A New Low-BMR Quantization Method for Wireless Channel Characteristics-based Secret Key Generation

Qiuhua Wang*[1], Qiuyun Lyu[1], Xiaojun Wang[1], Jianrong BAO[2]
[1]School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, P. R. China
[e-mail: wangqiuhua@hdu.edu.cn; laqyzj@ hdu.edu.cn; xiaojunwang01@sina.com]
[2] School of Information Engineering, Hangzhou Dianzi University, Hangzhou 310018, P. R. China
[e-mail: baojr@ hdu.edu.cn]
*Corresponding author: Qiuhua Wang

Received March 29, 2017; revised May 18, 2017; accepted June 17, 2017; published October 31, 2017

Abstract

Channel characteristics-based secret key generation is an effective physical-layer security method. The issues of how to remove the effect of random noise and to balance the key generation rate (KGR) and the bit mismatch rate (BMR) are needed to be addressed. In this paper, to reduce the effect of random noise and extract more secret bits, a new quantization scheme with high key generation rate and low bit mismatch rate is proposed. In our proposed scheme, we try to use all measurements and correct the differences caused by noise at the boundary regions instead of simply dropping them. We evaluate and discuss the improvements of our proposed scheme. The results show that our proposed scheme achieves lower bit mismatch rate as well as remaining high key generation rate.

Keywords: Secret key generation; Physical-layer security; Channel reciprocity; Quantization; Information reconciliation; Privacy amplification

This work was partially supported by National Natural Science Foundation of China (No.61401128， No. 61471152), Zhejiang Province Natural Science Foundation (No. LQ14F020010), Project of Zhejiang Provincial Key Enterprises Institute Construction and Project of Zhejiang Provincial Smart City regional synergy innovation center and the China Scholarship Council (CSC).
This work was done when Qiuhua Wang visited the Department of Electrical & Computer Engineering, Syracuse University, Syracuse, NY 13244, USA. We would like to thank Dr. Yingbin Liang at Syracuse University for her helpful discussion about this research project.

https://doi.org/10.3837/tiis.2017.10.021 **ISSN : 1976-7277**

1. Introduction

Recently, exploiting wireless channel characteristics to generate a shared secret key between two legitimate users has become a promising technique for its high reliability, easy implementation, and low energy consumption. It provides an excellent approach to the problem of key-establishment and can even achieve information theoretical secrecy [1]. The basic idea behind it is to take advantage of the inherent wireless channel reciprocity, randomness and spatial uncorrelation.

In a typical wireless network environment, the wireless channel between two users, Alice (A) and Bob (B), is reciprocal and varies randomly over space and time. Alice and Bob are able to measure some wireless channel characteristics (e.g., received signal strength (RSS) [1]-[7] or channel state information (CSI) [8]-[12]) many times. These measurements can then be used as shared random sources to generate a shared secret key. An eavesdropper, Eve (E), who is more than a half-wave-length away from Alice and Bob, can obtain no information about the secret key because she experiences independent fading [13] and thus cannot measure the same channel characteristics as Alice and Bob [1].

Consider a scenario in **Fig. 1**, in which two authorized users, Alice and Bob, wish to establish a shared secret key via wireless channel in the presence of an unknown passive eavesdropper Eve. Alice and Bob each sends probing data through the wireless channel from which they respectively measure the channel characteristics and construct the channel measurements, denoted by h_{ab} and h_{ba}. The channel characteristic may be Channel Impulse Response (CIR) itself, or any function of the wireless channel, e.g., the RSS, or different sub carriers of a multicarrier transmission system [14]. Due to the channel reciprocity, we have $h_{ab} \approx h_{ba}$ when they are conducted during the channel coherence time. Eve can estimate her channel to Alice or Bob, however, if Eve is more than $\lambda/2$ (λ is the wavelength) away from Alice and Bob, she will experience independent channel variations, hence, her observations h_{ae} and h_{be} are sufficiently uncorrelated with h_{ab} and h_{ba} due to the spatial variations, e.g., $h_{ae} \neq h_{ab}$ and $h_{be} \neq h_{ba}$ [13]. Using these similar channel variations, Alice and Bob can generate shared secret keys by performing the steps shown in **Fig. 2**. A brief explanation of each step is given below.

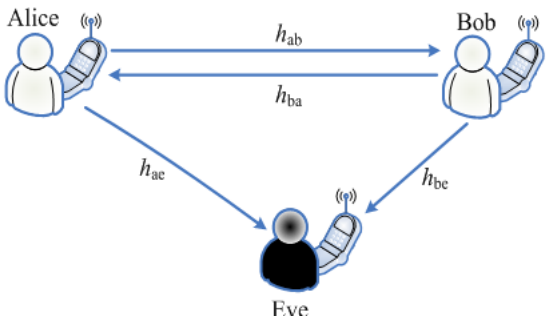


Fig. 1. Wireless communication scenario

(1) Step 1: Channel probing. In this step, Alice and Bob successively sending each other a known probing signal using the same frequency band. Suppose that Alice initiates the

process. In the first time slot, Alice transmits a known sequence to Bob. In the Second slot, Bob transmits the same sequence back to Alice. The length of the time slot is usually set as half of the channel coherence time. If multiple rounds of channel probing are run during the same coherence time period, the randomness of the generated key bits will decrease [15].

(2) Step 2: Channel characteristic estimation. From the received probing signals, both Alice and Bob estimate and extract the proper channel characteristics such as RSS [1]-[7], amplitude [8]-[9] and phase [10]-[12] of CIR, which are then used as common random sources to generate a shared secret key.

(3) Step 3: Quantization. Both Alice and Bob convert their extracted channel measurements into random binary bit sequences by using a quantization algorithm, respectively. The output of the quantizer is called as initial key sequence. The paper [16] summarizes some existing quantization methods and evaluates their performance.

(4) Step 4: Information reconciliation. The initial key sequences obtained at Alice and Bob are often subject to discrepancies due to imperfect channel reciprocity and noise [17]. Hence, an information reconciliation protocol will be used to reconcile the bit mismatches. During information reconciliation, Bob and Alice agree upon a same key by exchanging syndromes and/or parity check bits on public channel and applying an error correcting code. In our recent works [18] and [19], some typical information reconciliation protocols have been introduced and analyzed.

(5) Step 5: Privacy amplification. As the information reconciliation leaks some information about the secret key which can be used by the eavesdropper to guess portions of the extracted key, privacy amplification is used to remove the leaked information. In the privacy amplification phase, Alice and Bob use a universal hash function to distill a highly-secret key sequence, about which Eve knows a negligible amount of information [20-21].

