International Journal on Advanced Science Engineering Information Technology

Vol.9 (2019) No. 1
ISSN: 2088-5334

Performance Analysis of Loss Multilevel Quantization on the Secret Key Generation Scheme in Indoor Wireless Environment

Mike Yuliana[#,*], Wirawan[#], Suwadi[#]

[#] *Dept. of Electrical Engineering, Faculty of Electrical Technology, Institut Teknologi Sepuluh Nopember*
Jalan Raya ITS, Keputih, Sukolilo, Surabaya 60111, Indonesia
E-mail: mike16@mhs.ee.its.ac.id; wirawan@ee.its.ac.id; suwadi@ee.its.ac.id

[*]*Dept. of Electrical Engineering, Politeknik Elektronika Negeri Surabaya (PENS)*
Kampus PENS, Jalan Raya ITS, Keputih, Sukolilo, Surabaya 60111, Indonesia
E-mail: mieke@pens.ac.id

***Abstract*—The necessity for secured communication devices that has limited computing power has encouraged the development of key generation scheme. The generation of a symmetric key scheme that utilizes randomness of wireless channels offers a most promising solution as a result of the easy distribution of secret key mechanisms. In the last few years, various schemes have been proposed, but there are trade-offs between the performance parameters used. The expected parameters are the low Key Disagreement Rate (KDR), the high Key Generation Rate (KGR), and the fulfillment of standard of randomness. In this paper, we propose the use of a combination of pre-processing methods with multilevel lossy quantization to overcome the trade-off of performance parameters of the Secret Key Generation (SKG) scheme. Pre-process method used to improve reciprocity so as to reduce KDR, whereas multilevel quantization is used to improve the KGR. We use Kalman as the pre-processing method and Adaptive Quantization, Modified Multi-Bit (MMB), and 2-ary Quantization as the multilevel lossy quantization. Testing is conducted by comparing the performance between direct quantization with the addition of the pre-processing method in various multilevel lossy quantization schemes. The test results show that the use of Kalman as pre-processing methods and multilevel lossy quantization can overcome the trade-off performance parameters by reducing KDR and increasing KGR, with the best performance, was obtained when we use adaptive quantization. The resulting secret key has also fulfilled 6 random tests with p values greater than 0.01.**

***Keywords*— KDR; KGR; secret key generation; Kalman; multilevel lossy quantization.**

I. Introduction

In modern communication systems, data security efforts are crucial, especially for communication in wireless networks [1]-[5]. This underlines the need for a shared secret key to secure communication through the public network. Public key cryptography method is often used to build a secret key management system [6], but it relies on a problematic computation that is less attractive to most of Internet of Thing (IoT) applications [7]-[14]. Also, as the number of devices increases, the complexity of the secret key distribution also increases. The most appropriate solution to solve the problem is the secret key generation (SKG) scheme that utilizes the randomness of the wireless channel to get the secret key [15]-[20].

There are three properties of wireless channels that can be utilized to improve the secret key, i.e. reciprocity, variations in temporal and spatial variations. Reciprocity shows the similarity of multipath properties of the radio channel (gain, phase shift, and delay) of each user. Switching devices, human movement as well as objects will result in changes in multipath channels known as temporal variations. Another property of radio channels is the location uniqueness of two legitimate users. Eavesdroppers that are in the third location and more than half the wavelength of legitimate users will get different measurement results [21]-[24].

Some research shows that the secret key generation schemes run on two wireless devices using 802.11a radio can generate a secret key up to 1 bps [25]-[26]. These conditions resulted in the inability of the key length produced to achieve the minimum length of important keys due to a possible lost connection. The encryption method of Advanced Encryption Standard (AES) with a minimum length of 128-bit keys requires at least 2 minutes for generating the secret key. This serves as the basis for several new studies to increase the rate of key generation.

One viable solution to increase the key generation rate is using devices with multiple antennas [27]. However, this requires the addition of new protocols to ensure the success of the secret key generation mechanism. Another viable way without the addition of a new protocol is the optimization of multilevel schemes [28]-[30] either with a lossless or loss scheme. A lossless quantization scheme maps some wireless channel samples into some bits. No samples are discarded so the key generation rate can increase, but bit matches between two users may decrease. The loss scheme discards some samples that are located inside the interval guard. This scheme can increase the bit match between two users but the key generation rate decreases.

In general, three performance parameters are often used to determine the success of established secret key generation scheme, i.e., Key Generation Rate (KGR), Key Disagreement Rate (KDR), and randomness [31]. KGR shows the number of key bits generated in the duration of the measurement. KDR indicates a mismatch of quantization bits, whereas randomness indicates the randomness value of the secret key generated. As indicated by [29] and [31] there is always a trade-off between those parameters. Some researchers used a lossless scheme to increase KGR, but the resulting KDR would also increase; other researchers used a loss scheme to lower the KDR, but it resulted in a decrease in KGR. Because the secret key generation scheme aims to generate identical keys between two users, the quantization that generates high KDRs is not often used. Some researchers used pre-process schemes to improve the reciprocity channel in order to decrease KDR [30]. To overcome the problem of multilevel performance parameters, the use of a combination of pre-processing schemes with multilevel quantization can be considered to obtain low KDR while still obtain high KGR.

