Secret Key Extraction with Quantization Randomness Using Hadamard Matrix on QuaDRiGa Channel

Xuanxuan Wang[1], Lihuan Jiang[2], Lars Thiele[2], and Yongming Wang[1](✉)

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
wangyongming@iie.ac.cn
[2] Fraunhofer Institute for Telecommunications, Heinrich Hertz Institute, Berlin, Germany

Abstract. The existing scheme of secret key extraction based on the channel properties can be implemented in the three steps: quantization, information reconciliation and privacy amplification. Despite the tremendous researches of quantization and information reconciliation techniques, there is little consideration about the risk of information reconstruction by the unauthorized node due to the high correlation of subsequent quantization bits, which is unavoidably leaked on the public channel between quantization and information reconciliation. In this paper, we propose an improved scheme of secret key extraction with quantization randomness using Hadamard matrix on QuaDRiGa channel. Simulation results show that with this kind of quantization randomness, the correlation between the subsequent quantization bits can be significantly decreased, which can reduce the possibility of information reconstruction by the unauthorized node, and the improved scheme can increase the randomness of the final secret key bits as compared with the existing ones.

Keywords: Quantization randomness · Hadamard matrix · Correlation · Secret key extraction

1 Introduction

In recent years, how to make a great use of the randomness of the wireless channel for secret key extraction between two wireless nodes has been increasingly paid much attention to. Different from traditional security methods, which mainly rely on the cryptography encryption technology and mathematical tools with a large cost of computing complexity and focus on the upper communication protocol, the principle of secret key extraction from the randomness of the wireless channel is the uncorrelation between the channels lying in a pair of two communication nodes and other nodes [1]. The underlying randomness results from temporal and spatial variation in the wireless channel, which is a natural and perfect resource for secret key extraction to keep the information security in physical

S. Qing et al. (Eds.): ICICS 2015, LNCS 9543, pp. 50–61, 2016.
DOI: 10.1007/978-3-319-29814-6_5

layer (PHY). So, secret key extraction based on the underlying randomness appears a promising alternative of the existing security methods, especially for the devices with limited resource.

The essential idea of PHY-based secret key extraction is that two legitimate wireless devices measure the reciprocal properties of a common wireless channel on the basis of public information exchanged over the channel. This means that the measurements for two intended node are theoretically identical. However, the time-varying feature of wireless channel results in a non-ideal consistency of PHY-based measurements. In order to obtain the independent channel measurements, we perform the process during the coherence time period according to [2], during which the channel impulse response is considered to be unchanged. That is to say, we can get the high correlation between the sampled channel measurements and increase the measurements consistency.

The basic scheme of secret key extraction based on the channel measurements in coherence time can be implemented in three steps [3–5]: quantization, information reconciliation and privacy amplification. The quantization techniques on common measurements can be used to quantize the observations measured from the public channel and get an initial bit stream between two legitimate nodes, respectively. Due to the channel measurements done in coherence time, it has high correlation between subsequent bits in the initial quantization bit stream. Information reconciliation techniques tackle the mismatch quantization bits generated at two legitimate nodes and correct them through the initial quantized sequence exchanged over the public channel. Finally, in privacy amplification the two legitimate nodes apply a deterministic function to generate the secret key bits.

Most of the previous work mainly focuses on the development and analysis of quantization techniques [3,6,7] and information reconciliation techniques [8,9]. But ignores the possibility of information reconstruction by the unintended device through the high correlation of the initial subsequent quantization bits. Due to the broadcast nature of a common channel, it seems that the information leakage is unavoidable when the initial quantization bits exchange over the public channel for information reconciliation, which is an advantage for the unauthorized node to reconstruct and predict the information.

To deal with this issue, we propose an improved scheme of secret key extraction in this paper. The quantization bits are randomized with Hadamard matrix before being transmitted on a common channel for information reconciliation, which can reduce the correlation in the subsequent quantized bit stream. We carry out the operation on the QuaDRiGa channel. Simulation results show that this scheme can decrease the correlation of the subsequent quantized bit stream, as well as the possibility of information reconstruction by the unintended node, and can also improve the randomness of the final secrete key bits in comparison with the existing ones.