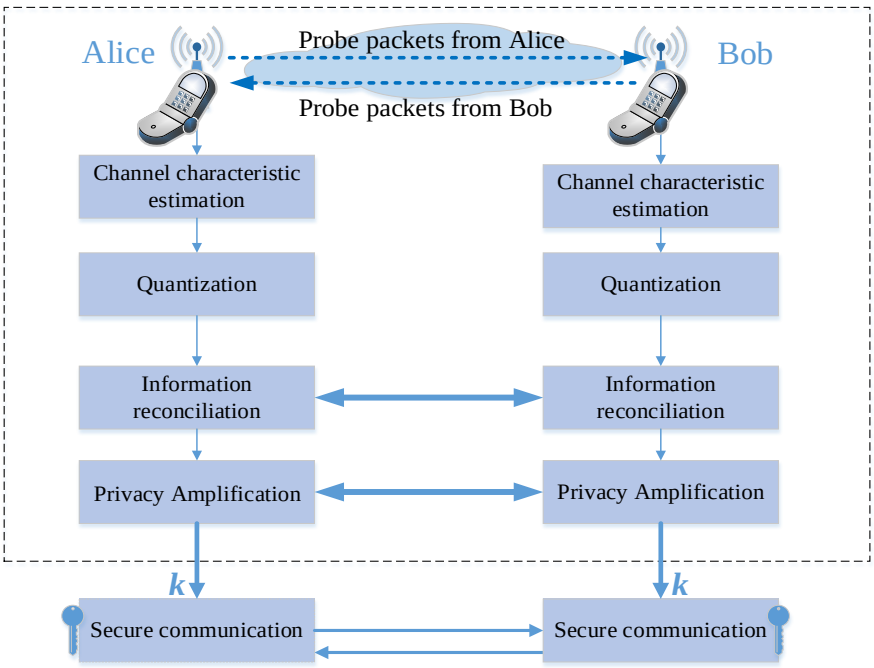


Fig. 2. Typical steps in a traditional secret key generation system

The rest of the paper is organized as follows. In Section 2, we introduce some existing quantization methods and discuss why the performance of those approaches is not satisfactory in terms of the bit mismatch rate and the key generate rate. In Section 3, we propose a low bit mismatch rate quantization scheme and provide the detailed description of it. In Section 4, the performance analysis and simulation results are presented. Finally, we conclude the paper in Section 5.

2. Quantization methods

From above introduction in Section 1, quantization is a crucial step in the wireless key establishment procedure because it provides initial information of the wireless channel. All the remaining steps expect an efficient and precise quantization output. In the quantization stage, the transmitter and the receiver quantize the channel measurements into binary bits based on particular thresholds to generate initial secret bit sequences. There are many proposals of channel quantization. The difference among these quantizers mainly results from their different choices of thresholds and the different number of thresholds they use. These quantization methods could generally be classified into two categories: Single-bit approaches and Multi-bit approaches [3].

• Single-bit approaches, in which each channel measurement is quantized into at most one bit.

• Multi-bit approaches, in which each channel measurement is quantized into multiple secret bits, *m*-bit (*m*>1).

In this section, we describe some existing quantization approaches and discuss why the performance of those approaches is not satisfactory in terms of the bit mismatch rate and the key generate rate.

2.1 Single-bit Quantization

Tope et al. [22] introduced the very first channel-based key generation protocol. They suggested a single-bit quantization scheme (also known as lossy quantization scheme) based on two thresholds, upper threshold q_+^u and lower threshold q_-^u, for converting channel measurements into random key bit sequence, as shown in **Fig. 3**.

Let $X^u = (x_1^u, x_2^u, ..., x_n^u)$ be the n real channel measurements at user $u = \{A, B\}$. Each measurement value x_i^u $(1 \le i \le n)$ is mapped to a temporary bit via a quantizer $Q^u(\cdot)$ such that measurements below the lower threshold q_-^u are encoded as bit 0, measurements above the upper threshold q_+^u are encoded as bit 1, while measurements within the interval $\left[q_-^u,\ q_+^u\right]$ are discarded.

$$Q^u(x_i^u) = \begin{cases} 1, & if \quad x_i^u > q_+^u \\ 0, & if \quad x_i^u < q_-^u \\ e, & otherwise \end{cases} \tag{1}$$

where e is an undefined state. The superscript u stands for user and may refer to either Alice, in which case the quantizer is $Q^A(\cdot)$, or to Bob, for which the quantizer is $Q^B(\cdot)$.

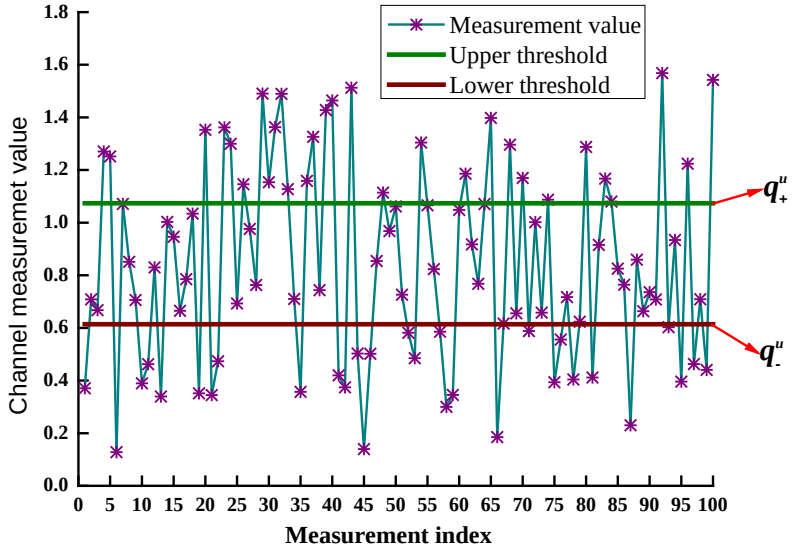


Fig. 3. A sample of single-bit quantizer

Alice and Bob maintain a list of indexes of discarded values and exchange it with each other, so that they exclude all such indexes from further consideration for secret key extraction.

Tope et al. defined q_+^u and q_-^u as fixed system parameters. Consequently, several schemes were proposed using different rules to determine the thresholds and selecting estimates [1], [2], [24], [25]. For example, in [1], the thresholds q_+^u and q_-^u were determined by calculating the mean and the standard deviation of the channel measurements:

$$q_+^u = \mu^u + \alpha \times \sigma^u \tag{2}$$

$$q_-^u = \mu^u - \alpha \times \sigma^u \tag{3}$$

where μ^u and σ^u represent the mean and the standard deviation over the measurement sequences X^u, and $0 < \alpha < 1$ is a parameter to be tuned.