In this paper, we will prove that the use of a combination of pre-processing methods with quantization of multilevel loss can overcome trade-off performance parameters as compared to the use of multilevel quantization directly. We used Kalman for the pre-processing method because this method can improve the reciprocity even to data that have a low correlation [28]. Our specific research contributions are:

- Conducting a performance analysis of the SKG scheme that performs a combination of the Kalman method with a multilevel loss scheme in an indoor environment. We used all the existing multilevel loss quantization schemes. To our knowledge, our research was the first that focused on performance comparisons of a multilevel loss quantization scheme. In addition to the research conducted by [28], we included the security factor by ensuring that the correlation of eavesdroppers did not exceed 0.5 and KDR exceed 0.25 (25%). With such a correlation and KDR value, eavesdroppers would not get the same key as legitimate users.
- Presenting the experimental results on performance comparisons between direct quantization methods and the addition of the Kalman method before quantization. The test results showed an increase in both KGR and KDR performance parameters with the addition of Kalman before quantization. KDR between a legitimate user and eavesdropper even increased to increase the security factor of the scheme built.

The remainder of this paper is organized as follows. Section 2 describes the material and method. Section 3 presents the results and discussion. Finally, section 4 presents the conclusion.

II. Material And Method

In this section will be explained in detail about the model, system design, and performance parameters used. The system model is used to determine the communication system carried out by legitimate users and tappers. The system design shows the steps used to generate the secret key along with the algorithm used, while the performance parameters are used to show the success of the system being built.

A. *Principle and Preliminaries*

This paper used a system model as shown in Fig. 1. The wireless communication system carried out by two legitimate users was Alice and Bob and an eavesdropper as a third party, i.e., Bob. The channel characteristics measured by Alice was h_A and h_B for Bob. Based on the principle of channel reciprocity that shows the similarity of channel characteristic, if the measurement is conducted in coherence time, it can be argued that $h_A \approx h_B$ [25], [26]. Some measurements n obtained by Alice and Bob are shown in Equation (1) and (2).

$$h_A = [h_A(1) + h_A(2) + h_A(3) + ... + h_A(n)] \tag{1}$$

$$h_B = [h_B(1) + h_B(2) + h_B(3) + ... + h_B(n)] \tag{2}$$

It is assumed that Eve was more than half the wavelength of two legitimate users so and was not correlated with and, in which was a channel characteristic measured by Eve from Alice and was a channel characteristic measured by Eve from Bob. Some measurements obtained by Eve are shown in Equation (3) and (4).

$$h_E = [h_E(1) + h_E(2) + h_E(3) + ... + h_E(n)] \tag{3}$$

$$h_E^{'} = [h_E^{'}(1) + h_E^{'}(2) + h_E^{'}(3) + ... + h_E^{'}(n)] \tag{4}$$

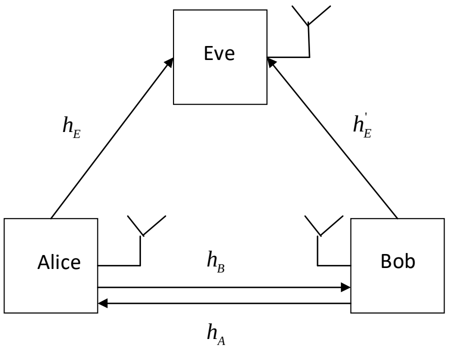

Fig. 1 System model

The coherence time T_c obtained from Equation (5) is the period in which two channel characteristics have a high correlation with the channel assumed to be fixed. Some of the parameters that determine T_c are maximum Doppler shift f_D as shown in Equation (6), the speed of the user defined by v and $\lambda = c / f_c$. Probing channel mechanism affected by the probing rate is r_p and the sampling rate is r_s [32]. Probing rate is the interval between the probing request and reply, and the sampling rate is the interval between the probing requests with one another. Measurement results are expected to meet the requirements of randomness then $r_s^{-1} > T_c$ while channel reciprocity will be fulfilled if $r_p^{-1} < T_c$.

$$T_c = \frac{1}{f_D} \tag{5}$$

$$f_D = \frac{v}{\lambda} \tag{6}$$

The SKG diagram block used to generate the secret key is based on the model proposed by [30] and shown in Fig. 2. There are six stages used to generate keys, which include channel probing, pre-process, quantization, information reconciliation, privacy amplification, and verification. Channel probing aims to collect channel characteristics within a certain time duration. We use received signal strength (RSS) as channel characteristics. Pre-process aims to increase the reciprocity of channel characteristics between two users, with the goal to reduce the KDR. Quantization used to change the channel characteristics of the pre-process results into bits, reconciliation of information will correct bit errors that occur between two users, privacy amplification will increase the quality of the resulting key to meet the entropy requirements, and the last stage, i.e. verification will ensure the secret key generated by two users is the same.

