Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment

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

[1]Dept. of Electrical Engineering, Faculty of Electrical Technology, Institut Teknologi Sepuluh Nopember, Surabaya, Indonesia
[2]Dept. of Electrical Engineering, Politeknik Elektronika Negeri Surabaya (PENS), Surabaya, Indonesia

***Abstract*:** The Secret Key Generation (SKG) scheme that exploits the reciprocity, randomness, and uniqueness of wireless channel between two users plays a significant part in a new increasing distributed security system. The scheme performance can be distinguished based on the low value of Key disagreement Rate (KDR), the high value of Key Generation Rate (KGR), as well as the fulfillment of the NIST randomness standard. The previous SKG scheme has a high KDR due to a direct quantization of a measurement result of the Received Signal Strength (RSS). To overcome the above issue, we conduct a pre-processing of measurement result before quantization with the Kalman method. The pre-process is carried out to improve the channel reciprocity between two legitimate users with the objective to reduce the bit mismatch. Through an experiment, we propose a new quantization scheme called a Modified Multi-Bit (MMB) that uses a multi-bit system on every level of quantization. The test results show that the proposed combination of preprocessing and the MMB scheme has a better performance compared to the existing schemes in terms of KDR and KGR. The Secret Key generated by our scheme also fulfills the NIST randomness standard.

***Keywords*:** SKG, RSS, Kalman, Reciprocity, MMB, NIST.

1. Introduction

A cryptographic scheme is critical to secure a wireless communication because radio channel is susceptible to interception by a third party [1-5]. Most of the schemes are public key cryptography types that require key exchange before sending information. Two notable disadvantages of this type of cryptography are the severity of computing process performed and the need for a public key infrastructure, and therefore, it is not suitable for use by a resource-constrained device and ad-hoc network [6-7]. Such conditions result in the creation of countless innovations to replace the public key. Quantum cryptography is one among such example of innovation, in which sharing of secret keys between two legitimate users is conducted by using the Quantum theory. Although the application of cryptography has started recently, the application is however still expensive and rare [6, 8].

The SKG scheme is an affordable and promising alternative of symmetric cryptography as well as suitable for any communication devices with limited power and computation. The scheme exploits the reciprocity, randomness, and uniqueness of the location of the wireless fading channel, resulting in high channel correlation and can be used to generate secret keys. RSS is one type of wireless channel parameter that is widely used as a source of extraction to generate secret keys in various implementations of Physical Layer Security (PLS) [9].

We use RSS as a parameter channel for generating secret key due to its easy accessibility using existing wireless driver without modification. In addition, most wireless devices also have the ability to conduct RSS measurements. The channel reciprocity ensures that the estimated channel parameters from two legitimate user communications on Time Division Duplex (TDD) system are the same [1, 10]. In this system, the legitimate users measure channel parameters at the same frequency but at different times. The third party, located more than half the wavelength of a legitimate user, may be able to tap but it would be very difficult for them to get the same channel parameter in a rich scattering environment. The problems arising from the use of this system is the non-identical measurement result acquired. Another influential factor is the noise from hardware that could not be avoided. The non-identical result of the measurement has the effect on different bits of the quantization result of every user. The bit mismatch of quantization result can be corrected by using an error correcting code so that the same key can be obtained from each user. The capacity correction of the used error correcting code technique is one of the success determinants of the key generation system. Bit mismatch that occurs between two legitimate users must be smaller than the capacity of technical correction. Several techniques that are often used include LDPC [11], BCH [12-14], and Linear Block Code [7]. Selection of the used techniques depends on the complexity and capacity of the correction. There are risks in which the mismatch correction bits exceed the capacity of the technique used so that the system will fail and re-start the key generation process [1]. Several studies have exploited the technique to reduce the mismatch either by using preprocessing or post-processing schemes. Authors in [15] propose the use of Level Crossing Algorithm as one of the schemes of post-processing, which is performed after quantization, wherein the method operates by searching for some bits of quantization results located sequentially along a certain parameter and replacing them with a single bit of 1 or 0. The result of the study demonstrates a significant reduction of mismatch bits between two users, but the key generation rate also decreased. This condition leads some researchers to conduct a preprocess RSS measurement result before quantization to improve the channel reciprocity to reduce the mismatched bit, however, it can still improve the KGR.

In this paper, we present the result of RSS experimental measurement from two legitimate users in an indoor wireless environment using a Wi-Fi card. The result shows that the farther the user distance, the lower is the channel reciprocity

between two users and the higher is the bit mismatch. Generally, there are two things that greatly affect the performance of SKG, i.e. the RSS measurement results and the used quantization scheme. Our specific contributions are:

- Investigating the effect of using Kalman method at SKG scheme in an indoor wireless environment on various distance measurement.
- Proposing a new quantization scheme i.e. MMB (Modified Multi-Bit) which is a modification of Ambekar method that uses a multi-bit system at every level of quantization so as to increase KGR, but maintain to have a low KDR.
- Presenting the experimental result that shows the comparison of MMB performance with Ambekar, as well as several existing quantization schemes.

The remainder of this paper is organized as follows. Related/prior works are described in chapter 2 followed by the SKG scheme in chapter 3. The proposed new quantization scheme is discussed in Chapter 4. The experimental setup in chapter 5, and the experimental results and performance evaluation are explained in chapter 6. Finally, the paper ends with a conclusion in chapter 7.

2. Prior Work

Our work adds to several previous types of research that address SKG schemes exploiting the reciprocity properties and randomness of wireless fading channels [16][17]. The SKG scheme outline consists of four stages which include probing frame exchanges to measure RSS, converting the obtained RSS into a bit form through quantization process, correcting the bit sequence obtained by each user using error correcting scheme and discarding the irreparable bit, and using the secure hash for the corrected bit sequence to prevent the possibility of such bits being predicted by the adversary [18].

