IEICE TRANS. INF. & SYST., VOL.E103–D, NO.2 FEBRUARY 2020

PAPER Special Section on Security, Privacy, Anonymity and Trust in Cyberspace Computing and Communications

A Practical Secret Key Generation Scheme Based on Wireless Channel Characteristics for 5G Networks

Qiuhua WANG[†a)], **Mingyang KANG**[†], **Guohua WU**[†], **Yizhi REN**[†], ***Nonmembers***, ***and*** **Chunhua SU**[††], ***Member***

SUMMARY Secret key generation based on channel characteristics is an effective physical-layer security method for 5G wireless networks. The issues of how to ensure the high key generation rate and correlation of the secret key under active attack are needed to be addressed. In this paper, a new practical secret key generation scheme with high rate and correlation is proposed. In our proposed scheme, Alice and Bob transmit independent random sequences instead of known training sequences or probing signals; neither Alice nor Bob can decode these random sequences or estimate the channel. User's random sequences together with the channel effects are used as common random source to generate the secret key. With this solution, legitimate users are able to share secret keys with sufficient length and high security under active attack. We evaluate the proposed scheme through both analytic and simulation studies. The results show that our proposed scheme achieves high key generation rate and key security, and is suitable for 5G wireless networks with resource-constrained devices.

key words: *secret key generation, physical-layer security, channel reciprocity, information reconciliation, privacy amplification*

1. Introduction

Establishing secure secret keys between two legitimate users is a fundamental requirement for secure communication. It remains a challenge especially in next generation wireless networks, such as 5G wireless network where a fixed key management infrastructure is not available. The process of key management (key generation and secure key exchange) becomes even more challenging for 5G wireless network because the number of nodes increases to a massive scale and nodes become more heterogeneous in their computational capabilities [1]. The traditional approach to this problem is to use public key cryptographies. However, such a scheme consumes a lot of computational resource and energy which are not available in some scenarios (e.g., the upcoming 5G wireless networks, wireless sensor networks, or the Internet of Ting (IoT)). Moreover, since public key cryptographies are based on the hardness of mathematical problems, they are only computational security.

Recently, many wireless-channel-characteristic-based methods have been proposed as an alternative solution to secret key establishment in wireless networks. Such technique provides an excellent approach to the problems of key-establishment and can even achieve information theoretical secrecy. The basic idea behind it is to make use of the inherent and unique randomness, reciprocity and spatial decorrelation of wireless physical fading channel, and an attacker cannot experience exactly the same channel fading as any legitimate user [2].

In typical wireless network environments, the wireless channel between two legitimate users, Alice and Bob, is reciprocal and varies randomly over time and space. Alice and Bob can measure some characteristics (e.g., wireless channel state information (CSI) [3]–[9] or received signal strength (RSS) [2], [10]–[14]) and then utilize them as shared random sources to generate a secret key. Even if an eavesdropper, Eve, who is more than a half-wave-length away from Alice and Bob, would obtain no information about the secret key because she experiences independent fading and thus cannot measure the same channel characteristics as Alice and Bob [2].

1.1 The Channel Characteristic-Based Secret Key Generation

The typical steps in a traditional channel characteristic-based secret key generation system are illustrated in Fig. 1. In the first step, Alice and Bob exchange known training sequences (or probing signals) with each other. From the received signals, both Alice and Bob can measure the channel characteristics such as RSS [2], [10]–[14], amplitude [3]–[5] and phase [6]–[9] of channel impulse response (CIR), respectively. These channel measurements are then quantized and converted into bit sequences to generate preliminary key sequences used in the third step. The quantization methods include binary quantization [10], adaptive secret bit generation [8], [15], differential quantization [16], non-uniform quantization [17] and multiple-bit quantization [18], [19], etc. The paper [20] summarizes some existing quantization methods. The preliminary key sequences obtained at Alice and Bob are often subject to discrepancies, particularly at very low SNR due to channel random noise and hardware limitations. Information reconciliation (IR) protocol is then used to correct or eliminate these errors. The objective of IR is to make Bob and Alice agree upon a shared secret key. Many IR protocols have been proposed such as the BBBSS protocol [21], the CASCADE protocol [22], the Winnow protocol [23], and so on. In our earlier work [24], some typical IR protocols have been introduced and analyzed theoretically and a new IR protocol was presented in [25]. While the IR strategies reduce the bit error rate (BER),