The rest of the paper is organized as follows. Section 2 describes the basic system model and the adversarial model. Section 3 details the improved scheme with Hadamard matrix. In Sect. 4, we present and discuss the numerical results. Finally, Sect. 5 concludes the paper.

2 A Basic Model

2.1 System Model

The general model of PHY-based secret key extraction discussed in this paper is a basic three-terminal system shown in Fig. 1, which consists of a legitimate transmitter (called Alice), an intended (legitimate) receiver (called Bob), and an unauthorized receiver (called Eve). In this security model, Alice and Bob try their best to establish a shared key based on the reciprocal measurements of the wireless channel. Eve, an eavesdropper, targets the derivation of the pairwise key generated by Alice and Bob.

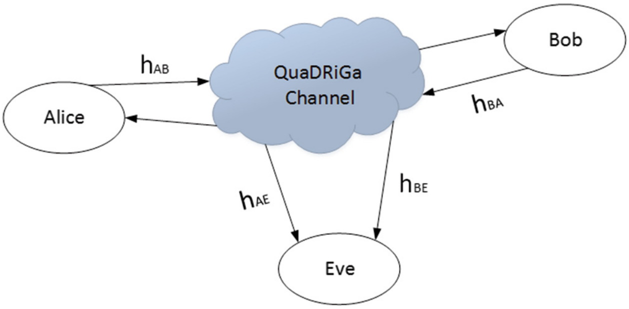


Fig. 1. System model

The particular properties of the wireless channel used for secret key extraction can be the parameters of the wireless channel, such as delay spread, amplitude, phase, Receive Signal Strength (RSS) and so on. Two legitimate nodes Alice and Bob measure the randomness and reciprocity of the wireless channel gains in coherence time, denoted by h_{AB} and h_{BA}, and follow the general three-step scheme of secret key extraction to obtain the shared key bits. In this scheme, the basic steps are as following:

Quantization: the existing quantization approaches aim to convert consecutive channel measurements into discrete random bits based on various thresholds setting. In general, it can be classified into two categories: lossy quantization and lossless quantization. The former is achieved at the cost of probabilistically dropping bits to maintain the high bit entropy, and the latter generates quantized data for the whole input stream so as to produce a high generation rate output.

Information Reconciliation: this is a reconciled process to deal with the discrepancy in the initial quantization bit stream, which mainly focuses on various error correct codes, such as LDPC code.

Privacy Amplification: privacy amplification is used to generate a final secret key bits. Alice and Bob use the same means (e.g., hash function) to generate a secret key bit stream by choosing a longer input randomly and fixing the output in a smaller length randomly. The random input and output in privacy amplification can make the final secret key bits strong.

The unauthorized party Eve can observe the channel measurements h_{AE} and h_{BE}. To Eve, how to perceive the related channel coefficient is subject to the relative distance from the two legitimate nodes in spatial dimension. The shorter the relative distance is, the higher the correlation is between h_{AE} and h_{AB} or h_{BE} and h_{BA} and the more possibility there is for Eve to extract the transmitted data exactly.

In this model, we choose the Quasi Deterministic Radio Channel Generator (QuaDRiGa) [10] as the channel model so as to achieve a better performance evaluation. The QuaDRiGa channel models wireless channel propagation in three dimensions (3D) over time (4D). Based on the collection of features created in Spatial Channel Model (SCM) and WINNER channel models, the QuaDRiGa channel provides features to enable quasi-deterministic multi-link tracking of user (receiver) movements in different propagation environments, which can evaluate a more realistic environment and play a great importance to the research on physical layer security. The QuaDRiGa channel follows a geometry-based stochastic channel model and creates an arbitrary double directional radio channel. The key impacts of the QuaDRiGa are: (i) to split MT trajectory into segments based on the geo-correlation of Large Scale Parameters (LSPs) and realize the continuous time evolution; (ii) to insert three dimensional antenna dependently; (iii) to support variable speed of the terminal by interpolation of channel coefficients.