Some researchers focus on problems of finding the optimal quantization scheme so as to improve the performance of SKG [7, 8, 19, 20]. There are three performance metrics that are generally used in several studies, namely: KGR, KDR, and randomness. KGR refers to the number of bits that can be generated within a given measurement time, KDR refers to the ratio of the total number of mismatch bits between Alice and Bob with the total bits generated from the quantization process, whereas randomness is intended to determine the level of randomness of the bit sequence obtained. As indicated by [8] and [15], each performance metric has an inter-metric tradeoff, in which the KDR reduction is not followed by an increase in KGR. This is shown clearly in [8], where a significant reduction of KDR also followed by a decrease in KGR. The research of [20] addresses the trade-off issues between the said performance metrics, in which the authors propose a scheme to improve reciprocity by reducing variations in RSS measurements from two users in order to reduce KDR. We show how the proposed SKG scheme of combining pre-processing scheme with MMB quantization can result in a better performance compared to [20] as well as some other existing quantization schemes.

3. Secret Key Generation System Design

The proposed SKG system design consists of five stages as illustrated in Figure 1.

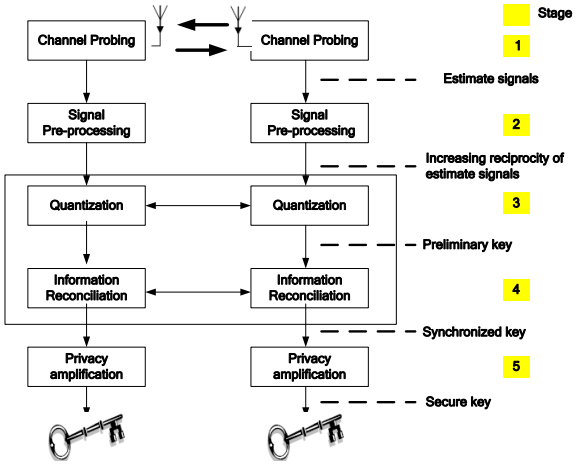

Figure 1. SKG system design

In the following, we describe in detail each stage.

3.1 Channel Probing

The first SKG stage is channel probing [18], in which two legitimate users i.e. Alice and Bob utilize a wireless environment that is rich in multipath to generate a secret key. A stochastic process $y(t)$ describes a wireless channel that varies over time between Alice and Bob. We assume $y(t)$ is RSS of Alice and Bob's multipath fading channel. To estimate the y parameters, Alice and Bob must send probe signals to each other. Each user can then use the received signal along with the probe signal to estimate $\tilde{y}$ from y. Since the radio communication mode used is a half-duplex communication mode, Alice must wait for the probe signal from Bob before sending the probe to Bob and vice versa. The estimated signal $\tilde{y}$ received by Alice and Bob is (1) and (2).

$$\tilde{y}_A(t_1) = y(t_1) + z_A(t_1) \quad (1)$$

$$\tilde{y}_B(t_1) = y(t_1) + z_B(t_2) \quad (2)$$

z_A and z_B are independent noise processes between Alice and Bob, whereas t_1 and t_2 are the times at which consecutive probe signals are received by Alice and Bob. By repeating the sending of the probe rapidly (the distance between probe signals is less than coherence time) [20], Alice and Bob can generate a series of correlated RSS signal estimation as illustrated in (3) and (4).

$$\tilde{y}_A = \{\tilde{y}_A[1], \tilde{y}_A[2], \ldots, \tilde{y}_A[n]\} \quad (3)$$

$$\tilde{y}_B = \{\tilde{y}_B[1], \tilde{y}_B[2], \ldots, \tilde{y}_B[n]\} \quad (4)$$

3.2 Signal Pre-processing

In this phase, RSS as the measured channel parameter will be estimated using prior and posterior estimation. Early predictions of RSS are performed on time update equations

and the prediction result will be corrected in measurement update equations. The results of the RSS estimation performed repeatedly as illustrated in Figure 2 will result in an increase in the reciprocity of RSS estimation.

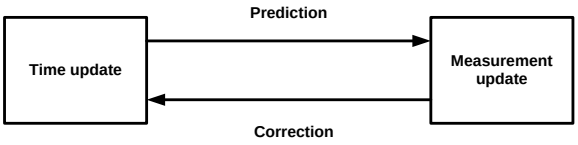

Figure 2. Signal pre-processing

We model the RSS channel parameters as a random sequence x_k using the following state-space model as shown in (5).

$$x_k = Ax_{k-1} + Bu_{k-1} + w_{k-1} \quad (5)$$

A is the $n x n$ matrix which shows the state of time $k-1$. B is the $n x l$ matrix which indicates the optional input controls u and w_k is the additive noise. $\tilde{y}_k$ is the measured channel parameter as shown in (6).

$$\tilde{y}_k = Hx_k + v_k \quad (6)$$

H is the $m x n$ matrix which shows the state of measurement at the time k and v_k is the measurement noise. The probability of the normal distribution of process noise and measurement noise is illustrated in (7) and (8).

$$p(w) \sim N(0, Q) \quad (7)$$

$$p(v) \sim N(0, R) \quad (8)$$

Where $N(\mu, \sigma^2)$ is multivariate Gaussian Distribution, whereas Q and R are the covariance matrix of process noise and measurement. $\hat{x}_k^-$ is the a priori estimation and $\hat{x}_k$ is a posterior estimation of the channel parameter, and errors during estimation can be defined as (9) and (10).

$$e_k^- = x_k - \hat{x}_k^- \quad (9)$$

$$e_k = x_k - \hat{x}_k \quad (10)$$

e_k^- and e_k are a posterior error estimation with a covariance error illustrated in (11) and (12).

$$P_k^- = E[e_k^- e_k^{-T}] \quad (11)$$

$$P_k = E[e_k e_k^T] \quad (12)$$

The time update equations used to predict RSS measurement results are illustrated in (13) and (14).

$$\hat{x}_k^- = A\hat{x}_{k-1} + Bu_{k-1} \quad (13)$$

$$P_k^- = AP_{k-1}A^T + Q \quad (14)$$

The updated measurement equation to correct the prior estimation of a priori RSS measurement results is illustrated in (15), (16) and (17).

$$K_k = P_k^- H^T (HP_k^- H^T + R)^{-1} \quad (15)$$

$$\hat{x}_k = \hat{x}_k^- + K_k(\tilde{y}_k - H\hat{x}_k^-) \quad (16)$$

$$P_k = (I - K_k H) P_k^- \quad (17)$$

Where K_k refer to the Kalman Gain.