Manuscript received March 9, 2019.
Manuscript publicized October 16, 2019.
[†]The authors are with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou 310018, China.
[††]The author is with the Division of Computer Science, University of Aizu, Aizuwakamatsu-shi, 965–8580 Japan.
a) E-mail: wangqiuhua@hdu.edu.cn
DOI: 10.1587/transinf.2019INI0001

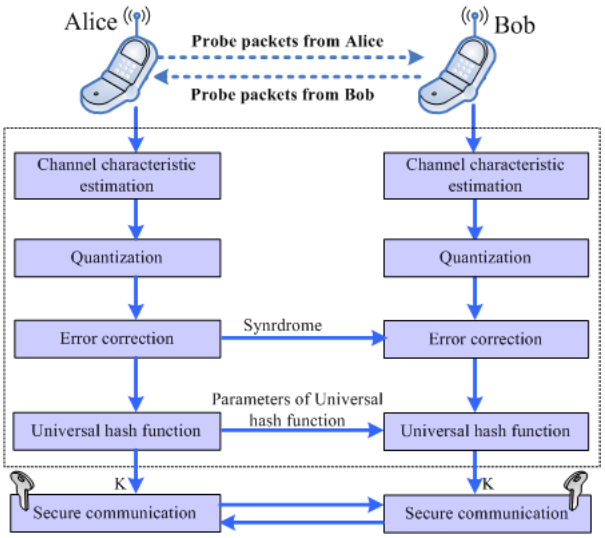


Fig. 1 Typical steps in a traditional channel characteristic-based secret key generation system.

they leak some information of the secret key to the eavesdropper who can use them to guess portions of the extracted key. Hence, privacy amplification (PA) protocol is used in the fifth step. In the PA phase, a universal hash function is used by Alice and Bob to distill a highly-secret key sequence, about which Eve knows a negligible amount of information [26].

1.2 Related Works

The idea of exploring wireless channel characteristics for secret key generation was first presented by Hershey et al. in [27]. After their fundamental work, many key generation schemes based on various aspects of physical channel characteristic came into research focus. These schemes mainly utilize RSS and other channel characters, such as amplitude and phase of CIR, as common random sources to generate secret keys [2]–[14]. A recent study in [28] has given a thorough literature review on the key generation techniques. In particular, the use of channel phase was studied and applied to wideband system [3] and narrowband system [4], [5]. However, only one practical phase-based key generation system was implemented in a narrowband system [5] and no practical schemes have been reported to be applied in wideband system. The reason is that the phase is susceptible to noise, time and carrier frequency offset and asynchronous clock drift at the receiver, etc [19]. The amplitude of CIR was also considered and has been extended to UWB systems [6]–[9]. However, these works assume that the channels observed at the users must be independent over time, which limits the key generation rate in slow fading channels. Some researchers considered using channel frequency response (CFR) which provides channel effect in frequency domain. CFR-based systems have been mostly implemented in IEEE 802.11 OFDM systems [29], [30], as it is convenient to extract channel estimation.

Currently, the most popular channel parameter used in key generation is RSS, especially for practical implementation. It is because of the fact that most of the current off-the-shelf wireless cards, without any modification, can measure it on a per packet/frame basis. The variation over time of the RSS caused by motion and multipath fading can be quantized and used for generating secret keys. Most RSS-based key generation schemes are mainly applied in IEEE 802.11 [2], [10]–[12] and IEEE 802.15.4 systems [13], [14]. However, only one RSS value can be obtained from each packet/frame, which limits the key generation rate. In addition, it is susceptible to predictable channel attacks, because RSS readings increases and decreases if the channel is blocked periodically [10]. What's more, it cannot work well in static scenarios due to infrequent and small-scale variations in channel measurements. The static channel scenarios can be very challenging for successful key generation. To address this issue, researchers came up with some possible solutions. For example, key generation schemes based on the artificially controlled fluctuation of the channel property are developed in [31]. The authors of [32] proposed a key generation scheme exploiting the frequency-selectivity of the fading channel. In [33], Huang et al. proposed to additionally utilize beamforming by employing a multiple antenna system. Another popular solution approaching the challenge of static channels is exploiting helper devices such as relays. In [13], Liu et al. proposed a collaborative scheme for relay-assisted generation of group keys. Yet they only addressed scenarios with out-of-range communication. The authors of [34] considered four different relaying methods comprising MIMO techniques, artificial noise as well as network coding. The challenge of generating secret keys from slow changing channels was particularly addressed by Lai et al. [35]. However, all these methods do not work well when the fluctuation of the channel property is so small that the generated keys become monotonic. It is easy for eavesdroppers to break such monotonic keys.