2.2 Adversarial Model

In our adversary model, we assume Eve can sense all the process of the communication between Alice and Bob. Eve can try his best to measure the channels between Alice or Bob and himself at the same time when Alice and Bob measure the channel between themselves for secret key extraction. We also assume Eve has the same calculation capability and knows the same scheme of channel estimation as Alice and Bob. There is no limitation on Eve's position from Alice and Bob. That is to say, Eve can choose the optimum position to estimate the correlated coefficients of the wireless channel between Alice and Bob by himself and then achieve their shared key successfully. We assume Eve is a passive attacker, who can neither obstruct the common channel between Alice and Bob nor modify any exchanged message transmitted on the common channel.

3 Methodology of Quantization Randomness

As highlighted before, the high correlation between subsequent bits in the initial quantized bit stream is a great advantage for Eve to recreate and predicate the secret key bits. So, it is very important to reduce the correlation between a bit and the subsequent bit in the initial quantization bit stream. In the following, we will present an improved scheme based on Hadamard matrix to randomize the quantization bits so as to weaken the correlation.

3.1 Hadamard Matrix

The Hadamard matrix is a symmetric matrix. Due to the symmetric property it has been poured into the applications, such as data encryption, randomness measures and so on [11]. The Hadamard matrix $\mathbf{H_m}$ can be achieved through the Hadamard transform. We define the 1×1 Hadamard transform H_0 by the identity $H_0 = 1$, then the Hadamard matrix $\mathbf{H_m}$ is:

$$\mathbf{H_m} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{H_{m-1}} & \mathbf{H_{m-1}} \\ \mathbf{H_{m-1}} & -\mathbf{H_{m-1}} \end{pmatrix} = \mathbf{H_1} \otimes \mathbf{H_{m-1}} \tag{1}$$

where m is the order of Hadamard matrix and $m > 0$.

The Hadamard matrix, $\mathbf{H_m}$, is a square matrix of order $m = 1, 2$ or $4k$, where k is a positive integer. The elements of $\mathbf{H_m}$ are either $+1$ or -1 and $\mathbf{H_m} \cdot \mathbf{H_m^T} = n\mathbf{I_m}$, where $\mathbf{H_m^T}$ is the transpose of $\mathbf{H_m}$ and $\mathbf{I_m}$ is the identity matrix of order m.

3.2 Random and Random_inverse

In this section, we detail the improved scheme of random and random_inverse for the quantization bits with Hadamard matrix based on [12]. Here we only consider the non-binary matrix to random the quantization bits based on the Hadamard matrix, so we carry out modulo operations on the negative values in the Hadamard matrix in order to make the negative values into the non-negative ones. We specify each negative number replaced with the corresponding modulo number. For example, with the operation of modulo 7, the elements -1 in the Hadamard matrix are replaced with 6 so as to make the elements in the matrix non-binary. In order to simplify the calculation, we only perform prime modulo operations that is because non-prime number can be divisible with numbers other than 1 and itself.

Figure 2 illustrates the process of randomizing the quantization bits with Hadamard matrix, which is composed of the following four steps:

1. choose an arbitrary prime number n and divide the quantization bits S into several bit groups, where the number of bits in each group is equal to n.
2. convert each group of binary bits into the corresponding decimal values D.
3. segment the decimal sequence and perform multiplication with Hadamard matrix. The decimal sequence D is broken down into chunks $D^{'}$, the size of which is equal to 2^n. Multiply each group of decimal subsequence $D^{'}$ with the corresponding Hadamard matrix $\mathbf{H}$ to get $D^{''}$. Here, the Hadamard matrix $\mathbf{H}$ is a $2^n \times 2^n$ modified matrix of the form modulo $(2^n - 1)$ in order to change the negative values in the matrix into the non-negative ones. Then perform the operation of modulo $(2^n - 1)$ on each resultant decimal subsequence $D^{''}$ to reduce the complexity of the calculation result.

4. combine each resultant multiplied decimal subsequence $D^{''}$ and convert them into the corresponding binary sequence $S^{'}$.