3.3 Existing Quantization

Quantization is used to change the estimated RSS channel parameters into a bit form. Some quantization schemes are designed for channel parameters in the form of Channel Impulse Response (CIR) [10, 21] and Channel Phase [22, 23]. However, most quantization schemes are designed for RSS channel parameters [24], since they are provided by almost all wireless communication chips.

Some Quantization scheme has been proposed by existing researchers [8, 15, 20]. The differences in proposed scheme come from the difference in threshold selection and the number of thresholds used. Aono scheme uses the median of RSS as a threshold [25] and disregards the RSS in the median. The Mathur scheme uses two thresholds i.e. $q+$ and $q-$ where $q+ = \mu + \alpha * \sigma$ and $q- = \mu - \alpha * \sigma$, μ is the mean, σ is the variance, and $0 < \alpha < 1$. The RSS value located above $q-$ and below $q+$ will be discarded. In the Jana scheme, the RSS measurement results are divided into smaller blocks. It uses the same threshold as in Mathur, but the latter has the same threshold for all RSS measurement result while the Jana scheme has different thresholds for each block.

3.4 Reconciliation

This phase is used to overcome the bit mismatch due to an imperfect channel reciprocity. We use Bose, Chaudhuri, and Hocquenghem (BCH) codes as proposed in [12] and [13]. As for performance evaluation, we apply BCH (127, 50, 13) with error value that can be corrected by 13 bits in each block. Blocks that are uncorrectable will be discarded so as to reduce the KGR obtained after the quantization process.

3.5 Privacy Amplification

Privacy amplification is required to maintain the integrity of the bit sequence without revealing information to the third parties over a public network. The function of one way is one of the ideal ways for two legitimate users to check the integrity of generated key without revealing information to a third party. We use SHA-1 to hash towards the resulting bit sequence, in which SHA-1 is of high security and often uses one-way function [26]. Alice will send the SHA-1 hash result to Bob, and Bob will also hash the bits of the acquired key. The same hash result shows the same set of key bits.

4. Proposed Quantization Scheme

Our proposed MMB quantization scheme consists of several steps that include:

1. Dividing the measurement data of Alice and Bob into several blocks.
2. Pre-process each block of data using a Kalman method.
3. Perform quantization on each block of data pre-process results, with the range of each level quantization and the resulted Gray Code are:
   a. $Level\,1 = [-\infty, \mu - \alpha * \sigma] = 01$
   b. $Level\,2 = [\mu - \alpha * \sigma, \mu] = 00$
   c. $Level\,3 = [\mu, \mu + \alpha * \sigma] = 10$
   d. $Level\,4 = [\mu + \alpha * \sigma, \mu] = 11$

Where μ is a mean, α is a parameter with range value between 0.01 up 0.06, while σ is the standard deviation.

4. Alice and Bob send the positions of the quantized levels generated and discard the different quantization levels.

5. Experimental Setup

We conduct RSS measurements as a channel parameter in an indoor environment. The measurement is conducted with various distance measurement between Alice and Bob. Each user uses a TL-WN722N adapter and frequency of 2.4 GHz to communicate. In this experiment, Alice acts as an initiator with Access point mode and Bob acts as a responder with station mode. Both of them equipped with Wireshark to conduct capture packets.

5.1 Experimental Environment

There are several experiments performed in RSS measurements, i.e. A, B, C, and D as seen in Figure 3. In all experiments, Alice walking back and forth at a predetermined distance, while Bob and Eve stationary with a distance of 10 cm (more than half the wavelength). The measurement distance variations between Alice and Bob are 1 to 4.12 meters (experiment A), 3 to 5 meters (experiment B), 5 to 6.4 meters (experiment C), and 7 to 8.06 meters (experiment D).

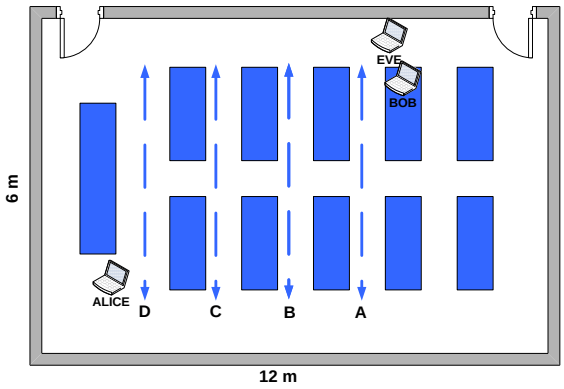

Figure 3. The layout of the experimental setup

5.2 Performance Metrics

This section describes the four metrics of performance used in this experiment, and those are the correlation coefficient, KGR, KDR, and randomness.

5.2.1 Correlation Coefficient

We use this parameter to estimate the linear dependence of RSS measurements between Alice and Bob by assigning values between +1 to -1. The value +1 shows a positive correlation, -1 shows a negative correlation, and 0 indicates no correlation. The correlation coefficient [27] between two measured data is shown in (18).

$$\rho_{A,B} = \frac{\text{cov}(A,B)}{\sigma_A.\sigma_B} = \frac{E[(A-\mu_A)(B-\mu_B)]}{\sigma_A.\sigma_B} \quad (18)$$

Where *cov* is the covariance, σ is the standard deviation, and μ_A, μ_B are the average of measurement between Alice and Bob, while *E* is the expectation.

5.2.2 KGR

KGR refers to the number of bits that can be generated within a given measurement time duration. This metric is often used to determine the quality of key generation schemes. In this experiment, we evaluate three types of KGR i.e. KGR after quantization, reconciliation, and privacy amplification. The notation KGR_{ik} shows the number of bits produced in the duration of measurement time after the quantization process, while KGR_r is obtained from the number of bits that can be corrected in the duration of measurement time after the reconciliation process. The corrected bits will be divided into blocks, where each block must pass the minimum requirement of randomness of the block frequency test and blocks that do not meet the requirement will be discarded. The remaining bits will produce KGR_{pa} .

5.2.3 KDR

We define KDR as the ratio of the total number of mismatch bits between Alice and Bob with the total bits generated from the quantization process.

5.2.4 Randomness

The randomness test is performed using the NIST, in which the test uses the $P-value$ parameter to determine the level of confidence. The resulted key bit series will be perfectly random if $P-value$ is equal to 1. The parameter α value is between 0.001 and 0.01, and the selected α value is 0.01. The resulting key bits pass the randomness requirements, if $P-value \geq \alpha$.