To increase the probability of key agreement, level crossing secret key generation scheme [23] was proposed, in which m consecutive measurements that are above q_+^u or below q_-^u are used to generate one bit. Due to the same reason, [26] only quantized the matching deep fades of measurements. In [2], Jana *et al.* proposed an adaptive secret bit generation (ASBG) scheme, where the measured sequence is broken into smaller blocks and the thresholds are calculated for each block. It can remove the components that vary slowly and thus increase the entropy of the generated bit sequence.

As the single-bit quantization method discards some of the channel measurements within thresholds $\left[q_-^u,\ q_+^u\right]$ which, however, may be valuable information used to generate the secret key bits, it has a low key generation rate (KGR) which is defined as the average number of secret key bits extracted per channel measurement.

To extract more secret key bits and increase the key bit generation rate, in [2], Jana et al. adopted a multiple-bit extraction method, in which multiple thresholds were used to convert each channel measurement into multiple binary bits by using Gray codes.

2.1 Multi-bit quantization

Direct multi-bit quantization-based approaches (also known as lossless schemes) process all the obtained channel measurements and map each measurement to *m* bits. These direct quantization schemes do not lose valuable information.

In order to extract *m* bits per measurement, the measurement value X^u is quantized into $N= 2^m$ equally-likely levels. We have the quantization levels $[q_0^u, q_1^u, ..., q_N^u]$ and quantization intervals $I_0 = [q_0^u, q_1^u), I_1 = [q_1^u, q_2^u), \ldots, I_{N-1} = [q_{N-1}^u, q_N^u]$, where $q_0^u = \min(X^u)$ and $q_N^u = \max(X^u)$ is the minimum and maximum value of X^u, respectively, and the value of q_i^u $(1 \le i \le N-1)$ is determined by:

$$q_i^u = q_0^u + \frac{q_N^u - q_0^u}{N} i, \quad i = 1, 2, ..., N-1 \tag{4}$$

Each measurement can be quantized to a certain level if it falls into the corresponding interval. More specifically, assume the measurement value x_i^u is located in the *k*th quantization interval $[q_{k-1}^u, q_k^u]$, both Alice and Bob convert their measurements into random key bits using a quantizer $Q^u(\cdot)$,

$$Q^u(x_i^u) = \begin{cases} 0, & \text{if } q_0^u \le x_i^u < q_1^u \\ 1, & \text{if } q_1^u \le x_i^u < q_2^u \\ \ldots & \\ k-1, & \text{if } q_{k-1}^u \le x_i^u < q_k^u \\ \ldots & \\ N-1, & \text{if } q_{N-1}^u \le x_i^u \le q_N^u \end{cases} \tag{5}$$

Then Gray coding technique (only one bit changes between adjacent code words) is employed to assign an *m*-bit ($m = \log_2^N$) binary code word to each quantization value. For example, quantization values 0, 1, 2 and 3 correspond to 00, 01, 11 and 10, respectively. If x_i^u falls into the second quantization interval, the resulting bits is 01.

Such direct multi-bit quantization methods quantize all the channel measurements and do not drop any bits, so compared with the single-bit quantization, the direct multi-bit quantization-based approaches can significantly increase the key generation rate. However, as the direct multi-bit quantization method places a more strict constraint on the accuracy of channel measurement, it leads to a higher bit mismatch rate (i.e., bits that do not match between two generated keys at Alice and Bob), which seriously influence the performance of key generation algorithm.

In fact, wrong decisions can be made if the channel measurements are close to the quantization region boundaries as shown in **Fig. 4.**. Considering particularly the measurements at the quantization border regions q_i^u $(1 \le i \le 3$ in this case), we can see clearly that they are the most error-prone. In fact a small difference of the cannel measurements as the result of channel estimation error may lead them to cross to the other quantization regions, which causes an error in the quantization process. Therefore the bit mismatch rate between Alice and Bob increases.

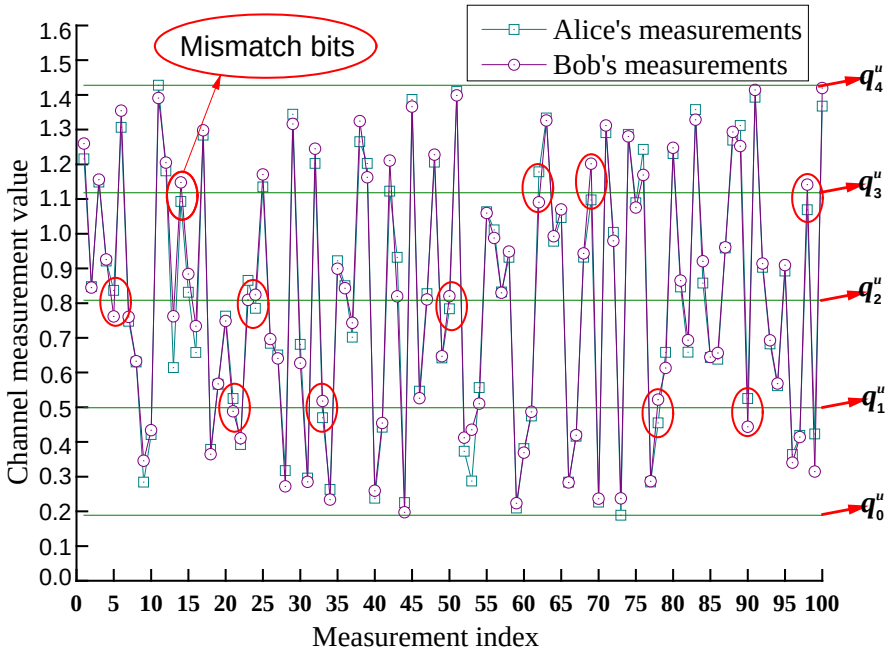


Fig. 4. A sample of 2-bit direct quantizer with four quantization intervals.

As we have discussed above, it is obvious that the high bit mismatch rate is mainly due to the measurements close to the border regions which are mainly caused by the random noise. Therefore, schemes should be designed to remove these effects. The noise presented in the measurements directly affects the bit mismatch rate, which is critical to the secret key establishment as a high bit mismatch rate leads to increased number of probe packets exchanging between Alice and Bob or even a failure to establish secret keys [26].

In order to decrease the bit mismatch rate, a guard-interval based quantization scheme [27] (also known as lossy quantization scheme) was proposed to reduce the error rate near the region boundaries, in which guard intervals separating the different quantization regions were used to avoid quantizing these values that may cause a mismatch. However, the guard-interval mechanism is not optimal in the sense of the efficiency of key extraction. In fact in this approach, measurements that fall in one of these guard intervals are simply discarded to reduce the bit mismatch rate. However, it also leads to a decrease in the key generation rate.

How to balance the key generation rate and the bit mismatch rate in channel character-based key generation is still an open issue.

3. Our proposed quantization method

As we have seen in the previous Section 2, the single-bit quantization-based approach leads to a low key generation rate while the direct multi-bit quantization-based approach is susceptible to the random noise. Moreover, the use of guard intervals lowers the efficiency of key extraction because many measurements along with useful mutual information are discarded.