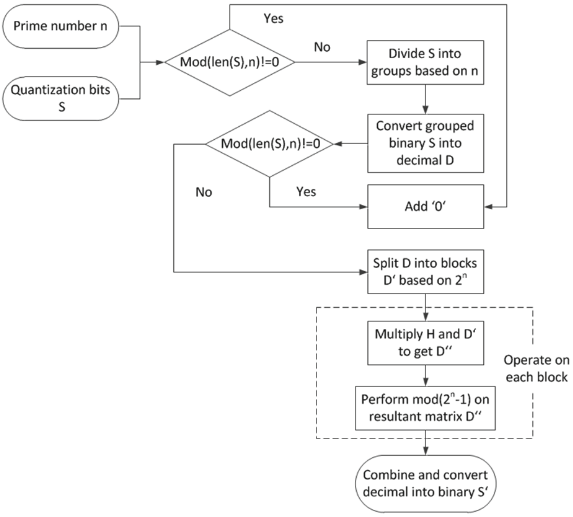

Prime number n
Quantization bits S
Mod(len(S),n)!=0
Yes
No
Divide S into groups based on n
Convert grouped binary S into decimal D
Mod(len(S),n)!=0
No
Yes
Add '0'
Split D into blocks D' based on 2^n
Multiply H and D' to get D''
Perform mod(2^n-1) on resultant matrix D''
Operate on each block
Combine and convert decimal into binary S'

Fig. 2. Block diagram of random for quantization bits

Note that the $'0'$ appending operation in (1) and (3) may be required in order to meet the requirement for the length of each bit block.

Figure 3 shows the process of random_inverse for the quantization bits with the Hadamard matrix. We choose the resultant binary sequence $S^{'}$ obtained in the randomness process and the prime number n as the input. Here n is the same as that in the randomness process.

1. split the input binary sequence $S^{'}$ into groups, where the number of bits in each group is equal to n, and convert them into corresponding decimal values D_1.
2. divide the input decimal sequence D_1 into blocks $D_1{'}$, whose length is equal to 2^n.
3. calculate the modular multiplicative inverse of $D_1{'}$ with respect to modulo $(2^n - 1)$ to get $D_1{''}$ and multiply each resultant subsequence $D_1{''}$ with the matrix $\mathbf{H^{-1}}$ on each block. Here the matrix $\mathbf{H^{-1}}$ is the inverse of the Hadamard matrix $\mathbf{H}$, which is a $2^n \times 2^n$ modified matrix of the form modulo $(2^n - 1)$.
4. combine each resultant decimal subsequence $D_1{''}$.
5. convert the combined decimal sequence into the corresponding binary sequence S.

Note that the $'0'$ dropping in (4) and (5) may be required if there is consecutive $0'$ at the end of the sequence.

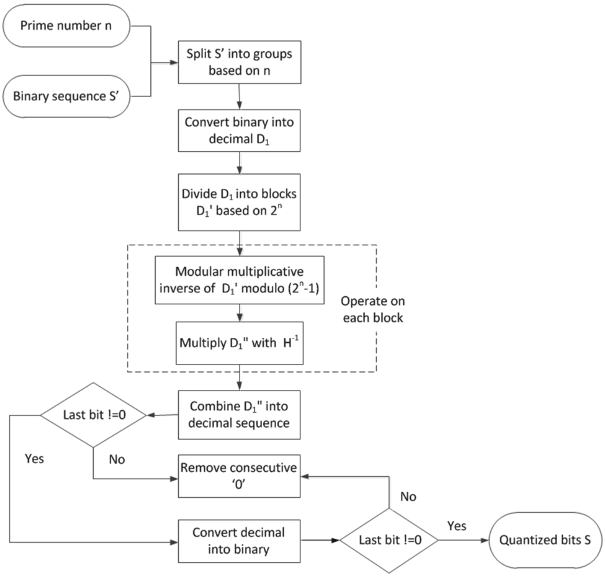

Prime number n
Binary sequence S'
Split S' into groups based on n
Convert binary into decimal D1
Divide D1 into blocks D1' based on 2^n
Modular multiplicative inverse of D1' modulo (2^n-1)
Multiply D1" with H^-1
Operate on each block
Combine D1" into decimal sequence
Last bit !=0
Yes
No
Remove consecutive '0'
Convert decimal into binary
No
Last bit !=0
Yes
Quantized bits S