6. Experimental Results and Performance Evaluation

In this section, we will present the experimental result from 4 experiments as well as evaluate the performance of the proposed SKG scheme.

6.1 Experimental Results

The data was collected by ICMP PING package transmission sent from Alice to Bob with a ping interval of 50 ms. The Wireshark application goes on the side of Alice and Bob to store all package received. In this experiment, the number of the package sent is 10,000. Figure 4 shows the probability distribution of Alice and Bob measurements on various experimental variations. The range of RSS values varies for each experiment i.e. 20 to -67 dBm (experiment A), -23 to -68 dBm (experiment B), -33 to -69 dBm (experiment C), and -34 to -70 dBm (experiment D). The experimental results show that the greater the measurement distances the lower the signal strength value, in which the lowest signal strength is obtained when experimenting D that has the farthest measurement distance.

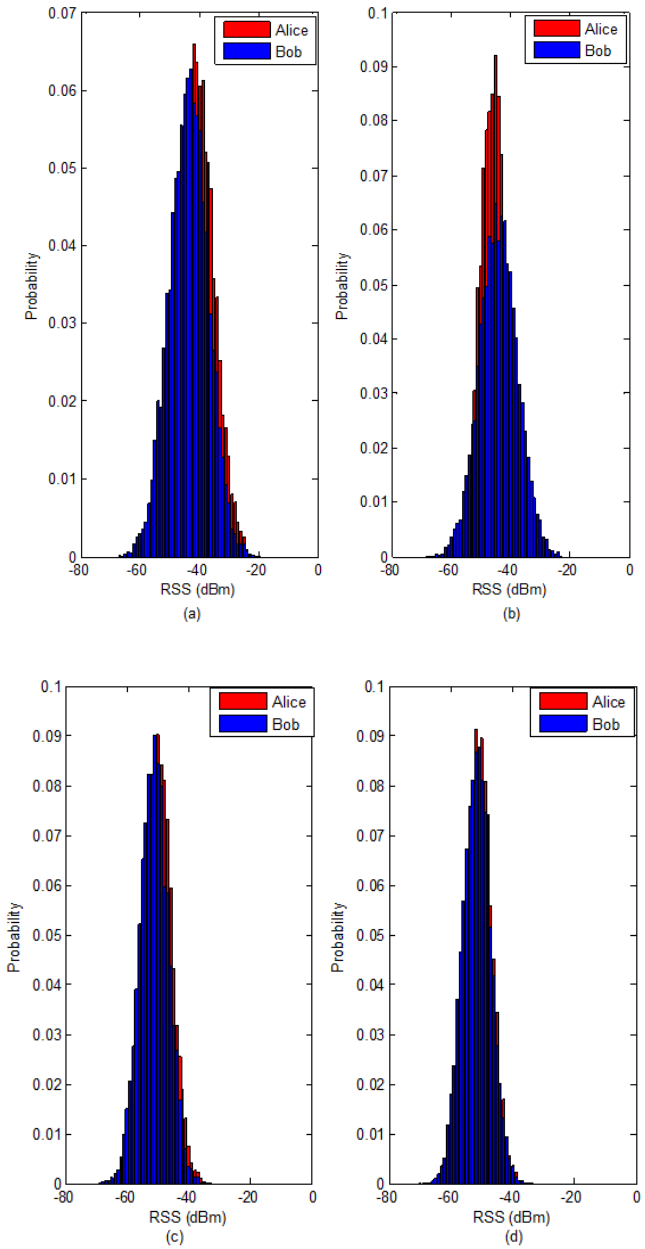

Figure 4. The Probability Distribution of Alice and Bob at experiment (a) A (b) B (c) C (d) D

6.2 Evaluation of Experimental Results

There are 3 sections to be evaluated in this section, which include the effect of using Kalman method on SKG scheme in an indoor wireless environment with various distance measurement and compare the performance between MMB and the other existing quantization scheme.

6.2.1 The Effect of Using Kalman Method on SKG Scheme

The two measured data have a high correlation if the correlation coefficient is more than 0.5 [28]. The correlation coefficient of RSS between Alice and Bob as shown in Table 1 ranges from 0.8396 to 0.5974. Hence, it can be concluded that the two RSS data from the legitimate user has a high correlation value. The farther the measurement distance from two legitimate users, the lower is the correlation coefficient generated. The above result occurs when the measurement distance becomes farther, the signal-to-noise-ratio (SNR) declines, and subsequently, the possibility of two legitimate users generate the same RSS also declines. The correlation coefficient between Eve with Alice and Bob shows a low correlation, because the value is far below 0.5, therefore making it difficult for Eve to get the same key as the two legitimate users.

Table 1. The correlation coefficient of data RSS measurement result

Experiment	Coefficient Correlation $(\rho_{A,B})$	Coefficient Correlation $(\rho_{B,E})$	Coefficient Correlation $(\rho_{A,E})$
A	0.8396	0.0936	0.1050
B	0.7642	0.0744	0.0981
C	0.6924	0.0651	0.0945
D	0.5974	0.0561	0.0795

We use the Kalman method to preprocess the two data of measurement results so as to increase the reciprocity, expressed by the Pearson correlation coefficient. The higher the reciprocity data, the higher is the correlation value. This experiment divides 10,000 RSS measurement data into blocks ranging from 10 to 50 data in each block. The test results in Table 2 shows that the highest reciprocity is obtained when the number of data in the block is 20, with the highest correlation coefficient value obtained when the distance measurement is at 5 meters. An interesting point from using the Kalman method is the improvement of correlation coefficient obtained is not linear with high correlation coefficient, on the contrary, significant increases actually occur at lower correlation coefficient.