To reduce the effect of random noise and extract more secret bits, all channel measurements should be considered, which means that no channel measurement should be dropped. Moreover, any exchange of parameters should be done without any loss of secrecy. Based on these basic requirements, we propose a new multi-bit quantization approach to decrease errors

in the quantization phase and improve the performance of quantization. In our proposed scheme, we try to correct the differences of the measurements at the boundary regions instead of simply dropping them. Hence, the key generate rate doesn't decrease.

3.1 Our proposed quantization method

Let $X^u = (x_1^u, x_2^u, ..., x_n^u)$ be the n real channel measurements at user $u = \{A, B\}$. In our proposed scheme, we suppose, without loss of generality, that Alice is the leading node while Bob is the follower.

(1) Alice and Bob first quantize their channel measurements respectively by performing the following steps:

a) Compute the minimum and maximum value of X^u, such as $q_0^u = \min(X^u)$ and $q_N^u = \max(X^u)$.

b) Divide the range $[q_N^u - q_0^u]$ into $N = 2^m$ equal sized intervals $I_0^u = [q_0^u,\ q_1^u),\ I_1^u = [q_1^u,\ q_2^u),\ ...,\ I_{N-1}^u = [q_{N-1}^u,\ q_N^u]$, and the quantization level $q_i^u (1 \le i \le N-1)$ is determined by

$$\begin{aligned} q_i^u &= q_0^u + \frac{q_N^u - q_0^u}{N} i \\ &= q_0^u + \Delta^u i, \quad i = 1, 2, ..., N-1 \end{aligned} \tag{6}$$

where $\Delta^u = \frac{q_N^u - q_0^u}{N}$.

c) The measurement sequence X^u is then fed into quantizer $Q^u(\cdot)$, in which each measurement x_i^u is represented by an array of three elements $(x_{i\_\text{index}}^u,\ x_{i\_value}^u,\ x_{i\_\text{sign}}^u)$. $x_{i\_\text{index}}^u$ represents the index/position of x_i^u, $x_{i\_\text{index}}^u = i$ for x_i^u; $x_{i\_value}^u$ represents the quantization value of x_i^u, $x_{i\_value}^u = k$ if x_i^u is in the kth quantization bin $I_{k-1}^u = [q_{k-1}^u, q_k^u)$; $x_{i\_\text{sign}}^u$ represents the sign of x_i^u, $x_{i\_\text{sign}}^A = '+'$ for $q_{k-1}^u \le x_i^u < q_{k-1}^u + \beta^u$ and $x_{i\_\text{sign}}^A = '-'$ for $q_k^A - \beta^u \le x_i^u < q_k^u$. The concrete design of the quantizer $Q^u(\cdot)$ is as follows:

If the channel measurement value x_i^u is located in the first quantization interval $I_0^u = [q_0^A,\ q_1^A)$,

$$Q^u(x_i^u) = (x_{i\_\text{index}}^u,\ x_{i\_value}^u,\ x_{i\_\text{sign}}^u) = \begin{cases} i,\ 0,\ '-', & \text{if } q_1^u - \beta^u \le x_i^u < q_1^u \\ i,\ 0,\ 'e', & \text{if } q_0^u < x_i^u < q_1^u - \beta^u \end{cases} \tag{7}$$

If x_i^u is located in the kth quantization interval $I_{k-1}^u = [q_{k-1}^u, q_k^u)$, k=2,…, N-1,

$$Q^u(x_i^u) = (x_{i\_\text{index}}^u,\ x_{i\_value}^u,\ x_{i\_\text{sign}}^u) = \begin{cases} i,\ k-1,\ '+', & \text{if } q_{k-1}^u \le x_i^u < q_{k-1}^u + \beta^u \\ i,\ k-1,\ '-', & \text{if } q_k^u - \beta^u \le x_i^u < q_k^u \\ i,\ k-1,\ 'e', & \text{if } q_{k-1}^u + \beta^u \le x_i^u < q_k^u + \beta^u \end{cases} \tag{8}$$

If x_i^u is located in the Nth quantization interval $I_{N-1}^u = [q_{N-1}^u, q_N^u]$,

$$Q^u(x_i^u) = (x_{i\_\text{index}}^u,\ x_{i\_value}^u,\ x_{i\_\text{sign}}^u) = \begin{cases} i,\ k,\ '+', & \text{if } q_k^u \le x_i^u < q_k^u + \beta^u \\ i,\ k,\ 'e', & \text{if } q_k^u + \beta^u \le x_i^u \le q_{k+1}^u \end{cases} \tag{9}$$

where '*e*' is an undefined state, and β^u is a guard interval parameter to be tuned. The superscript u may refer to either Alice ($Q^A(\cdot)$), or to Bob ($Q^B(\cdot)$).

(2) If $x_{i\_\text{sign}}^A = '+'$ or $x_{i\_\text{sign}}^A = '-'$, Alice puts the index and sign $(x_{i\_\text{index}}^A, x_{i\_\text{sign}}^A)$ into a table and sends it to Bob over the public channel.

(3) After receiving the table from Alice, Bob checks his quantized values at the positions specified by Alice to find the mismatch bits which will then be corrected using the following rule:

$$x_{i\_value}^B = \begin{cases} k+1, & if\ \ x_{i\_sign}^B = '-'\ and\ x_{i\_sign}^A = '+' \\ k-1, & if\ \ x_{i\_sign}^B = '+'\ and\ x_{i\_sign}^A = '-' \end{cases} \tag{10}$$

(4) Finally, Alice and Bob use Gray coding to assign a m-bit ($m = \log_2^N$) binary code word to each quantization value whose decimal value is equal to the quantization level index.

Note that Eve may intercept the transmission, however, the indexes and signs do not reveal the quantization region, and therefore the transmission of $(x_{i\_\text{index}}, x_{i\_\text{sign}})$ does not compromise secrecy. On the contrary, Bob can use these information to correct quantization errors, resulting in an increased bit agreement rate.

To give a better review of our quantization scheme, we describe an illustrative example in **Fig. 5**, which are the first twenty measurements from **Fig. 4**. The number of quantization level is 4 and the adjustment parameter $\beta = \frac{1}{4}\Delta^u$.

