography and Network Security: Principles and Practice*, 6th ed.; Prentice Hall Press: Upper Saddle River, NJ, USA, 2013.
12. Carbajal-Gomez, V.H.; Tlelo-Cuautle, E.; Mu, J.M.; Gerardo, L.; Fraga, D.; Sanchez-Lopez, C.; Fernandez-Fernandez, F.V. Optimization and CMOS design of chaotic oscillators robust to PVT variations: INVITED. *Integration* **2018**, in press. [CrossRef]
13. Carbajal-gomez, V.H.; Tlelo-cuautle, E.; Sanchez-lopez, C. PVT-Robust CMOS Programmable Chaotic Oscillator: Synchronization of Two 7-Scroll Attractors. *Electronics* **2018**, *7*, 252. [CrossRef]
14. Moara-Nkwe, K.; Shi, Q.; Lee, G.M.; Eiza, M.H. A Novel Physical Layer Secure Key Generation and Refreshment Scheme for Wireless Sensor Networks. *IEEE Access* **2018**, *6*, 11374–11387. [CrossRef]
15. Wan, J.; Lopez, A.; Faruque, M.A.A. Physical Layer Key Generation. *ACM Trans. Cyber-Phys. Syst.* **2018**, *3*, 1–26. [CrossRef]
16. Sun, L.; Du, Q.A. Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions. *Entropy* **2018**, *20*, 730. [CrossRef]
17. Pecorella, T.; Brilli, L.; Mucchi, L. The Role of Physical Layer Security in IoT: A Novel Perspective. *Information* **2016**, *7*, 49. [CrossRef]
18. Margelis, G.; Fafoutis, X.; Piechocki, R.J.; Oikonomou, G.; Tryfonas, T.; Thomas, P. Practical limits of the secret key-capacity for IoT physical layer security. In Proceedings of the IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016.
19. Kreiser, D.; Dyka, Z.; Kornemann, S.; Wittke, C.; Kabin, I.; Stecklina, O.; Langendoerfer, P. On Wireless Channel Parameters for Key Generation in Industrial Environments. *IEEE Access* **2017**, *6*, 79010–79025. [CrossRef]
20. Van Torre, P. Channel-Based Key Generation for Encrypted Body-Worn Wireless Sensor Networks. *Sensors* **2016**, *16*, 1453. [CrossRef] [PubMed]
21. Li, Z.; Pei, Q.; Markwood, I.; Liu, Y.; Zhu, H. Secret Key Establishment via RSS Trajectory Matching Between Wearable Devices. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 802–817. [CrossRef]
22. Wang, Q. A Novel Physical Layer Assisted Authentication Scheme for Mobile Wireless Sensor Networks. *Sensors* **2017**, *17*, 289. [CrossRef] [PubMed]
23. Yuliana, M.; Wirawan; Suwadi. Performance evaluation of the key extraction schemes in wireless indoor environment. In Proceedings of the 2017 International Conference on Signals and Systems (ICSigSys), Sanur, Indonesia, 16–18 May 2017; pp. 138–144.

24. Ambekar, A.; Kuruvatti, N.; Schotten, H.D. Improved method of secret key generation based on variations in wireless channel. In Proceedings of the International Conference on Systems, Signals and Image Processing (IWSSIP), Vienna, Austria, 11–13 April 2012; pp. 60–63.
25. Zhan, F.; Yao, N.; Gao, Z.; Yu, H. Efficient key generation leveraging wireless channel reciprocity for MANETs. *J. Netw. Comput. Appl.* **2018**, *103*, 18–28. [CrossRef]
26. Zhan, F.; Yao, N. Efficient key generation leveraging wireless channel reciprocity and discrete cosine transform. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 2701–2722.
27. McGuire, M. Channel Estimation for Secret Key Generation. In Proceedings of the International Conference on Advanced Information Networking and Applications, Victoria, BC, Canada, 13–16 May 2014; pp. 490–496.
28. Ali, S.T.; Sivaraman, V.; Ostry, D. Secret Key Generation Rate vs. Reconciliation Cost Using Wireless Channel Characteristics in Body Area Networks. In Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, Hong Kong, China, 11–13 December 2010; pp. 644–650.
29. Yuliana, M.; Wirawan; Suwadi. Improving performance of secret key generation from wireless channel using filtering techniques. In Proceedings of the Tenth International Conference on Signal Processing Systems, Singapore, 16–18 November 2018.