Fig. 3. Block diagram of random_inverse for quantization bits

3.3 Secret Key Extraction with Quantization Randomness

Figure 4 illustrates the process of secret key extraction with quantization randomness based on Hadamard matrix. In this paper, we take the Alice as the leader to perform the information exchange with Bob. We take the RSS measurements from the QuaDRiGa channel as the target and apply the multiple bits quantization scheme as proposed in [3]. In order to reduce the correlation between subsequent quantization bits, we first random the quantization bits collected from RSS measurements by Alice rather than directly transmit them over the common channel to Bob in information reconciliation. Different from the highly correlated bit stream obtained by Bob in [3], a bit sequence with less correlation between subsequent bits is received. We choose the LDPC code as the information reconciliation scheme to deal with the asymmetry lying in the two randomized quantization bit streams. This is an iterative scheme and LDPC encode is carried out in small blocks. So it is important for Bob to perform the LDPC decode and random_inverse for the received sequence once the randomized quantization bit stream is obtained. Finally, we choose the most popular methods, hash function, to fix the size and obtain a small length output from the long bit stream in privacy amplification.

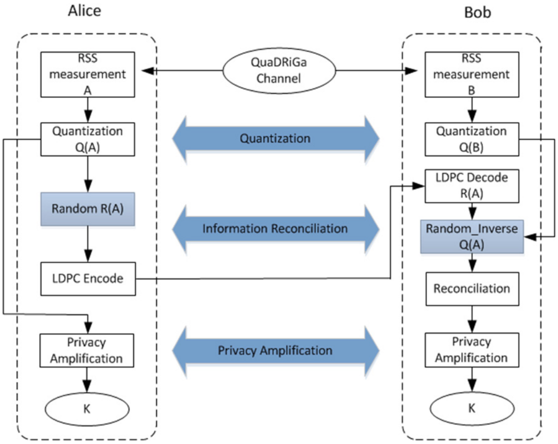


Fig. 4. Flowchart of extracting secret key with quantization randomness

4 Numerical Results

4.1 Performance Evaluation

We choose the autocorrelation function to identify the correlation of the subsequent bits in a bit stream. Given the data sequence $X_1, X_2, X_3, \ldots, X_N$ at times $t_1, t_2, t_3, \ldots, t_N$, the kth autocorrelation (lag k) is defined as:

$$r_k = \frac{\sum_{i=1}^{N-k} \left(X_i - \overline{X}\right)\left(X_{i+k} - \overline{X}\right)}{\sum_{i=1}^{N} \left(X_i - \overline{X}\right)^2} \tag{2}$$

where $\overline{X}$ is the mean of the data sequence X_i, $i = 1, 2, \ldots, N$.

The result of Eq. (2) is a correlation coefficient, which represents the correlation between values at different times t_i and t_{i+k} in the same variable. If the data values are random, such autocorrelation coefficients should be near zero for any time-lag separations. If they are not random, then one or more of the autocorrelation coefficients will be significantly non-zero.

Guaranteeing the randomness of the final secret key is essential for physical layer security because Alice and Bob are intended to rely on the secret keys for information encryption [13]. Since we have assumed Eve can sense all the process of the communication between Alice and Bob and has the same calculation ability as them, any bad randomness behavior of the final secret key can result in the low complexity of cracking the key for Eve. In order to evaluate the randomness of the secret key bits, we focus on the following equation [11]:

$$R = 1 - \frac{1}{n-1} \sum_{k=1}^{n-1} \left(|r_k|\right) \tag{3}$$

where n is the period of the data sequence and r_k is the autocorrelation coefficient figured out according to the Eq. (2). If the given data sequence is random, the randomness R should be nearer to one.

4.2 Simulation Results

In this section, we perform extensive simulations to evaluate the performance of the improved scheme of secret key extraction with quantization randomness based on Hadamard matrix introduced in the previous sections. We carry out the simulations on the QuaDRiGa channel and show results by means of exemplary implementation. In order to validate the scheme, we also present our executed analysis on simulation results.