It can be seen from **Fig. 5** that, after the quantization phase, Alice obtains the initial key bit sequence "10111011111001010000101001111110110000101" with **Table 1**, and Bob obtains the initial key bit sequence "10111011011001010000101001101101100000101" with **Table 2**. Alice finds that there are nine quantization values with $x_{i\_\text{sign}}^A = '+'$ or $x_{i\_\text{sign}}^A = '-'$. To correct these mismatch bits, Alice sends **Table 3** (subset of **Table 1**) to Bob. After receiving Table 3, Bob checks his quantization values at positions 2, 3, 5, 7, 12, 14, 15, 19 and 20. Bob finds that his quantization values at positions 5 and 14 have opposite signs with Alice's. i.e., $x_{5\_sign}^A = '+'$ while $x_{5\_sign}^B = '-'$ and $x_{14\_sign}^A = '-'$ while $x_{14\_sign}^B = '+'$. So Bob will correct his quantization values at positions 5 and 14 using the rule in *Eq.* (10). Thus the mismatches between Alice and Bob are corrected.

Note that in our proposed scheme, only one time communication is needed, in other words, Bob does not need to send any information back to Alice. While in the guard-interval quantization method, two-way communication is needed, that is, Bob needs to send information back to Alice.

Table 1. Quantization results of Alice

$x_{i\_\text{index}}^{A}$	$x_{i\_value}^{A}$	$x_{i\_\text{sign}}^{A}$
1	3	‘e’
2	2	‘+’
3	3	‘+’
4	2	‘e’
5	2	‘+’
6	3	‘e’
7	1	‘-’
8	1	‘e’
9	0	‘e’
10	0	‘e’
11	3	‘e’
12	3	‘+’
13	1	‘e’
14	2	‘-’
15	2	‘+’
16	1	‘e’
17	3	‘e’
18	0	‘e’
19	1	‘+’
20	1	‘-’

Table 2. Quantization results of Bob

$x_{i\_\text{index}}^{B}$	$x_{i\_value}^{B}$	$x_{i\_\text{sign}}^{B}$
1	3	‘e’
2	2	‘+’
3	3	‘+’
4	2	‘e’
5	1	‘-’
6	3	‘e’
7	1	‘-’
8	1	‘e’
9	0	‘e’
10	0	‘-’
11	3	‘e’
12	3	‘e’
13	1	‘-’
14	3	‘+’
15	2	‘+’
16	1	‘-’
17	3	‘e’
18	0	‘e’
19	1	‘+’
20	1	‘-’

Table 3. Values that Alice sends to Bob

$x_{i\_\text{index}}^{A}$	$x_{i\_\text{sign}}^{A}$
2	‘+’
3	‘+’
5	‘+’
7	‘-’
12	‘+’
14	‘-’
15	‘+’
19	‘+’
20	‘-’

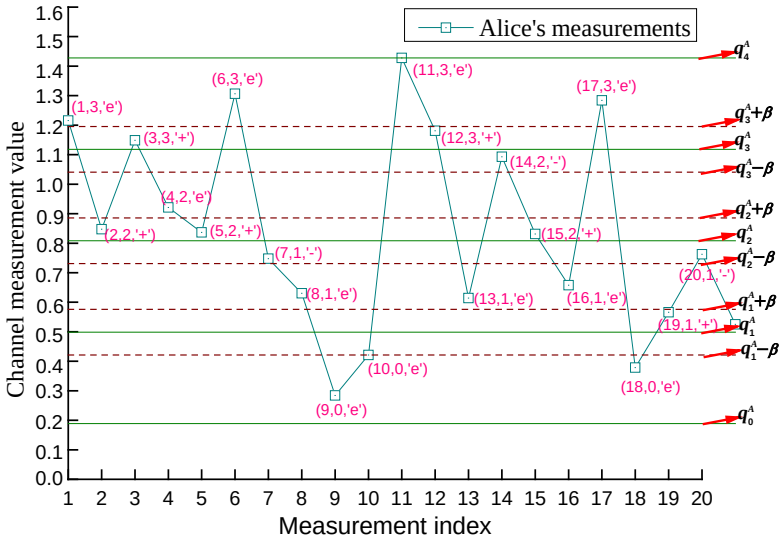
In practice, it could still happen that Alice and Bob come up with different bits. By increasing the parameter β^{u}, we can decrease the chance of disagreement. To make sure that Alice and Bob generate the same key, they can apply further improvements, e.g. information reconciliation and privacy amplification.

3.2 Further Improvements

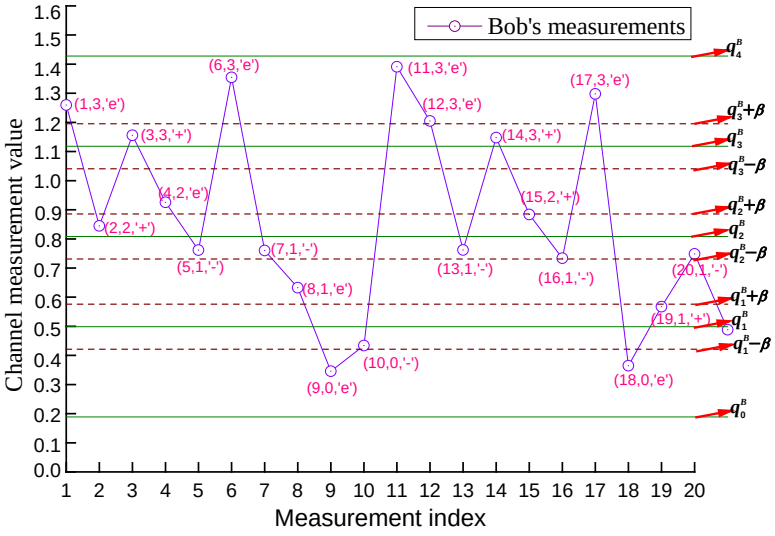
(1) Information Reconciliation

Since key mismatches may still occur, particularly at low SNR levels, a reconciliation step is required to obtain exactly the same shared key bits between Alice and Bob. We used the reconciliation protocol presented in our early work [19] to ensure that the secret keys

generated by Alice and Bob are identical. In the reconciliation protocol, not only the bit error rate comes down quickly to 0, but also the date remaining rate remains high, which makes the subsequent privacy amplification be easily performed. Hence, the total secret key generation rate is improved.



(a) Alice's quantization results



(b) Bob's quantization results

Fig. 5 An example of our proposed quantizer with four quantization intervals.

(2) Privacy Amplification

As the information reconciliation protocol leaks certain bit information to Eve, which she can use to guess partial part of the secret key. So we apply a universal hash function for privacy amplification to eliminate Eve's partial information about the key by reducing the length of the output bit sequence. Although the generated bit sequence is shorter in length it is higher in entropy.

4. Further Performance analysis and simulation results

In this section, we compare our proposed scheme to other existing approaches (the direct multi-bit quantization approach and the guard-interval multi-bit quantization approach) to show a significant improvement in the performance of key generation.

4.1 Bit mismatch rate

The generated bits at Alice and Bob may be different. Each different bit is a mismatch. Bit mismatch rate (BMR) is the ratio of the number of mismatch bits between Alice and Bob to the total number of quantized bits, which is usually be used as a performance parameter to evaluate the quantization approach. A large BMR indicates that the quantization approach is more susceptible to random noise and imperfect channel reciprocity [27].