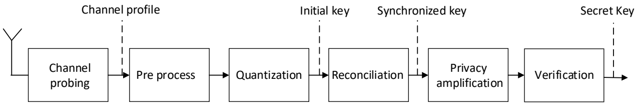

Fig. 2 SKG diagram block

B. System Design

We built the SKG scheme by the design shown in Fig. 2, where the scheme was implemented on 3 Raspberry Pi model B which acted as Alice, Bob and Eve. Alice acted as an initiator while Bob acted as a responder. Each device was equipped with a TP-Link TL-WN722N WiFi USB adapter and operated in 802.11b mode. The carrier frequency used was 2.4 GHz, while in the probing channel mechanism a periodical ping request was sent from Alice to Bob every 110 ms as shown in Fig. 3. In this research, the coherence time that must be fulfilled was 104.16 ms (if we assumed $v = 1.2 m/s$ and $\lambda = \frac{3.10^8}{2.4.10^9} \approx 0.125$ m, then $f_D = \frac{1.2}{0.125} \approx 9.6 Hz$, so that $T_c = 1/9.6 = 104.16$ ms). The periodical ping request has exceeded the coherence times. Therefore the randomness requirements were met. Eve as eavesdropper would also get a pair of the ping request and response.

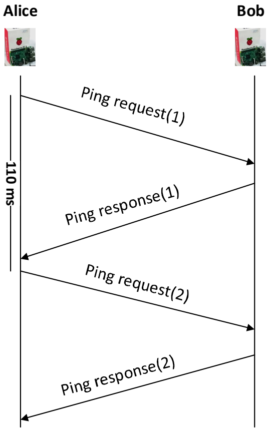

Fig. 3 Probing channel mechanism

Data from the probing channel was recorded using Wireshark software and divided into blocks of data containing 50 samples before entry into the pre-processing stage. The pre-processing stage was performed using the Kalman method as proposed by [33] to increase the signal resemblance for each data block.

In contrast to [20], we focused on split data blocks by BCH code to be used so it would show the level of influence of Kalman use towards performance improvement scheme built SKG. The next step was the quantization mechanism using the multilevel loss scheme proposed by [27], [28], and [33]. To overcome the bit mismatch caused by imperfect reciprocity, we used a BCH code at the information reconciliation stage. The BCH code used was (127.50). Before starting the privacy amplification stage, the number of samples in 1 block of data was converted to 256. This change aimed to adjust the number of bits in a data block to match the expected secret key length for AES of 256 bits. Universal Hash Function [29] used in the privacy amplification stage was to increase the entropy of the generated key. The selected data blocks were blocks of data that had the highest entropy. The final stage was verifying to ensure the secret key generated between two users was the same. Verification was done by sending a hash generated from SHA-256.

C. Performance Parameter

Four parameters of performance will be used to determine the success of the system is built, where the parameter includes the value of the Pearson correlation coefficient generated, KDR, KGR, and randomness. Detailed explanations of each parameter can be seen in the following summary.

1) Pearson Correlation

In this research, Pearson's correlation derived from Equation (7) was used to show the dependence between Alice and Bob measurement data. The resulting value ranged from 1 to -1, where the value 1 indicated absolute dependence whereas the value -1 denotes an opposite dependency.

$$\rho_{AB} = \frac{\sum_{i=0}^{n-1}(A_i - \overline{A})(B_i - \overline{B})}{\sqrt{\sum_{i=0}^{n-1}(A_i - \overline{A})^2}\sqrt{\sum_{i=0}^{n-1}(B_i - \overline{B})^2}} \quad (7)$$

Where $\overline{A} = \frac{1}{n}\sum_{j=0}^{n-1} A_j$, while $\overline{B} = \frac{1}{n}\sum_{j=0}^{n-1} B_j$.

2) KDR

This parameter was used to measure the resulting mismatch bits after quantization. The value obtained was the ratio between the different bits b_e to the total bits b generated after quantization as shown in Equation (8). An increase in the value obtained would increase the workload from the information reconciliation phase to make a bit correction.

$$KDR = \frac{b_e}{b} \quad (8)$$

3) KGR

This parameter was used to determine how fast Alice and Bob can generate the same key. There were 2 types of KGR to calculate, i.e., KGR included KGR after quantization (KGR_{ik}) and KGR after reconciliation (KGR_r). KGR after quantization was performed to determine the efficiency of the quantization scheme as indicated by the number of bits of the initial key. KGR after reconciliation was used to determine the number of bits of synchronized keys.

4) Randomness

There were 6 types of randomness tests from the National Institute of Standards and Technology (NIST) that were used to validate the generated secret key. The tests were the frequency test, block frequency test, runs test, the longest run of ones in a block test, approximate entropy test, and cumulative sums (cusum) test. For each test, the value p was used to determine the quality of the generated secret key, while the significance level α was used to determine the boundary between random and non-random. If the value was $p \geq \alpha$, then the key to otherwise fulfilled the requirements of randomness. NIST recommended values from 0.001 to 0.1 ($0.001 \leq \alpha \leq 0.01$) which shows the randomness of the key was true with a probability of 99%. For cryptographic applications, the value chosen was 0.01 [34].

III. Results and Discussion

We conducted the test in an indoor environment to find out the performance of the combination of the Kalman method and a multilevel loss quantization scheme. The number of samples was 10,000.