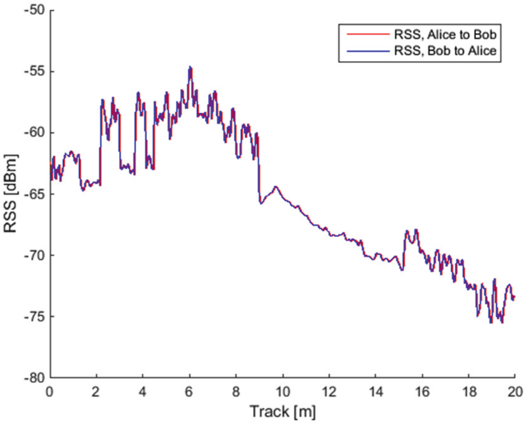
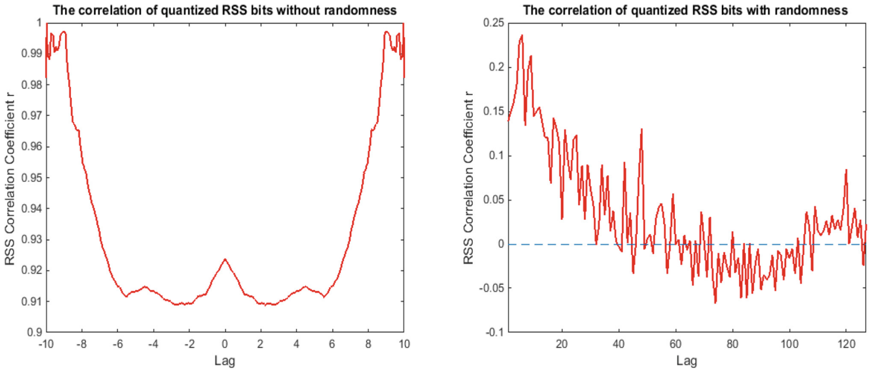


Fig. 5. The RSS measurements between Alice and Bob

Figure 5 illustrates the RSS measurements at Alice (red) and Bob (blue) vs. track based on the QuaDRiGa channel. It can be seen that, the two measurements between Alice and Bob have a great similarity. That is to say, because of the broadcast nature of the wireless communication channel, Eve can easily wiretap any shared RSS measurements between Alice and Bob by choosing his optimum position as a passive attacker.

Figure 6 shows the comparison of the correlation between a bit and the subsequent bit in a quantized RSS bit stream without (a) and with (b) randomness with Hadamard matrix. It can been seen that in Fig. 6(a), the quantization bit stream exhibits a highly-correlated connection between subsequent bits, where the correlation coefficient r lies between 0.9 and 1. From the security perspective, the highly-correlated quantized RSS bits can supply an advantage for Eve to eavesdrop and reconstruct the message due to the broadcast nature of the common channel and the unavoidable information leakage during the information reconciliation. Consequently, Eve can make use of the correlation to easily

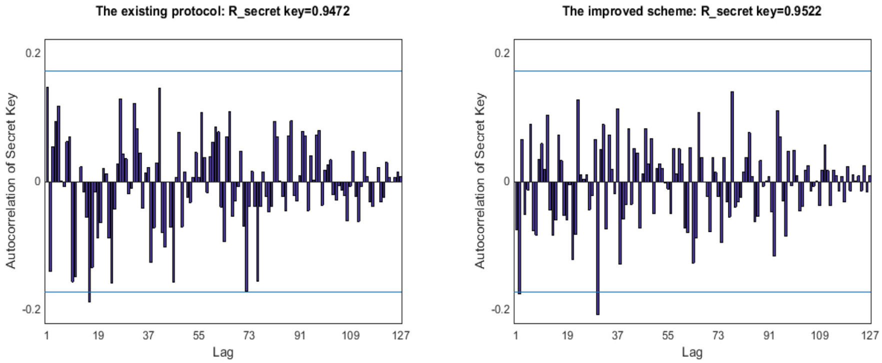


(a) (b)

Fig. 6. Comparison of the correlation of quantized RSS bits without (a) and with (b) randomness

deduce the considerable amount of the legitimate node′s key, which is a great threat for secret key generation.

Figure 6(b) illustrates the correlation coefficients decrease to less than 0.25 and even some values are less than 0, which are lower than those showed in Fig. 6(a). With the Hadamard matrix to randomize the quantization bit stream, the subsequent bits of the initial quantization bit stream have less correlation. So, little possibility is supplied for Eve to reconstruct the secret key bits when this randomized quantization bit stream is transmitted over the public channel for information reconciliation.