1.3 Issues in the Channel Characteristic-Based Secret Key Generation

Current secret key generation techniques highly depend on a rapid changing environment to ensure a high key generation rate. Static channel scenario is the main challenge for successful secret key generation. In a static or low-mobility wireless environment, the channel changes so slowly that the schemes can hardly obtain enough uncorrelated bits in a short time. Moreover, the key generation rate is relatively low in static wireless environments. Several schemes have been proposed to address this issue. However, they cannot work well due to infrequent and small-scale variations in channel measurements. In these schemes, the key generation rate is low and accordingly the security is reduced. Moreover, weak secret keys are generated under an environment where the fluctuation of channel characteristics is not deeply undulated [36]. Although researchers have come up with a variety of methods to introduce randomness into

static channels [17], [33], [37]–[40], these methods are not generic as described in [28]. It still remains a challenge to generate secret key with high rate for the application of channel characteristic-based key generation systems in static environments.

On the other hand, existing key generation schemes are mainly designed and analyzed under passive attacks. Almost all of the previous methods are suffering from the active attack in which the smart adversary tries to manipulate the channel characteristic by inserting or removing intermediate objects [10], [41]. The fundamental reason is that Alice and Bob only use the channel measurements to generate secret keys. If the channel is manipulated by the attacker, the generated keys can also be inferred. How to achieve a robust key generation scheme under above active attack is also an open issue. In [41], Zeng proposed to integrate user-generated randomness into the channel probing to defend against the aforementioned active attacks. The idea that the legitimate users exchange random signals to form common key source is also investigated in [42] and [43]. We think it is a sound idea. And based on this idea and taking into account the green communication interests for the next generation wireless systems, we design and implement a practical and generic channel characteristic-based secret key generation scheme. Different from [41] and [43], our proposed scheme simplifies the multiplication operations to XOR, and this simplification is reasonable and valuable to avoid multiplication operation, which is easy to implement and enables lightweight security in 5G IoT scenarios. Our proposed scheme is more energy efficient and practical and it neither requires special hardware or any helper to inject noise into the system, which also prolongs its battery life. Furthermore, the key generation rate of our proposed scheme is high because it is not limited by the channel randomness.

1.4 Our Work and Contributions

Our work and main contributions include three aspects.

1. We propose a practical and generic secret key generation scheme. In our proposed scheme, Alice and Bob transmit random sequences to each other instead of known training sequences or probing signals, neither Alice nor Bob can decode these random sequences or estimate the channel characteristics. And user random sequences together with the channel characteristics serve as the source of common randomness to generate shared secret keys. Compared with existing approaches which only use the channel characteristics, our proposed scheme is highly more flexible and can be applied in both static and mobile environments.
2. Our proposed scheme introduces extra randomness to key generation and removes the reliance on user mobility in contrast to constant probing signal-based approaches. Different from previous solutions coping with static channel scenarios, our approach does not rely on specialized hardware and still exploits temporal and spatial diversity. Moreover, our proposed scheme can prevent the active attack introduced in Sect. 2, and can generate stronger secret keys in a shorter time.
3. We evaluate our proposed scheme through both analytic and simulation studies. The results show that our proposed scheme achieves lower bit error ratio between the legitimate users, while ensuring very high error probability at the eavesdropper. At the same time, our proposed scheme ensures high key generation rate and key security.