A. Experimental Environment

The test was conducted during the day with a temperature of 24^{o} Celsius in a room of 14.72-meters long by 8-meters wide. Alice walked according to the trajectories shown in Fig. 4 with a speed of about 1.2 m/s, while Bob and Eve were stationary at a very close distance (5 cm). The room consisted of a table, chair, and a glass cabinet. A glass cabinet blocked Alice and Bob. Nobody passed by the time of measurement. There were 3 experiments in this research, i.e., experiment 1, experiment 2 and experiment 3. Alice started the probing channel at a distance of 7.8 m (experiment 1), 9 m (experiment 2), and 10.8 m (experiment 3) Bob. In each test, Alice went straight to the variations in the distance between 7.8 m to 8.7658 m (experiment 1), 9 m to 9.8489 m (experiment 2), 10.8 m up to 11.5169 m (experiment 3).

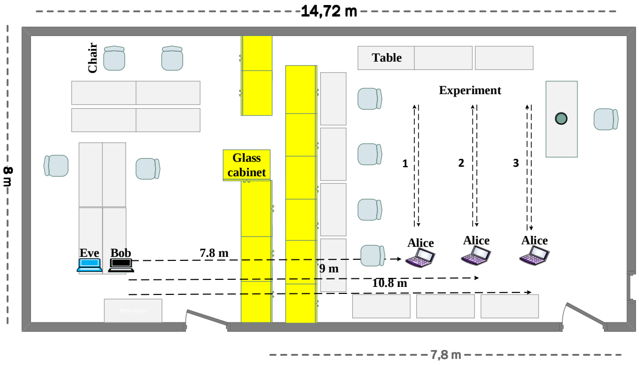

Fig. 4 Probing channel mechanism

B. Performance Analysis

The determination of the SKG scheme performance is carried out by testing in an indoor environment with various measuring distances. The tests included an increased correlation using Kalman, and the performance comparison between the uses of Kalman before quantization with direct quantization. The first test was conducted to determine how much influence the use of Kalman to increase reciprocity of legitimate users and eavesdropper. The second test was conducted to determine the comparison of performance between the use of pre-processing methods and direct quantization on various quantization schemes.

1) Improved Correlation Using Kalman

The results of the RSS measurement value of two legitimate users in all experiment ranged between -77 dBm to -48 dBm, the initial correlation for each experiment can be seen in Table 1. The correlation value is considered high if the resulting correlation coefficient is greater than 0.5 [35]. In this research, the correlation value generated between Alice and Bob in all scenarios was greater than 0.5, whereas the correlation value between legitimate users and the eavesdroppers was minimal, i.e., below 0.5. This resulted in the difficulty of eavesdroppers to get the same key as Eve. The measurement results showed that as the distance increased, the RSS data between Alice and Bob became increasingly different; consequently, the correlation was also lower. Detailed correlation values from RSS are shown in Fig. 5-7. The correlation value was obtained from the RSS data block, with each block containing 50 RSS data. The selection of the amount of data for each of these blocks was adjusted to the BCH code used, i.e. (127.50). The test results show that the average correlation value of RSS data blocks between legitimate users mostly exceeded 0.5, whereas the correlation with eavesdroppers was mostly below 0.1.

TABLE I
CORRELATION COEFFICIENT OF MEASUREMENT RESULTS

Experiment	User	Correlation Coefficient
1	Alice-Bob	0.8056
	Alice-Eve	0.0073
	Bob-Eve	0.0140
2	Alice-Bob	0.6961
	Alice-Eve	0.0153
	Bob-Eve	0.0112
3	Alice-Bob	0.6549
	Alice-Eve	0.0079
	Bob-Eve	0.0059