30. Yuliana, M.; Wirawan; Suwadi. Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment. *Int. J. Commun. Netw. Inf. Secur.* **2017**, *9*, 474–483.
31. Yuliana, M.; Wirawan; Suwadi. Performance Analysis of Loss Multilevel Quantization on the Secret Key Generation Scheme in Indoor Wireless Environment. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2019**, *9*, 100–108. [CrossRef]
32. Yuliana, M.; Wirawan; Suwadi. A Simple Secret Key Generation by Using a Combination of Pre-Processing Method with a Multilevel Quantization. *Entropy* **2019**, *21*, 192. [CrossRef]
33. Guillaume, R.; Winzer, F.; Zenger, C.T.; Paar, C.; Czylwik, A. Bringing PHY-based key generation into the field: An evaluation for practical scenarios. In Proceedings of the 2015 IEEE 82nd Vehicular Technology Conference (VTC2015-Fall), Boston, MA, USA, 6–9 September 2015.
34. Sudarsono, A.; Yuliana, M.; Kristalina, P.; Barakbah, A.R. An Implementation of Shared Key Generation Extracted from Received Signal Strength in Vehicular Ad-Hoc Communication. In Proceedings of the 2018 Sixth International Symposium on Computing and Networking (CANDAR), Takayama, Japan, 23–27 November 2018; pp. 57–65.
35. Zhang, J.; Duong, T.Q.; Marshall, A.; Woods, R. Key Generation from Wireless Channels: A Review. *IEEE Access* **2016**, *4*, 614–626. [CrossRef]
36. Zhang, J.; Woods, R.; Duong, T.Q.; Marshall, A.; Ding, Y.; Huang, Y.; Xu, Q. Experimental Study on Key Generation for Physical Layer Security in Wireless Communications. *IEEE Access* **2016**, *4*, 4464–4477. [CrossRef]
37. Ali, S.T.; Sivaraman, V.; Ostry, D. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2763–2776. [CrossRef]
38. Premnath, S.N.; Jana, S.; Croft, J.; Gowda, P.L.; Clark, M.; Kasera, K.S.; Patwari, N.; Krishnamurthy, S.V. Secret key extraction from wireless signal strength in real environments. *IEEE Trans. Mob. Comput.* **2013**, *12*, 917–930. [CrossRef]
39. Ambekar, A. Exploiting Radio Channel Aware Physical Layer Concepts. Ph.D. Thesis, Ruhr-University Bochum, Bochum, Germany, 5 October 2015.
40. Zhan, F.; Yao, N.; Gao, Z.; Lu, Z.; Chen, B. Efficient key generation leveraging channel reciprocity and balanced gray code. *Wirel. Netw.* **2019**, *25*, 611–624. [CrossRef]
41. Cheng, L.; Zhou, L.; Seet, B.-C.; Li, W.; Ma, D.; Wei, J. Efficient Physical-Layer Secret Key Generation and Authentication Schemes Based on Wireless Channel-Phase. *Mob. Inf. Syst.* **2017**, *2017*, 7393526. [CrossRef]
42. Jiang, Y.; Hu, A.; Huang, J. A lightweight physical-layer based security strategy for Internet of things. *Clust. Comput.* **2018**. [CrossRef]
43. Carter, J.L.; Wegman, M.N. Universal Classes of Hash Functions. *J. Comput. Syst. Sci.* **1979**, *18*, 143–154. [CrossRef]
44. Publication, F. Archived Publication Secure Hash Standard. *Public Law* **1987**, *2*, 100–235.
45. NIST, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Available online: http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501 (accessed on 6 May 2019).

46. Zenger, C.T.; Zimmer, J.; Pietersz, M.; Posielek, J.-F.; Paar, C. Exploiting the Physical Environment for Securing the Internet of Things. In Proceedings of the New Security Paradigms Workshop (NSPW), Twente, The Netherlands, 8–11 September 2015; pp. 44–58.
47. Moore, T. *IEEE 802.11-01/610r02: 802.1.x and 802.11 Key Interactions*; Technical Report; Microsoft Research: Cambridge, UK, 2001.
48. Margelis, G.; Fafoutis, X.; Oikonomou, G.; Piechocki, R.; Tryfonas, R.; Thomas, P. Efficient DCT-based secret key generation for the Internet of Things. *Ad Hoc Netw.* **2018**, in press.