We implemented several quantization schemes namely the direct multi-bit quantization, the guard-interval multi-bit quantization and our proposed approach on the collected channel phase measurements to analyze and compare the bit mismatch rate and the key generation rate. For evaluation purposes, we tried two different quantization levels, 4 and 8. It is clear that larger boundary regions lead to a lower bit mismatch rate.

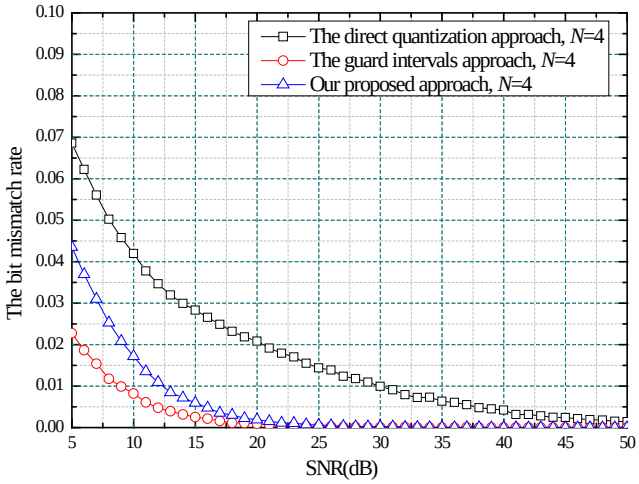
In our proposed scheme, an error occurs only when $|x_i^A - x_i^B|$ is large enough, i.e., $|x_i^A - x_i^B| > 2\beta^u$. **Fig. 6** and **Fig. 7** illustrated the bit mismatch rate under different SNR and β^u. From **Fig. 6** and **Fig. 7**, we can see that for the direct multi-bit quantization approach, the bit mismatch rate is high, while as for the guard-interval multi-bit quantization and our proposed method, the bit mismatch rate decreases as intended. It is below 0.001 when the SNR is higher than 30. The bit mismatch rate of our proposed scheme is as low as that of the guard-interval multi-bit quantization approaches when the SNR is higher than 25. However, the key generation rate of our proposed approach is higher than that of the guard-interval multi-bit quantization approaches as shown in the next Section 4.2.

4.2 Key generation rate

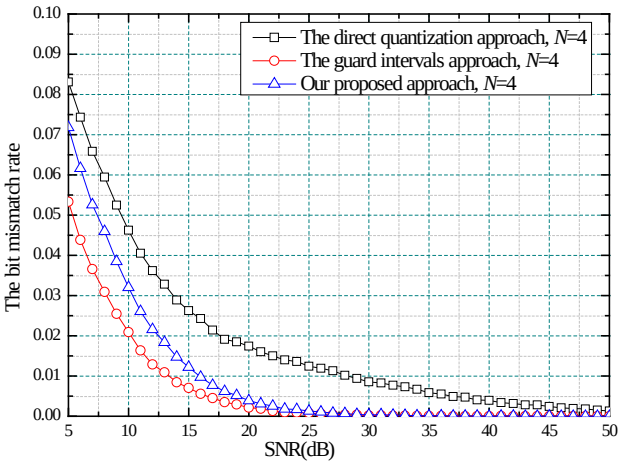
A higher key generation rate indicates that a longer key can be generated in a shorter period of time, thereby achieving a high communication efficiency[17]. In **Fig. 8**, we compare the key generation rate of our proposed method with that of the guard-interval multi-bit approach under SNR of 30dB and $\beta^u = \Delta^u / v$. From the above Section 4.1 and **Fig. 8**, it is obvious that larger boundary regions lead to a lower bit mismatch rate. However, for the guard-interval approach, it will also cause a lower key generation rate as channel measurement lying in the guard intervals are more likely to be discarded. This decreases the bit generation rate and hence the length of the key bit string.

On the contrary, it is not the case in our proposed approach. In our proposed scheme, the key generation rate remains unchanged as we correct the differences of the channel measurements at the boundary regions and no measurements are discarded.

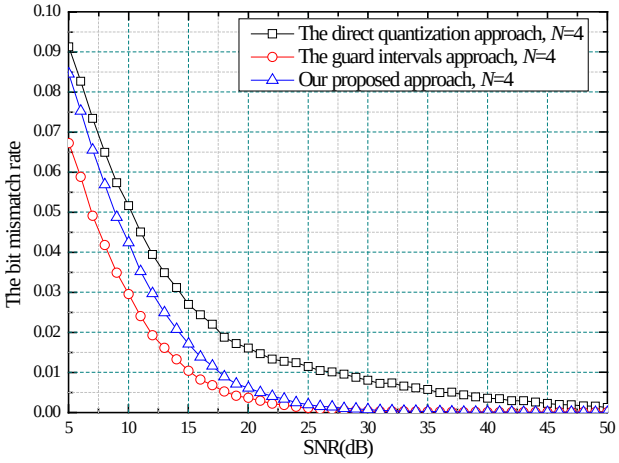
Therefore, our proposed scheme performs better than the guard-interval one and yields more secret key bits. For example, our proposed scheme can extract 3 secret bits per measurement compared to average 1.63 for the guard-interval approach with N=8.