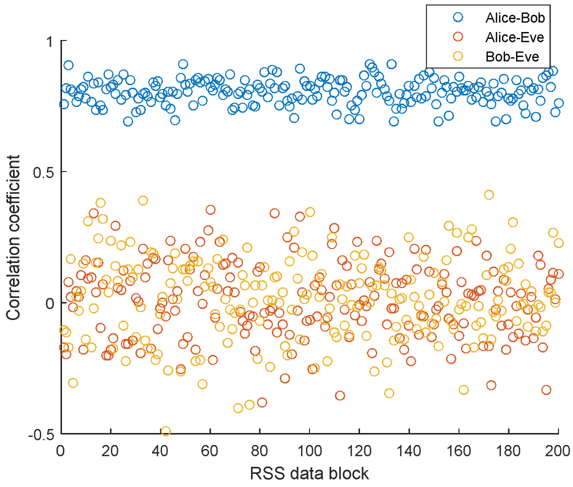

Fig. 5 The correlation coefficient of RSS data block on experiment 1

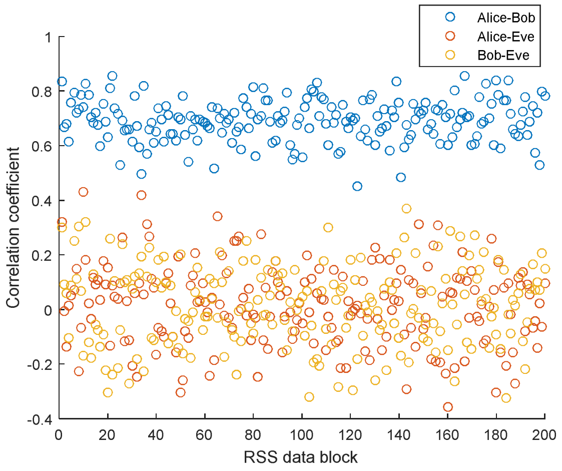

Fig. 6 The correlation coefficient of RSS data block on experiment 2

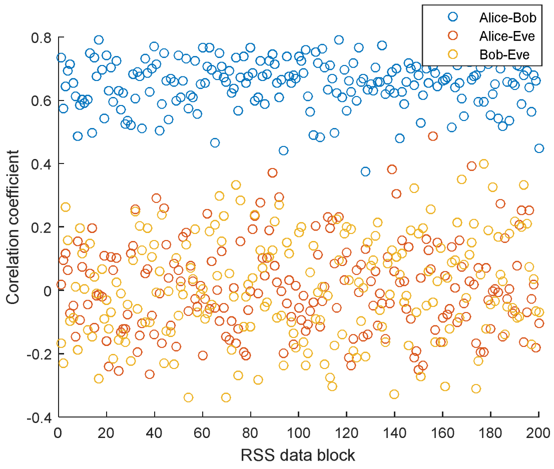

Fig. 7 The correlation coefficient of RSS data block on experiment 3

We used the Kalman method to improve the reciprocity of RSS data between two legitimate users. An increase in the correlation coefficient indicated increased reciprocity. In contrast to research conducted by [20], in this paper, we also included the security factor by ensuring that the correlation of the eavesdroppers did not exceed 0.5. In addition to improving the correlation coefficients of legitimate users, the use of pre-processing methods can also improve the correlation coefficient of eavesdroppers. There was an increase in the correlation of legitimate users as well as eavesdroppers in all scenarios as shown in Table 2. However, the increase did not happen to the data Eve got from Bob. The resulting correlation coefficient tends to decline in all scenarios. This condition occurs because data Eve obtained from Bob tends to be static, while Bob's RSS data as a legitimate user tends to be dynamic. We also show improved correlation results for each of the RSS data blocks in Fig. 8-10. Overall legitimate user data experienced significant improvements, especially in experiment 2 and 3. Eavesdropper data in this case Eve's RSS data obtained from Alice also rose, but most still below 0.5.

TABLE II
IMPROVED CORRELATION COEFFICIENT OF MEASUREMENT RESULTS

Experiment	User	Correlation Coefficient
1	Alice-Bob	0.8522
	Alice-Eve	0.2408
	Bob-Eve	-0.2227
2	Alice-Bob	0.7671
	Alice-Eve	0.2033
	Bob-Eve	-0.1513
3	Alice-Bob	0.7431
	Alice-Eve	0.2262
	Bob-Eve	-0.1390

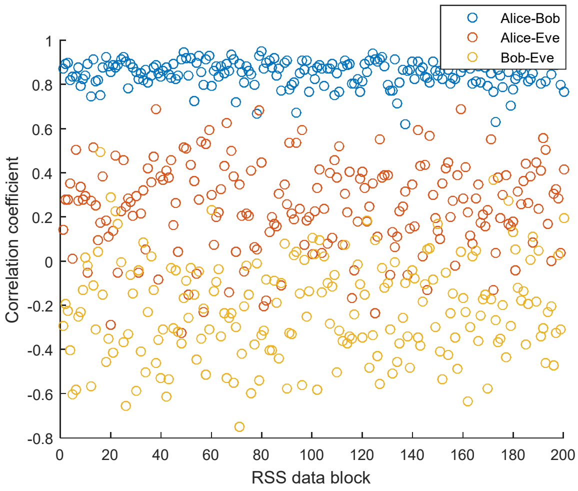

Fig. 8 Improvement of the correlation coefficient in experiment 1

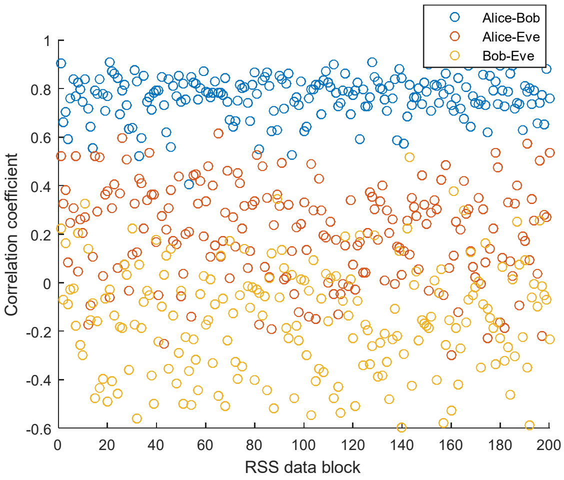

Fig. 9 Improvement of the correlation coefficient in experiment 2

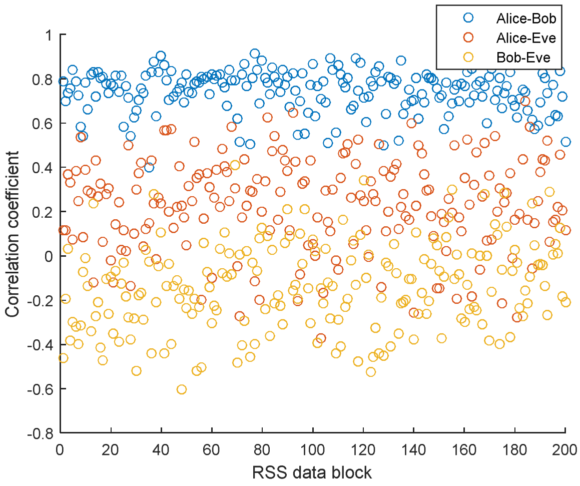

Fig. 10 Improvement of the correlation coefficient in experiment 3

2) Performance Comparison of SKG Scheme between Utilization of the Kalman Method and Direct Quantization