1.5 Organization of the Paper

The rest of the paper is organized as follows. Section 2 introduces the system model used in our proposed scheme. Section 3 provides the detailed description of our proposed scheme including random signal transmission, common randomness obtaining, information reconciliation and privacy amplification. Section 4 presents the performance analysis and simulation results. Finally, we conclude the paper in Sect. 5.

2. System Model

We consider a generic wireless communication scenario as depicted in Fig. 2, where two authorized users, Alice and Bob, want to extract a shared secret key via wireless channel in the presence of an unknown eavesdropper, Eve. h_{ab} and h_{ba} are modeled as the forward and reverse channels between Alice and Bob. h_{ae} and h_{be} are the channels from Alice to Eve and from Bob to Eve. According to the channel reciprocity, we have $h_{ab} = h_{ba} = h$ over the coherence time period τ, but $h_{ae} \neq h_{ab}$ and $h_{be} \neq h_{ba}$ due to the spatial decorrelation if Eve keeps a short distance, say at least $\lambda/2$ (λ is the wavelength) away from the legitimate receiver. For networks working at 2.4GHz the distance is 6.25cm. Eve is assumed to be able to listen to all the communications between Alice and Bob. Eve aims to derive the secret key generated between Alice and Bob, and she is not interested in disrupting the key establishment protocol by jamming the communication channels, so she won't prevent Alice and Bob from generating secret keys or modify any message exchanged by Alice and Bob. However, she has some abilities to affect the communication channel between Alice and

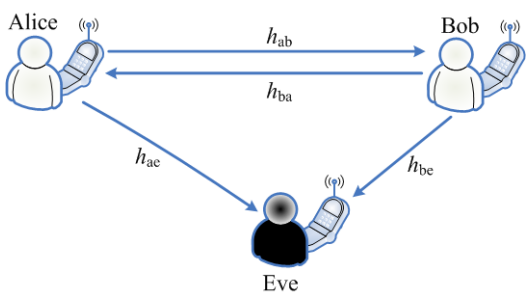


Fig. 2 Wireless communication scenario.

Bob, for example, by inserting or removing intermediate objects [10]. In addition, the whole key generation protocol is known to Eve, and during key generation process, she can also perform estimation based on the received signals. We assume the legitimate nodes are all trusted, and node compromise and man-in-the middle attacks are not considered here as in the most existing approaches [10], [16].

3. Our Proposed Key Generation Scheme

Existing approaches only use the channel measurements to extract secret keys, and they do not work well in static or low-mobility environments. Also, if an attacker can manipulate the channel measurements, she can manipulate the distribution of bits or infer the extracted keys. With these observations in mind, we propose a practical secure key generation approach in which another randomness is introduced into the channel probing. In our proposed scheme, instead of transmitting known training sequences or probing signals, Alice and Bob transmit secret random sequences to each other. After receiving the random sequence, both of them add their own random sequence to it to generate a common randomness which is further used to generate a shared secret key. It is difficult for Eve to generate the same key by using her received signals because her channel characteristics are different and she has no knowledge of Alice's or Bob's random sequences.

In our proposed scheme, we suppose, without loss of generality, that Alice is the leading node and Bob is the follower. Alice first generates a random sequence and transmits it to Bob who then directly generates and transmits another random sequence back to Alice. Also, to enhance the robustness of the proposed scheme, we use information reconciliation and privacy amplification to reconcile bit discrepancies and improve the randomness of generated keys.

The key generation procedure of our proposed scheme is divided into four stages: random signal transmission, common randomness obtaining, information reconciliation and privacy amplification, as illustrated in Fig. 3.

3.1 Random Signal Transmission

Alice and bob each generates a secret random signal and send it to each other. The two parties can use the same-frequency half-duplex technology to transmit in turn during the channel coherence time, or they can use the same-frequency full-duplex technology to transmit.

1. Alice generates a secret random bit sequence $\mathbf{X}_a = [x_a(1), x_a(2), \ldots\ldots, x_a(n)] \in (0,1)^n$ which is not known to any other party. Then Alice modulates $\mathbf{X}_a(n)$ which is then transmitted to Bob in the form of radio frequency (RF) signal $x_a(t)$ over the wireless fading channel.
2. Similarly, Bob generates another different secret random bit sequence $\mathbf{X}_b = [x_b(1), x_b(2), \ldots\ldots, x_b(n)] \in (0,1)^n$ (which is independent to $\mathbf{X}_a(n)$), modulates it and then transmits it to Alice in the form of a RF signal $x_b(t)$ over the wireless fading channel.