(a) $\beta^u = \Delta^u / 3$

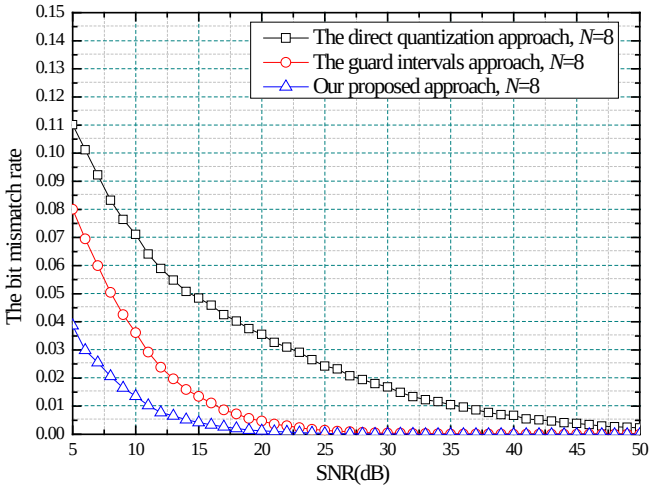


(b) $\beta^u = \Delta^u / 6$

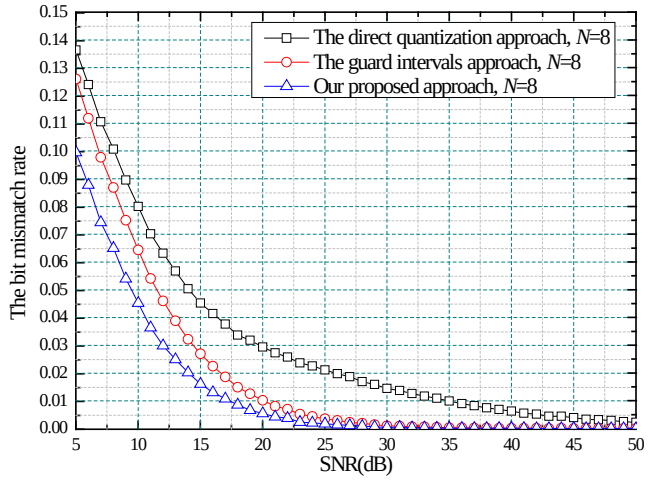


(c) $\beta^u = \Delta^u / 9$

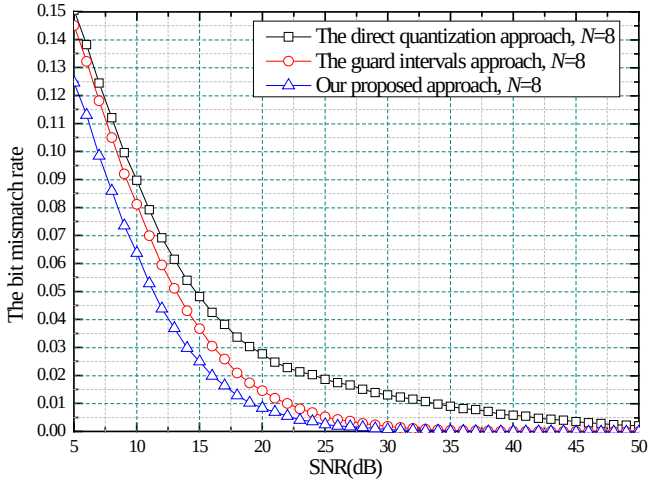
Fig. 6. The bit mismatch rate at different SNR, N=4



(a) $\beta^u = \Delta^u / 3$



(b) $\beta^u = \Delta^u / 6$



(c) $\beta^u = \Delta^u / 9$

Fig. 7. The bit mismatch rate at different SNR, *N*=8

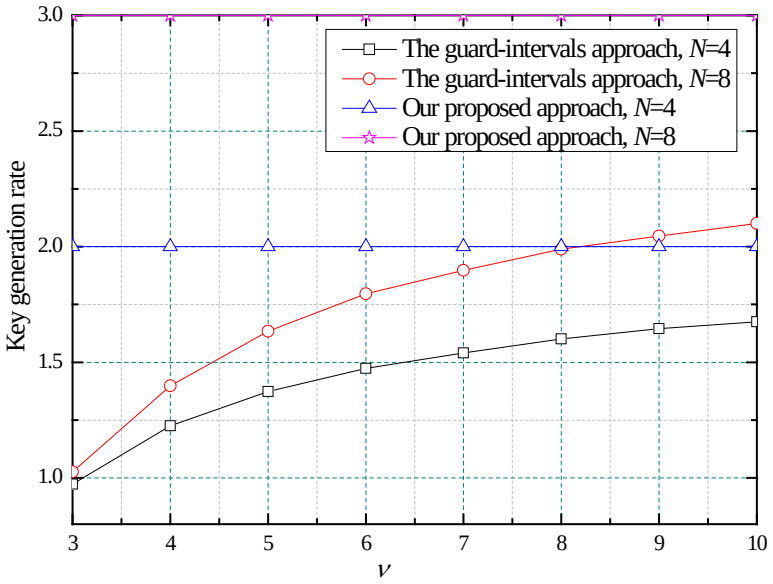


Fig. 8. The comparation of the key generation rate under different β^u.

4.3 Security

As for the security, on the one hand, Eve's observations from the channel probing do not provide her any useful information about measurement sequences X^A and X^B due to the spatial variations. On the other hand, the transmission of $(x_{i\_\text{index}}, x_{i\_\text{sign}})$ over the public channel does not reveal any information about the secret key to the eavesdropper either. This is because that they contain position indexes and signs only, whereas the generated secret bits depend upon the values of the channel measurements at those indexes. Further, Eve cannot use these signs to infer the values of the channel estimates of Alice or Bob at those indexes. Hence, our proposed scheme is secure and causes no loss of secrecy.

Note that, our proposed scheme can be performed in conjunction with other quantization algorithms such as the multi-bit adaptive secure bit generation (ASBG) [2] and the difference-based quantization [28] to further improve the quantization performance.

5. Conclusions and future work

Using wireless channel characteristics to generate a shared secret key is becoming a proliferate area for its high reliability, easy implementation, and low energy consumption. In this paper, we investigated and discussed the quantization methods in the channel characteristics-based secret key generation process. We focused on the issues of how to remove the effect of random noise and to balance the key generation rate and the bit mismatch rate. We presented a new quantization scheme with high key generation rate and low bit mismatch rate. In our proposed scheme, we try to use all channel measurements and correct the differences between them caused by noise at the boundary regions instead of simply dropping them. We evaluated the proposed schemes in terms of the bit mismatch rate, key generation rate and security. The simulation results show that our proposed scheme can work reliably with high efficiency. Our proposed scheme achieves lower bit mismatch rate and at the same time remains high key generation rate. Moreover, our proposed scheme can be performed in conjunction with other

quantization algorithms such as ASBG and the difference-based quantization to further improve the quantization performance.

The main problem of the secret key generation based on wireless channel characteristics is that the efficiency of the existing quantization methods and information reconciliation protocols and thus the total secret key generation rate are still low, so designing higher efficient quantization methods and information reconciliation protocols is our future work.

References

[1] S. Mathur, W. Trappe, N. Mandayam, C. Ye and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proc. of 14th ACM international conference on Mobile computing and networking (MobiCom)*, pp. 128-139, Sep. 14-19, 2008. Article (CrossRef Link).

[2] S. Jana, S.N. Premnath, M. Clark, S.K. Kasera, N. Patwari and S.V. Krishnamurthy, "On the Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environments," in *Proc. of 15th ACM international conference on Mobile computing and networking (MobiCom)* MobiCom, pp. 321-332, Sep. 20-25, 2009. Article (CrossRef Link).

[3] Y. Luo, L. Pu, Z. Peng and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: advantages, challenges, and performance improvements," *IEEE Communications Magazine*, vol. 54, no. 2, pp. 32-38, Feb., 2016. Article (CrossRef Link).

[4] H. Liu, J. Yang, Y. Wang and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," *in Proc. of 31st IEEE International Conference on Computer Communications (INFOCOM)*, pp. 927-935, Mar. 24-30, 2012. Article (CrossRef Link).