Table 3 and 4 shows the comparison of SKG scheme performance between the utilization of the Kalman method as a pre-processes method before quantization with direct quantization. The results of the experiments performed indicate a decline in KDR from legitimate users in all experiments. In general, KDR values of the legitimate user that were exceeding 0.25 (25%) indicate the need for a pre-processing method to reduce the KDR since the correction ability of BCH is 25% [15]. If the KDR exceeds 25%, then many data blocks are discarded because the BCH used is not capable of correcting the error. The test results also showed that the highest KDR obtained when we use 2-Ary quantization with KDR value in scenario 2 and 3 is above 0.3 (30%). However, in terms of security, 2-Ary quantization is the most secure quantization method because it has a high KDR value between eavesdroppers with legitimate users, so the possibility to get the same secret key is also getting smaller. It is also interesting that the use of the pre-processing method could increase the KDR between Alice and Eve on the Adaptive quantization method so that it could improve the security of the SKG scheme built. The results of KGR_{ik} showing almost the same results for all types of quantization, with the lowest KGR, obtained when using 2-Ary quantization.

TABLE III
PERFORMANCE OF SKG SCHEME WITH THE USED OF DIRECT QUANTIZATION

Experiment	**Quantization**	**User**	KGR_{ik} **(bps)**	**KDR**
1	MMB	Alice-Bob	18.12	0.226
		Alice-Eve	18.11	0.245
		Bob-Eve	17.98	0.244
	2-Ary	Alice-Bob	16.36	0.258
		Alice-Eve	16.36	0.500
		Bob-Eve	16.36	0.489
	Adaptive	Alice-Bob	18.12	0.267
		Alice-Eve	18.11	0.283
		Bob-Eve	17.98	0.546
2	MMB	Alice-Bob	18.15	0.223
		Alice-Eve	18.15	0.252
		Bob-Eve	18.02	0.245
	2-Ary	Alice-Bob	16.36	0.324
		Alice-Eve	16.36	0.498
		Bob-Eve	16.36	0.496
	Adaptive	Alice-Bob	18.15	0.263
		Alice-Eve	18.15	0.287
		Bob-Eve	18.02	0.549
3	MMB	Alice-Bob	18.13	0.237
		Alice-Eve	18.13	0.245
		Bob-Eve	18.10	0.253
	2-Ary	Alice-Bob	16.36	0.334
		Alice-Eve	16.36	0.491
		Bob-Eve	16.36	0.492
	Adaptive	Alice-Bob	18.13	0.275
		Alice-Eve	18.16	0.279
		Bob-Eve	18.10	0.558

TABLE IV
PERFORMANCE OF SKG SCHEME WITH THE USED OF KALMAN

Experiment	Quantization	User	KGR_{ik} (bps)	KDR
1	MMB	Alice-Bob	18.16	0.195
		Alice-Eve	18.10	0.253
		Bob-Eve	18.12	0.252
	2-Ary	Alice-Bob	16.36	0.245
		Alice-Eve	16.36	0.487
		Bob-Eve	16.36	0.505
	Adaptive	Alice-Bob	18.18	0.178
		Alice-Eve	18.18	0.383
		Bob-Eve	18.18	0.571
2	MMB	Alice-Bob	18.15	0.238
		Alice-Eve	18.12	0.242
		Bob-Eve	18.14	0.258
	2-Ary	Alice-Bob	16.36	0.308
		Alice-Eve	16.36	0.484
		Bob-Eve	16.36	0.502
	Adaptive	Alice-Bob	18.18	0.229
		Alice-Eve	18.18	0.397
		Bob-Eve	18.18	0.584
3	MMB	Alice-Bob	18.16	0.264
		Alice-Eve	18.12	0.250
		Bob-Eve	18.13	0.249
	2-Ary	Alice-Bob	16.36	0.396
		Alice-Eve	16.36	0.476
		Bob-Eve	16.36	0.499
	Adaptive	Alice-Bob	18.18	0.229
		Alice-Eve	18.18	0.381
		Bob-Eve	18.18	0.585

Figure 11 shows KGR_r of the legitimate user obtained from direct quantization. The highest KGR_r obtained from the MMB quantization of all experiments. This happens because MMB has the lowest KDR when compared to other quantization (as shown in Table 3 and 4). Fig. 12 shows KGR_r of the legitimate user with the addition of the Kalman method after quantization. The results of the tests show that Adaptive quantization yields a higher average KGR on all tests. The KDR generated by this quantization is also lower than the other quantization (as shown in Table 3 and 4). From all experiment, it could be seen that the combination of the multilevel loss quantization scheme with the pre-process method could improve the performance of the SKG scheme built. Table 5-7 shows the results of the NIST test on each experiment, where the test of the resulting secret key randomness has fulfilled the randomness requirements ($p \geq 0.01$).