Table 2. Improvement of correlation coefficient with Kalman method

Experiment	Actual Coefficient Correlation	Improving Coefficient Correlation with Kalman Scheme			
		10	20	40	50
A	0.8396	0.8792	0.8895	0.8851	0.8894
B	0.7642	0.8520	0.8657	0.8609	0.8648
C	0.6924	0.9031	0.9137	0.9171	0.9027
D	0.5974	0.8868	0.9003	0.8952	0.8964

6.2.2 The Effect of Difference Range Level between MMB and Ambekar

Author [20] tries to overcome the trade-off metric performance problem by conducting a pre-process of the measured RSS data and using a multi-bit system at each level of quantization. In the multi-bit system, each quantization level is converted to binary form by using Gray Code. The range of each level and the resulted Gray Code are:

a) $Level\,1 = \left[-\infty, \mu - \sigma^2/2\right] = 00$

b) $Level\,2 = \left[\mu - \sigma^2/2, \mu\right] = 01$

c) $Level\,3 = \left[\mu, \mu + \sigma^2/2\right] = 11$

d) $Level\,4 = \left[\mu + \sigma^2/2, \infty\right] = 10$

Where μ is the mean, σ^2 is the variance, while the effect of providing a range level towards RSS distribution of pre-processed result between two legitimate users at various experiments is illustrated by Joint Probability in Figure 5 to 8. In this method, the range of each level results in two

legitimate users having the highest level of quantization similarity at a level of 2 and 3. The higher the correlation value of data obtained, the higher is the possibility of similar quantitative level equations so as to decrease the KDR as indicated in Figure 13. However, the weakness of this method lies when the correlation decreases, the difference in the quantization level between two legitimate users also increases significantly in all range level as shown in Figure 5.

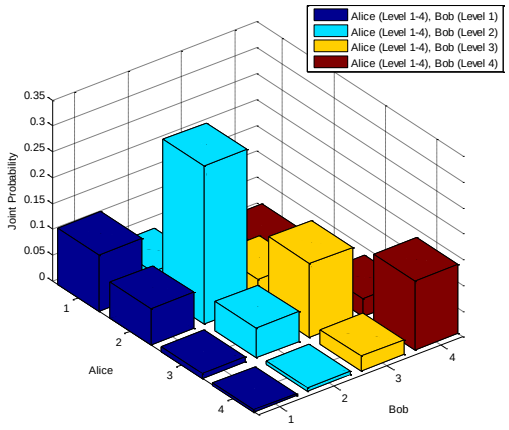

Figure 5. The joint probability distribution of the RSS at experiment A with the Ambekar scheme

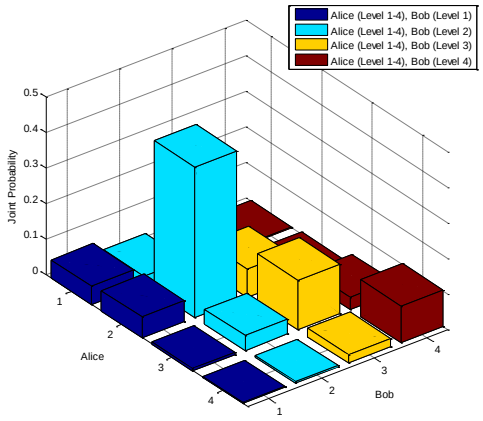

Figure 6. The joint probability distribution of the RSS at experiment B with the Ambekar scheme

Our proposed MMB quantization scheme aims to overcome the problems of Ambekar scheme, by changing the range of each level as shown in section 4. The effect of assigning a range level on RSS distribution of pre-processing result between two legitimate users on different experiments is illustrated by the Joint Probability in Figure 9 to 12. The range of every level with this method results in two legitimate users having the similarity of the highest quantization level between two legitimate users on level 1 and 4. The advantage of this scheme compared to the Ambekar scheme is when the correlation decreases, the difference of quantization level between 2 legitimate users do not increase significantly on all range levels as illustrated clearly in Figure 9 to 12.

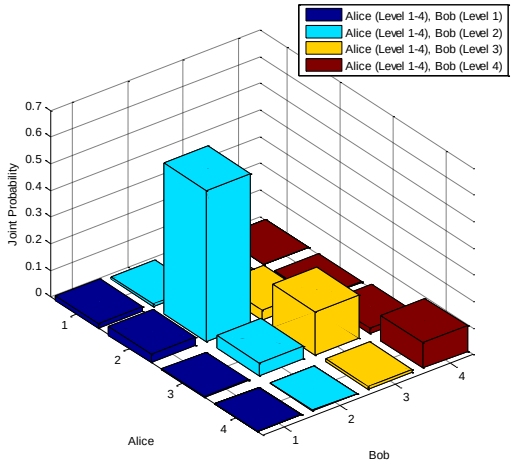

Figure 7. The joint probability distribution of the RSS at experiment C with the Ambekar scheme

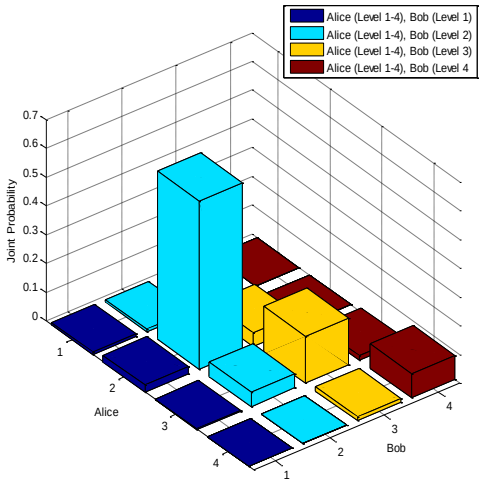

Figure 8. The joint probability distribution of the RSS at experiment D with the Ambekar scheme

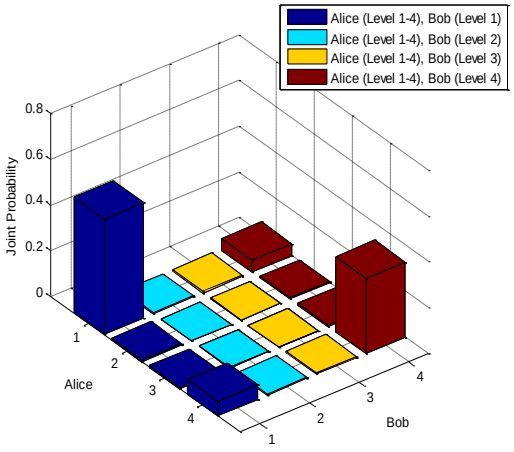

Figure 9. The joint probability distribution of the RSS at experiment A with the MMB scheme