[5] S.N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917-930, May, 2013. Article (CrossRef Link).

[6] S. T. Ali, V. Sivaraman and D. Ostry, "Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices," *IEEE Transactions on Mobile Computing*, vol. 13, no.12, pp. 2763-2776, Dec., 2014. Article (CrossRef Link).

[7] R. Guillaume, F. Winzer, A. Czylwik, C.T. Zenger and C. Paar, "Bringing PHY-based Key Generation into the Field: An Evaluation for Practical Scenarios," in *Proc. of 82nd IEEE Vehicular Technology Conference (VTC Fall)*, pp. 1-5, Sep. 6-9, 2015. Article (CrossRef Link).

[8] S. Mathur, R. Miller, A. Varshavsky, W. Trappe and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proc. of the 9th ACM international conference on Mobile systems, applications, and services (MobiSys)*, pp. 211-224, June 28-July 1, 2011. Article (CrossRef Link).

[9] Q. Wang, K. Xu and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, no.9, pp. 1666-1674, Sep. 2012. Article (CrossRef Link).

[10] M. G. Madiseh, S. He, M. L. McGuire and C. Paar, "Verification of secret key generation from UWB channel observations," in *Proc. of IEEE International Conference on Communications (ICC)*, pp. 1-5, June 14-18, 2009. Article (CrossRef Link).

[11] S. T. B. Hamida, J. B. Pierrot and C. Castelluccia, "An Adaptive Quantization Algorithm for Secret Key Generation Using Radio Channel Measurements," in *Proc. of 3rd International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1-5, Dec. 20-23, 2009. Article (CrossRef Link).

[12] J. Huang and T. Jiang, "Dynamic secret key generation exploiting Ultra-wideband wireless channel characteristics," in *Proc. of IEEE Wireless Communications and Networking Conference (WCNC)*, pp.1701-1706, Mar. 9-12, 2015. Article (CrossRef Link).

[13] G. D. Durgin, Space-time wireless channels. Prentice Hall, Upper Saddle River, NJ, USA, 2003.
[14] 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. of 18th International OFDM Workshop (InOWo)*, pp. 1-5, Aug. 27-28, 2014.
[15] K. Ren, H. Su and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Communications*, vol. 18, no.4, pp.6-12, Apr. 2011. Article (CrossRef Link).
[16] C. T. Zenger, J. Zimmer and C. Paar, "Security Analysis of Quantization Schemes for Channel-based Key Extraction," *in Proc. of Workshop on wireless communication security at the physical layer(WiComSec-Phy)*, pp. 267-272, July 22, 2015. Article (CrossRef Link).
[17] T. Wang, Y. Liu and A. V. Vasilakos, "Survey on channel reciprocity based key establishment techniques for wireless systems," *Wireless Networks*, vol.21, no.6, pp.1835-1846, June, 2015. Article (CrossRef Link).
[18] Q. Wang, X. Wang, Q. Lv, X. Ye, Y. Luo and L. You, "Analysis of the information theoretically secret key agreement by public discussion", *Security and Communication Networks*, vol.8, no.15, pp. 2507-2523, Oct. 2015. Article (CrossRef Link).
[19] Q. Wang, X. Wang, Q. Lv, X. Ye, L. You and R. Zeng. "A New Information Reconciliation Protocol in Information Theoretically Secret Key Agreement," *Journal of Computational Information Systems*, vol.10, no.21, pp. 9413-9420, Nov. 2014. Article (CrossRef Link).
[20] C. H. Bennett, G. Brassard, C. Crépeau and U. Maurer, "Generalized privacy amplification", *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915-1923, June, 1995. Article (CrossRef Link).
[21] Q. Wang, X. Wang and Q. Lv, "A privacy amplification protocol against active attacks in information theoretically secret key agreement," in *Proc. of International Conference on Network Security and Communication Engineering (NSCE)*, pp.3-6, Dec. 25-26, 2014.
[22] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over fading channels," in *Proc. of Military Communications Conference (MILCOM)*, pp.54-58, Oct. 28-31, 2001. Article (CrossRef Link).
[23] 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, Feb. 2010. Article (CrossRef Link).
[24] 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 Transactions on Antennas and Propagation*, vol.53, no.11, pp. 3776-3784, Nov. 2005. Article (CrossRef Link).
[25] A. Ambekar, M. Hassan H. D. Schotten, "Improving channel reciprocity for effective key management systems," in *Proc. of IEEE International Symposium on Signals, Systems, and Electronics (ISSSE)*, pp. 1-4, Oct. 3-5, 2012. Article (CrossRef Link).
[26] H. Liu, Y. Wang, J. Yang and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," *in Proc. of 29st IEEE International Conference on Computer Communications (INFOCOM)*, pp.3048-3056, Apr. 14-19, 2013. Article (CrossRef Link).
[27] K. Zeng, D. Wu, A. Chan and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," *in Proc. of 32st IEEE International Conference on Computer Communications (INFOCOM)*, pp. 1-9, Mar. 15-19, 2010. Article (CrossRef Link).
[28] B. Zan, M. Gruteser and F. Hu, "Improving robustness of key extraction from wireless channels with differential techniques," *in Proc. of International Conference on Computing, Networking and Communications (ICNC)*, pp. 980-984, Jan. 30- Feb.2, 2012. Article (CrossRef Link).

Qiuhua Wang received her B.S. and M.S. degrees in communication engineering from Liaoning Technical University, Fuxin, China, in 2000 and 2003, respectively. She received her Ph.D. degree in communications and information systems from Zhejiang University, Hangzhou, China, in 2013. Now, she is an Associate Professor of the School of Cyberspace, Hangzhou Dianzi University. Her current research interests include information security, security issues in wireless networks, key management and physical layer security, *etc*.

Qiuyun Lyu received her B.S. and M.S. degrees in Computer Science and Technology from Chang'an University, Xi'an, China, in 2000 and 2003, respectively. Now, she is an Associate Professor of the School of Cyberspace, Hangzhou Dianzi University. Her current research interests include information security and privacy, security issues in wireless networks.

XiaojunWang received his B.S. and M.S. degrees in communication and information system from University of Electronic Science and Technology of China, Chengdu, china, in 1997 and 2000 respectively. Now, he is a teacher of the School of Cyberspace, Hangzhou Dianzi University. His research interests include information security, vulnerability analysis and software security.

Jianrong Bao received his B.S. degree in Polymer Materials & Eng., and the M.S.E.E. degree from Zhejiang University of Technology, Hangzhou, China, in 2000 and 2004, respectively. He received his Ph.D. E.E. degree from the Department of Electronic Engineering, Tsinghua University, Beijing, China, in 2009. He is with the school of Information Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include space wireless communications, communication signal processing, information security & channel coding, *etc*.