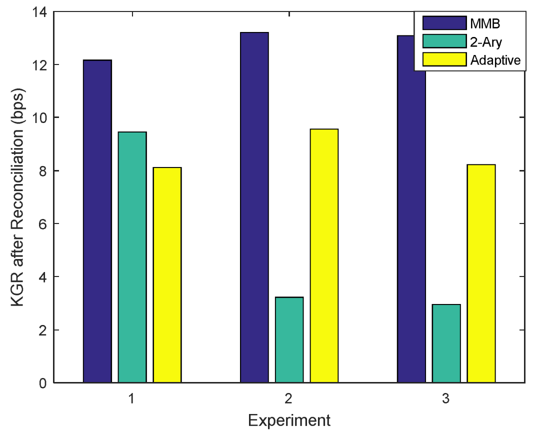

Fig. 11 KGR_r with the used of direct quantization

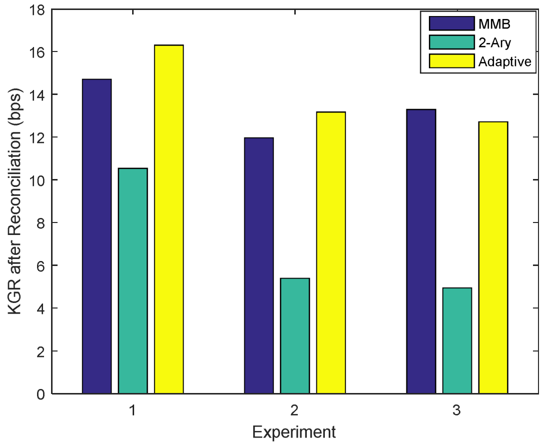

Fig. 12 KGR_r with the used of Kalman

TABLE V
NIST TEST ON EXPERIMENT 1

NIST Test	Value of p		
	MMB	2-Ary	Adaptive
Frequency	0.2	0.15	0.2
Block Frequency	0.3	0.22	0.45
Cusum (fwd)	0.05	0.3	0.25
Cusum (rev)	0.4	0.35	0.1
Runs	0.7	0.2	0.2
Longest of runs	0.2	0.4	0.25
Approximate entropy	0.8	0.31	0.22

TABLE VI
NIST TEST ON EXPERIMENT 2

NIST Test	Value of p		
	MMB	2-Ary	Adaptive
Frequency	0.23	0.6	0.4
Block Frequency	0.7	0.25	0.3
Cusum (fwd)	0.6	0.56	0.2
Cusum (rev)	0.5	0.7	0.1
Runs	0.9	0.5	0.34
Longest of runs	0.2	0.23	0.33
Approximate entropy	0.35	0.4	0.28

TABLE VII

NIST TEST ON EXPERIMENT 3

NIST Test	Value of p		
	MMB	**2-Ary**	**Adaptive**
Frequency	0.02	0.13	0.24
Block Frequency	0.1	0.22	0.33
Cusum (fwd)	0.3	0.3	0.26
Cusum (rev)	0.25	0.34	0.37
Runs	0.4	0.7	0.44
Longest of runs	0.3	0.2	0.87
Approximate entropy	0.2	0.3	0.11

IV. CONCLUSIONS

In this research, we propose the use of Kalman as pre-processing methods and multilevel loss quantization to overcome the trade-off issues of performance parameters of the Secret Key Generation (SKG) scheme. The results show that our propose SKG scheme can show better performance when compared with the use of direct quantization. The best performance is obtained from a combination of Kalman methods with Adaptive quantization, in which KGR and KDR generated are better than other quantization. Also, we also ensure the security of schemes built by ensuring the correlation value generated between legitimate users and eavesdroppers is less than 0.5, and the resulting KDR is more than 0.25 (25%). The resulting secret key has also fulfilled 6 random tests with p values greater than 0.01.

Our future work consists of developing the SKG scheme by proposing a new pre-process and multi-bit quantization method in various types of indoor environments such as a line of sight (LOS) and non-line of sight (NLOS). The successful testing of the system is done by comparing the performance of the proposed scheme with the existing scheme.

ACKNOWLEDGMENT

This research was supported by the Ministry of Research, Technology, and Higher Education through scholarship program BUDI-DN by LPDP of the Ministry of Finance of the Republic of Indonesia.

REFERENCES

[1] L. Chen, J. Ji, and Z. Zhang, Eds., *Wireless Network Security: Theories and Applications.* Springer, 2013.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, 2013.

[3] T. Belkhouja, X. Du, A. Mohamed, A.K. Al-Ali, and M. Guizani, "Symmetric Encryption Relying on Chaotic Henon System for Secure Hardware-Friendly Wireless Communication of Implantable Medical Systems, " *J. Sens. Actuator Netw.*, vol.7, 2018.

[4] A.Rezai, P.Keshavarzi, and Z.Moravej, "Key management issue in SCADA networks: A review," *Engineering Science and Technology, an International Journal*, vol.20, pp. 354-363, 2017.

[5] R. Khalilian, A. Rezai, and F. Mesrinejad, "Secure Wireless Body Area Network (WBAN) Communication Method using New Random Key Management Scheme," *International Journal of Security and Its Applications*, vol.10, no.11, pp. 13-22, 2016.

[6] A.Rezai, P. Keshavarzi, and Z. Moravej, "Advance hybrid key management architecture for SCADA network security," *Security and Communication Networks*, vol.9, no.17, pp. 4358-4368, 2016.