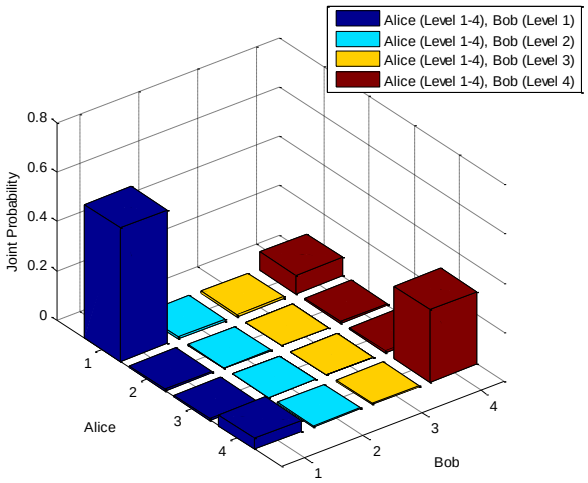

Figure 10. The joint probability distribution of the RSS at experiment B with the MMB scheme

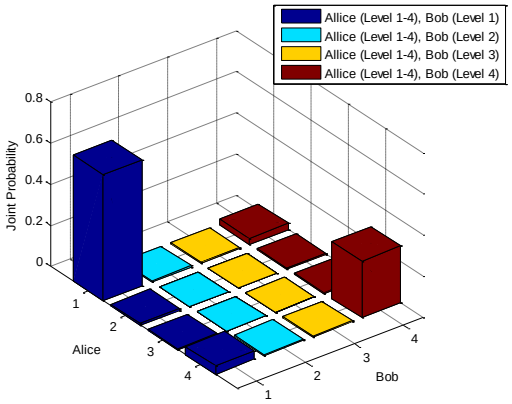

Figure 11. The joint probability distribution of the RSS at experiment C with the MMB scheme

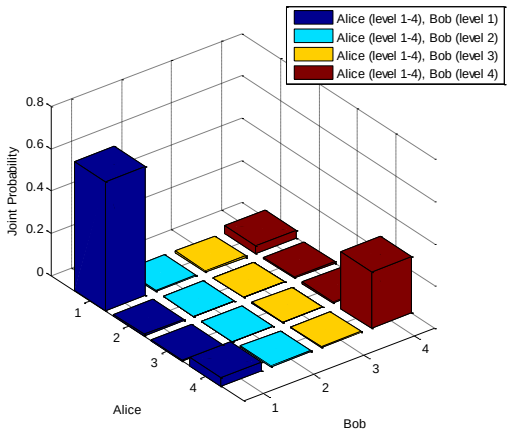

Figure 12. The joint probability distribution of the RSS at experiment D with the MMB scheme

6.2.3 Performance Comparison between MMB and Ambekar Scheme

In this section, we compare the performance of MMB scheme with the Ambekar scheme in terms of KGR, KDR, and randomness. The test results show that our proposed scheme produces better performance than the Ambekar method in terms of KGR and KDR.

The test results in Figure 13 show that our proposed scheme is able to decrease the average $KDR_{pka,pkb}$ by 2.3%, for all experiments variations. This is due to a level range which allows an increase in the number of pre-processing data between two legitimate users on the same level. The test result also shows that the higher the correlation coefficient, the lower is the KDR, wherein the lowest KDR is resulted in when the distance measurement is 5 to 6.4 meters (experiment C).

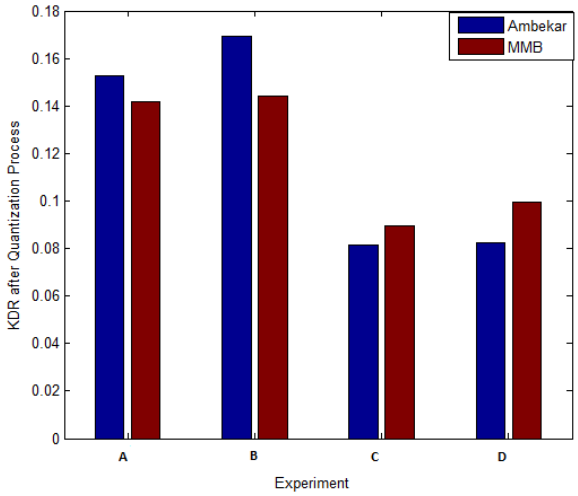

Figure 13. Comparison KDR between MMB and Ambekar Scheme

There is no significant difference in KGR_{ik} between MMB and Ambekar scheme on all distance variations, with an average KGR yield of 39 Mbps. The decrease in KDR has an indirect effect on the increasing KGR. Lower KDR will result in higher KGR, because of the lower the KDR, the less likely it is for the data block to be discarded, mainly due to the inability of the error correcting technique to reconcile the wrong data. There is also no significant difference between KGR_r of both schemes as shown in Figure 14. The lowest KGR_r occurs at a measurement distance of 3 to 5 meters (experiment B), in which at this distance, the test result indicates the highest KDR as illustrated in Figure 13. The comparison result of KGR_{pa} in Figure 15 shows that our proposed scheme compared to Ambekar is able to increase KGR_{pa} between 3.2% to 32.74%, for all experiment variations. The test results on our proposed scheme also show that there is no significant decrease from KGR_r to KGR_{pa}. This condition occurs because a lot of data blocks of correction results are able to meet the randomness requirements so they don't need to be discarded.

To ensure the randomness of the bits generated by the MMB scheme, we also run a randomness test using NIST suite. We divide the reconciliation bits into blocks, each contains 128 bits. Table 3 shows that the value of randomness tests on all distance variations is above 0.01. Therefore, it can be concluded that the secret key bits generated are completely random with a 99% confidence level. A frequency test is used to determine whether the sum of 1 and 0 in a series of key bits is the same, whereas a block test frequency is used to

test whether the frequency of bit 1 in block M is *M/2*. The value obtained from this table is the key bit that has the highest value of frequency block.