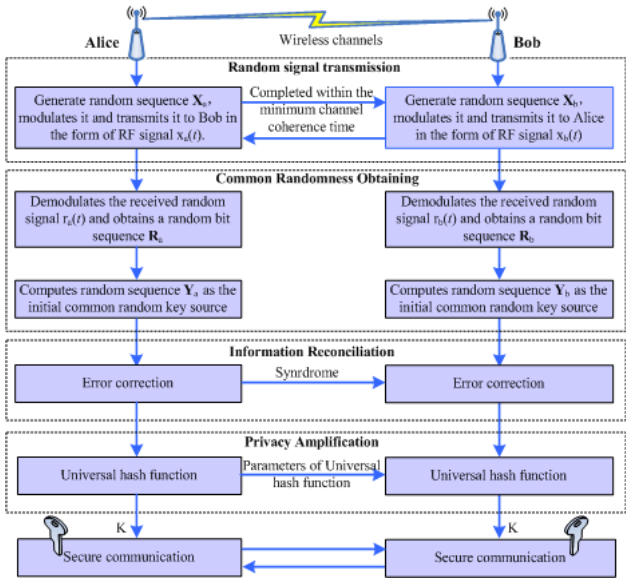


Fig. 3 The key generation procedures of our proposed scheme.

The two transmissions difference is smaller than the channel coherence time so the channel properties can be regarded as constant.

3.2 Common Randomness Obtaining

After receiving the random signal from the other party, Alice and Bob generate an initial common random key source for generating the shared key. Common randomness obtaining is the key step to harvest the randomness from the user random sequence and the channel.

1. Affected by channel and noise, Alice receives signal $r_a(t)$ with

$$r_a(t) = h_{ba}(t)x_b(t) + n_a(t) \tag{1}$$

in which $h_{ba}(t)$ is the channel responses from Bob to Alice, $n_a(t)$ is the zero mean zero mean Additive Gaussian Noises (AWGN) with variance δ_a^2. It is reasonable to assume that all noises are independent of each other.
Similarly, Bob receives signal $r_b(t)$ with

$$r_b(t) = h_{ab}(t)x_a(t) + n_b(t) \tag{2}$$

in which $h_{ab}(t)$ is the channel responses from Alice to Bob, $n_b(t)$ is the zero mean AWGN with variance δ_b^2.
2. Alice demodulates the received random signal $r_a(t)$ and obtains a random bit sequence $\mathbf{R}_a = [r_a(1), r_a(2), \ldots\ldots, r_a(n)]$. The influence of both channel and noise cause the demodulated sequence $\mathbf{R}_a$ to be erroneous with respect to the original sequence $\mathbf{X}_b$ transmitted by Bob. Hence, the demodulated random sequence $\mathbf{R}_a$ can be written in the following form:

$$\mathbf{R}_a = \mathbf{X}_b \oplus \mathbf{H}_{ba} \oplus \mathbf{N}_a \tag{3}$$

where, $\mathbf{H}_{ba} = [h_{ba}(1), h_{ba}(2), \ldots\ldots, h_{ba}(n)] \in (0,1)^n$ denotes errors that the wireless channel causes to the random sequence $\mathbf{X}_b$ during demodulating $r_a(t)$, and $\mathbf{N}_a = [n_a(1), n_a(2), \ldots\ldots, n_a(n)] \in (0,1)^n$ indicates errors that the noise causes to the random sequence $\mathbf{X}_b$ during demodulating $r_a(t)$; Symbol $\oplus$ represents exclusive or (XOR).