(a) (b)

Fig. 7. Comparison of the autocorrelation and randomness of secret key extraction with the existing protocol (a) and the improved scheme (b)

Figure 7(a) illustrates the autocorrelation and randomness of the final secret key bit stream which is generated with the existing scheme of secret key extraction. It can be seen that with the existing scheme of secret key extraction, which little considers the randomness of the quantization bits, the randomness of secret key bits R_{secret_key} is 0.9472. Figure 7(b) illustrates the autocorrelation and randomness of the final generated secret key bit stream based on the improved scheme proposed in this paper. It can be seen that in the case the randomness of the final secret key bits R_{secret_key} can rise to 0.9522, which increases by 0.05 in comparison with the randomness without quantization randomness in the existing scheme. The slight increase on the randomness of the final secret key bits can affect the secret key robustness behavior and increase difficulty for Eve in cracking the key [13].

5 Conclusion

It has the high correlation between subsequent quantized RSS bit stream. Due to the openness feature of the common channel, the highly-correlated quantization bit stream is unavoidably leaked when it is exchanged over the public channel for information reconciliation, which is a perfect source of secret key reconstruction for the unintended node.

Based on RSS measurements from the QuaDRiGa channel model, we present an improved scheme of secret key extraction with quantization randomness using Hadamard matrix. Our simulation results show that the improved scheme with Hadamard matrix significantly decreases the correlation between adjacent quantization bits, reduces the possibility of secret information reconstruction by the unauthorized party, and can increase the randomness of the final secret key bits as compared with the existing ones, which plays a great role in preventing passive attacker Eve from cracking the key.

References

1. Sayeed, A., Perrig, A.: Secure wireless communications: secret keys through multipath. In: Speech and Signal Processing, Acoustics, pp. 3013–3016 (2008)
2. Guillaume, R., Mueller, A., Zenger, C.T., Paar, C., Czylwik, A.: Fair comparison and evaluation of quantization schemes for PHY-based key generation. In: Proceedings of 18th International OFDM Workshop (InOWo 2014), pp. 1–5 (2014)
3. Jana, S., Premnath, S.N., Clark, M., Kasera, S.K., Patwari, N., Krishnamurthy, S.V.: On the effectiveness of secret key extraction from wireless signal strength in real environments. In: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking, pp. 321–332. ACM (2009)
4. Zenger, C.T., Chur, M.-J., Posielek, J.-F., Paar, C., G. Wunder: A novel key generating architecture for wireless low-resource devices. In: International Workshop on Secure Internet of Things (SIoT), pp. 26–34. IEEE (2014)
5. Bloch, M., Barros, J.: Physical-Layer Security: from Information Theory to Security Engineering. Cambridge University Press, Cambridge (2011)

6. Tope, M., McEachen, J.C.: Unconditionally secure communications over fading channels. In: Military Communications Conference, MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force, vol. 1, pp. 54–58. IEEE (2001)
7. Mathur, S., Trappe, W., Mandayam, N., Ye, C., Reznik, A.: Radio- telepathy: extracting a secret key from an unauthenticated wireless channel. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking, pp. 128–139. ACM (2008)
8. Bloch, M., Thangaraj, A., McLaughlin, S.W., Merolla, J.-M.: LDPC-based secret key agreement over the Gaussian wiretap channel. In: IEEE International Symposium on Information Theory, pp. 1179–1183. IEEE (2006)
9. Etesami, J., Henkel, W., Wakeel, A.: LDPC code construction for wireless physical-layer key reconciliation. In: First IEEE International Conference on Communications in China (ICCC 2012). Beijing (2012)
10. http://www.hhi.fraunhofer.de/departments/wireless-communications-and-networks/research-areas/system-level-analysis-and-concepts/quadriga.html
11. Ella, V.S.: Randomization using quasigroups, hadamard and number theoretic transforms (2012). arXiv preprint arXiv:1202.0223
12. Reddy, R.S.: Encryption of binary and non-binary data using chained hadamard transforms (2010). arXiv preprint arXiv:1012.4452
13. http://cs.nyu.edu/dodis/randomness-in-crypto/random1.pdf