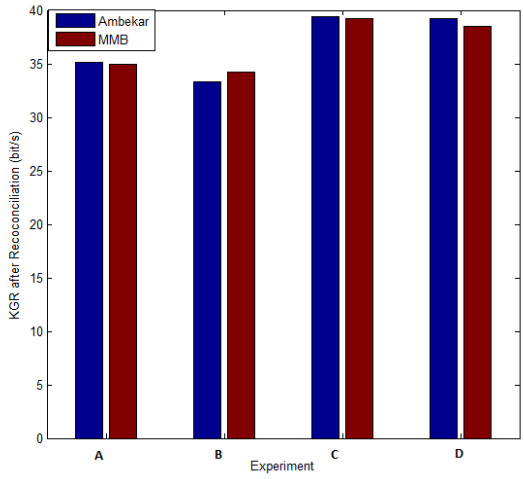

Figure 14. Comparison KGR_r between MMB and Ambekar Scheme

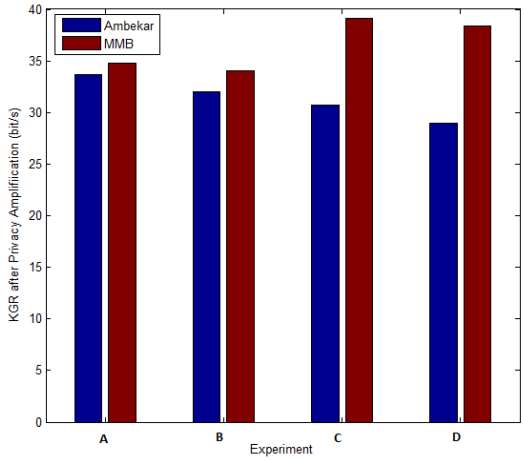

Figure 15. Comparison KGR_{pa} between MMB and Ambekar Scheme

Table 3. NIST test for Ambekar and MMB scheme

Experiment	Ambekar		MMB	
	Frequency	Block Frequency	Frequency	Block Frequency
A	0.7909	0.9609	0.9296	0.9999
B	0.1329	0.9953	0.7909	0.9999
C	0.1824	0.9998	0.7909	0.9999
D	0.1849	0.9953	0.9296	0.9999

6.2.4 Performance Comparison between MMB and Other Existing Schemes

In this section, we compare the performance of MMB with other existing schemes. The MMB quantization scheme is conducted after pre-process measurement data mechanism using the Kalman method, while another quantization scheme is conducted directly after a measurement data is obtained. In MMB quantization scheme, we select parameter α is 0.01, with the objective that the KDR remains low and a series of bits obtained still meets the requirements of randomness. There are 3 parameters used in Mathur scheme, in which the parameters include *q+*, *q-*, and *m*. To make sure that the number of the bits removed is not too large, we determine that the parameter value of *m* used is 3 and α is 0.2. In Jana quantization and Jana Multi-bit scheme, we use the same parameter *m* and α as in Mathur scheme. In Jana Multi-bit quantization scheme, we only extract every RSS data into two bits.

The performance comparison of several quantization schemes can be seen in Table 4 to 7. The Aono scheme produces a higher KGR when compared to other existing quantization schemes; however, the resulted KDR is also significantly increased for all variations of the experiment. The lowest KDR is obtained when we use the Mathur scheme, but the resulted KGR is also significantly low. The Jana scheme also produces KDR that is almost the same as that of Mathur, but the KGR is still higher. One interesting point of this experiment is that the resulted KGR from Jana Multi-bits, in which KGR_{ik} and KGR_r generated from Jana Multibit, is still higher than the KGR obtained from Mathur and Jana scheme, however at the time of KGR_{pa}, the value produced is lower than that of Mathur and Jana schemes. This is because many data blocks are discarded due to inability to fulfill the randomness requirements. Compared to the other existing schemes, the MMB produces the highest KGR. The resulted KDR is also lower than that of Aono and is comparable with those of Jana and Mathur when the distance measurement is 5 to 6.4 meters (experiment C), and 7 to 8.06 meters (experiment D).

Table 4. KDR between MMB and other existing schemes

Experiment	Aono	Jana	Jana MultiBit	Mathur	MMB
A	0.1524	0.0017	0.0246	0.0026	0.1417
B	0.1893	0.0058	0.0402	0.0058	0.1442
C	0.2203	0.0040	0.0928	0.0040	0.0896
D	0.2632	0.0219	0.1642	0.0218	0.0993

Table 5. KGR_{ik} between MMB and other existing schemes

Experiment	KGR_{ik} (bit/s)				
	Aono	Jana	Jana MultiBit	Mathur	MMB
A	17.848	2.288	4.628	0.764	39.922
B	17.286	2.06	3.882	0.688	39.926
C	16.688	1.49	3.428	0.498	39.926
D	16.664	1.37	3.284	0.458	39.939

Table 6. KGR_r between MMB and other existing schemes

Experiment	KGR_r (bit/s)				
	Aono	Jana	Jana MultiBit	Mathur	MMB
A	17.4	2.2	4.6	0.7	35
B	16.5	2	3.8	0.6	34.2
C	15.1	1.4	3.2	0.4	39.2
D	13.8	1.3	2.9	0.4	38.5

We also conduct randomness test on data bits generated by Aono, Jana, Jana multi-bit and Mathur quantization schemes. In the same way as the description in Table 4, we performed Frequency and Frequency Block test. The result of the tests performed on Tables 8 and 9 shows that all data bits have

met the randomness requirements since the $P-value$ obtained is above 0.01.

Table 7. KGR_{pa} between MMB and other existing schemes

Experiment	KGR_{pa} (bit/s)				
	Aono	Jana	Jana MultiBit	Mathur	MMB
A	17.152	1.536	0.768	0.512	34.816
B	16.384	1.024	0.256	0.512	34.048
C	14.848	0.768	0.512	0.256	39.168
D	13.568	0.768	1.024	0.256	38.4

Table 8. NIST test for Aono and Mathur scheme

Experiment	Aono		Mathur	
	Frequency	Block Frequency	Frequency	Block Frequency
A	0.1875	0.9847	0.0625	0.8487
B	0.1875	0.9609	0.5000	0.8487
C	0.0625	0.9609	0.3750	0.8487
D	0.0625	0.9847	1.2500	0.9170

Table 9. NIST test for Jana and Jana Multibit scheme

Experiment	Jana		Jana Multibit	
	Frequency	Block Frequency	Frequency	Block Frequency
A	0.0625	0.1531	0.6875	0.0138
B	0.1250	0.1014	0.8125	0.0239
C	0.0625	0.0648	0.2500	0.1014
D	1.1875	0.2224	0.6875	0.0648

7. Conclusion

In this paper, we have been investigating the effect of using Kalman method at SKG scheme in indoor wireless environments on various experiments. The results of the tests show that there is a correlation improvement of the two measured data, with significant increases occurring at a distance of 5 to 6.4 meters (experiment C), and 7 to 8.06 meters (experiment D). Our SKG scheme that proposed the combination of pre-processing and MMB quantization methods also has the ability to overcome the trade-off metric performance problem, resulting in low KDR but still yielding high KGR, and performing better performance when compared with another existing quantization method.