[7] J. Zhang, T. Q. Duong, R. Woods, and A. Marshall, "Securing wireless communications of the internet of things from the physical layer, an overview," *Entropy*, vol. 19, no. 8, pp. 1–16, 2017

[8] S. T. Ali, V. Sivaraman, and D. Ostry, ''Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices,'' *IEEE Trans. Mobile Comput*., vol. 13, no. 12, pp. 2763–2776, Dec. 2014.

[9] Y. Jiang, A. Hu, and J. Huang, "A lightweight physical-layer based security strategy for the Internet of things, " *in Cluster Computing*, vol.20, pp.1-13, March 2018.

[10] S. Zhang, J. Peng, K. Huang, X.Xu, Z. Zhong, "Physical Layer Security in IoT:A spatial-temporal perspective," *in 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*, Nanjing, China, 11-13 Oct. 2017.

[11] G. Margelis, X.Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, "Physical Layer Secret-Key Generation with Discrete Cosine Transform for the Internet of Things," *in 2017 IEEE International Conference on Communications (ICC)*, Paris, France, 21-25 May 2017.

[12] M.H.Chinaei, V.Sivaraman, D.Ostry, "An experimental study of secret key generation for passive Wi-Fi wearable devices," *2017 IEEE 18th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Macau, China, 12-15 June 2017.

[13] A.M.Adeshina, and R.Hashim, "Computational Approach for Securing Radiology-Diagnostic Data in Connected Health Network using High-Performance GPU-Accelerated AES," *Interdisciplinary Sciences: Computational Life Sciences*, vol.9, pp. 140-152, 2017.

[14] R. Khalilian, A. Rezai, and E. Abedini, "An Efficient Method to Improve WBAN Security," *Advanced Science and Technology Letters*, vol.64, pp. 43-46.

[15] 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.

[16] 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.

[17] B. U. V Prashanth and Y. Pandurangaiah, "Generation of Secret Key for Physical Layer to Evaluate Channel Characteristics in Wireless Communication," *Ercica*, pp. 251–255, 2013.

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

[19] G.Li, A.Hu, J. Zhang, L.Peng, and C. Sun, "High-Agreement Uncorrelated Secret Key Generation Based on Principal Component Analysis Preprocessing," *IEEE Trans. On Communications*, vol. 66, no. 7, pp. 3022-3034, July 2018.

[20] S. Zhang, L.Jin, Y.Lou, and Z. Zhong, "Secret Key Generation Based on Two-Way Randomness for TDD-SISO System," *in China Communications*, vol.15, issue (7): 202-216, 2018.

[21] R. Guillaume, F. Winzer, C. T. Zenger, C. Paar, and A. Czylwik, "Bringing PHY-based key generation into the field: An evaluation for practical scenarios," *2015 IEEE 82nd Veh. Technol. Conf. VTC Fall 2015 - Proc*., 2016.

[22] C. T. Zenger, J. Zimmer, and C. Paar, ''Security analysis of quantization schemes for channel-based key extraction,'' *in Proc. Workshop Wireless Commun. Secure. Phys. Layer*, Coimbra, Portugal, Jul. 2015.

[23] 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.

[24] R. Guillaume, A. Mueller, C. T. Zenger, C. Paar, and A. Czylwik, ''Fair comparison and evaluation of quantization schemes for PHY-based key generation,'' *in Proc. 18th Int. OFDM Workshop (InOWo)*, Essen, Germany, Aug. 2014, pp. 1–5.

[25] 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, Sep. 2008, pp. 128–139.

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

[27] Z. Kai, D. Wu, C. An, and P. Mohapatra, “Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks BT - *INFOCOM*, 2010 Proceedings IEEE,” pp. 1–9, 2010.

[28] M. Yuliana, “Performance Improvement of Secret Key Generation Scheme in Wireless Indoor Environment,” *IJCNIS*, vol. 9, no. 3, pp. 474–483, 2017.

[29] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, “Secret Key Extraction fromWireless Signal Strength in Real Environments,” *Mobile Computing, IEEE Transactions on*, vol. 12, no. 5, pp. 917–930, May 2013.

[30] A. Ambekar, M. Hassan, and H. D. Schotten, “Improving channel reciprocity for effective key management systems,” *Conf. Proc. Int. Symp. Signals, Syst. Electron.*, pp. 1–4, 2012.

[31] M. Yuliana, Wirawan, and Suwadi, “Performance evaluation of the key extraction schemes in the wireless indoor environment,” *in Proceedings - International Conference on Signals and Systems*, ICSigSys 2017, 2017.

[32] C. T. Zenger, J. Zimmer, M. Pietersz, J.-F. Posielek, and C. Paar, “Exploiting the Physical Environment for Securing the Internet of Things,” *Proc. New Secur. Paradig. Work. ZZZ - NSPW ’15*, pp. 44–58, 2015.

[33] A. Ambekar, Exploiting Radio Channel Aware Physical Layer Concepts Zur Nutzung von Kanalzustandsinformation in Funk ¨ ubertragungskonzepten. 2015.

[34] A. Rukhin et al., “A statistical test suite for random and pseudorandom number generators for cryptographic applications,” *Natl. Inst. Stand. Technol.*, vol. 800, no. April, p. 131, 2010.

[35] 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.