8. Acknowledgement

This research was supported by Institut Teknologi Sepuluh Nopember (ITS) through Laboratory Research Grant (Penelitian Laboratorium) Scheme 2017.

References

[1] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, Vol. 4, pp. 614–626, 2016.

[2] A. Sadeghi, M. Zorzi, and F. Lahouti, "Analysis of key generation rate from wireless channel in in-band full-duplex communications," *2016 IEEE Int. Conf. Commun. Work.*, Kuala Lumpur, Malaysia, pp. 104–109, 2016.

[3] M.I. Khalil, "Quaternion-based encryption/decryption of audio signal using digital image as a variable key," *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 9, No. 2, pp. 216-221, 2017.

[4] G.V. Mini, and K.S. A. Viji, "A comprehensive cloud security model with enhanced key management, access control and data anonymization features," *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol.9, No.2, pp.263-272, 2017.

[5] R. Aouinatou, M. Belkasmi, and M. Askali, "A dynamic study with side channel against an identification based encryption," *International Journal of Communication Networks and Information Security (IJCNIS)*,Vol. 7, No. 1, pp. 8-19, 2015.

[6] B. Zan, M. Gruteser, and F. Hu, "Improving robustness of key extraction from wireless channels with differential techniques," *2012 Int. Conf. Comput. Netw. Commun. ICNC'12*, Maui, HI, USA, pp. 980–984, 2012.

[7] M. Yuliana, Wirawan, and Suwadi, "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, 2017.

[8] S. N. Premnath, S. Jana, J. Croft, P.L. Gowda, M. Clark, S.K. Kasera, N. Paatwari and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mob. Comput.*, Vol. 12, No. 5, pp. 917–930, 2013.

[9] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wirel. Commun.*, Vol. 18, No. 4, pp. 6–12, 2011.

[10] J. Zhang, R. Woods, T.Q.Duong, A. Marshall, and Y. Ding, "Experimental study on channel reciprocity in wireless key generation ", *2016 IEEE 17th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, Edinburgh, UK, pp. 1-5,2016.

[11] Y. Liu, S. C. Draper, and A. M. Sayeed, ''Exploiting channel diversity in secret key generation from multipath fading randomness,'' *IEEE Trans. Inf. Forensics Security*, Vol. 7, No. 5, pp. 1484–1497, Oct. 2012.

[12] K. Liu, "On enhancements of physical layer secret key generation and its application in wireless communication systems", *Electronic Thesis and Dissertation Repository*. 3342, 2015.

[13] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: An efficient key generation protocol with artificial interference," *IEEE Trans. Inf. Forensics Security*, Vol. 8, No. 11, pp. 1731–1745, 2013.

[14] R. Guillaume, C. Zenger, A. Mueller, C. Paar, and A. Czylwik, "Fair comparison and evaluation of quantization schemes for PHY-based key generation," *OFDM 2014, 19th Int. OFDM Work. 2014 (InOWo'14); Proc.*, Essen, Germany, pp. 1–5, 2014.

[15] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, ''Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel,'' *in Proc. 14th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, San Francisco, CA, USA, pp. 128–139, Sep. 2008.

[16] T. Castel, P.V. Torre, H. Rogier, "RSS-based secret key generation for indoor and outdoor WBANs using on-body sensor nodes", *2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, Belgium, pp. 1-5, 2016.

[17] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, Vol. 16, No. 3, pp. 1550-1573, Aug. 2014.

[18] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mob. Comput.*, Vol. 12, No. 9, pp. 1842–1852, 2013.

[19] S. T. Ali, V. Sivaraman, and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Trans. Mob. Comput.*, Vol. 13, No. 12, pp. 2763–2776, 2014.

[20] A. Ambekar, M. Hassan, and H. D. Schotten, "Improving channel reciprocity for effective key management systems,"

Conf. Proc. Int. Symp. Signals, Syst. Electron., Potsdam, Germany, pp. 1–4, 2012.

[21] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *IEEE Trans. on Information Forensics and Security*, Vol. 5, No. 2, pp. 240–254, 2010.

[22] Q. Wang, H. Su, K. Ren, and K. Kim, ''Fast and scalable secret key generation exploiting channel phase randomness in wireless networks,'' *in Proc. 30th IEEE Int. Conf. Comput. Commun. (INFOCOM),* Shanghai, China, pp. 1422–1430, Apr. 2011.

[23] Q. Wang, K. Xu, and K. Ren, ''Cooperative secret key generation from phase estimation in narrowband fading channels,'' *IEEE J. Sel. Areas Commun.*, Vol. 30, No. 9, pp. 1666–1674, Oct. 2012.

[24] H. Liu, J. Yang, Y.Wang, and Y. Chen, ''Collaborative secret key extraction leveraging received signal strength in mobile wireless networks,'' *in Proc. 31st IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Orlando, FL, USA, pp. 927–935, Mar. 2012.

[25] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, ''Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels,'' *IEEE Trans. Antennas Propag*., Vol. 53, No. 11, pp. 3776–3784, Nov. 2005.

[26] J. Zhao *et al.*, "Efficient and secure key extraction using CSI without chasing down errors," *arXiv Prepr. arXiv1208.0688*, pp.1-9, 2012.

[27] D.Lavrova and A.Pechenkin, "Applying correlation and regression analysis to detect security incidents in the internet of things," *International Journal of Communication Networks and Information Security (IJCNIS)*, Vol. 7, No. 3, pp.131-137, December 2015.

[28] S. T. Ali and V. Sivaraman, "Secret key generation rate vs . reconciliation cost using wireless channel characteristics in body area networks," *2010 IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing Secret*, Hong Kong, China, pp. 644-650, 2010.