Similarly, Bob demodulates $r_b(t)$ and obtains the random bit sequence $\mathbf{R}_b = [r_b(1), r_b(2), \ldots\ldots, r_b(n)]$, which can be written with

$$\mathbf{R}_b = \mathbf{X}_a \oplus \mathbf{H}_{ab} \oplus \mathbf{N}_b \tag{4}$$

where, $\mathbf{H}_{ab} = [h_{ab}(1), h_{ab}(2), \ldots\ldots, h_{ab}(n)] \in (0,1)^n$ denotes errors that the wireless channel causes to the random sequence $\mathbf{X}_a$ during demodulating $r_b(t)$, and $\mathbf{N}_b = [n_b(1), n_b(2), \ldots\ldots, n_b(n)] \in (0,1)^n$ indicates errors that the noise causes to the random sequence $\mathbf{X}_a$ during demodulation.

3. Alice computes random sequence

$$\begin{aligned}\mathbf{Y}_a &= \mathbf{X}_a \oplus \mathbf{R}_a \\ &= \mathbf{X}_a \oplus \mathbf{X}_b \oplus \mathbf{H}_{ba} \oplus \mathbf{N}_a\end{aligned} \tag{5}$$

Bob computes random sequence

$$\begin{aligned}\mathbf{Y}_b &= \mathbf{X}_b \oplus \mathbf{R}_b \\ &= \mathbf{X}_a \oplus \mathbf{X}_b \oplus \mathbf{H}_{ab} \oplus \mathbf{N}_b\end{aligned} \tag{6}$$

Alice and Bob repeat the above stages 3.1 and 3.2 every T_s with $T_s > \tau$, until the length of the common key sequence has reached the required length.

3.3 Information Reconciliation

Due to the imperfect reciprocity of the wireless channel, the generated bit sequences at Alice and Bob, $\mathbf{Y}_a$ and $\mathbf{Y}_b$, are usually not identical, particularly at low SNR levels. This is mainly due to two reasons: Alice and Bob cannot measure the channel simultaneously due to the half-duplex property of the channel, and the noises at Alice's and Bob's sides are usually independent. Here, we used reconciliation protocol presented in our earlier work [25] to ensure that the secret keys generated by Alice and Bob are identical. In the information reconciliation protocol, the bit error rate comes down quickly to 0.

3.4 Privacy Amplification

As the information reconciliation protocol leaks a certain amount of bit information to Eve, who can use it 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 and security.

4. Analysis and Simulation Results

In our proposed scheme, user random sequence together with the channel affects are used as common randomness source to generate the secret key. Instead of transmitting known training sequences or probing signals, Alice and Bob transmit secret random sequences $\mathbf{X}_a$ and $\mathbf{X}_b$, respectively, to each other, neither Alice nor Bob can decode this random sequence or estimate the channel correctly. If every transmission of this protocol is completed within the minimum channel coherence time, the channel reciprocity holds, i.e. $h_{ab} = h_{ba} = h$, that is, the transmitted signals from each other will experience the same fading, and Alice and Bob may obtain a shared randomness $\mathbf{X}_a \oplus \mathbf{X}_b \oplus \mathbf{H}_{ba}$, hence, $\mathbf{Y}_a$ and $\mathbf{Y}_b$ can be used as secret key candidate to generate a shared key K. From $(\mathbf{Y}_a, \mathbf{Y}_b)$, Alice and Bob can generate a shared key with the upper bound rate $\mathbf{R}_s \leqslant \min[I(\mathbf{Y}_a; \mathbf{Y}_b), I(\mathbf{Y}_a; \mathbf{Y}_b \mid \mathbf{Y}_e)]$ [37].

Although Eve can eavesdrop the transmitted signals $x_a(t)$ and $x_b(t)$ sent by Alice and Bob, the signals received by her are completely different due to the spatial decorrelation of wireless channel:

$$r_{ae}(t) = h_{ae}(t)x_a(t) + n_{ae}(t) \tag{7}$$

$$r_{be}(t) = h_{be}(t)x_b(t) + n_{be}(t) \tag{8}$$

Where $h_{ae}(t)$ and $h_{be}(t)$ denote the channel responses from Alice to Eve and from Bob to Eve, respectively; $n_{ae}(t)$ and $n_{be}(t)$ are zero mean additive Gaussian noises with variances δ_{ae}^2 and δ_{be}^2, respectively. $n_a(t)$, $n_b(t)$, $n_{ae}(t)$ and $n_{be}(t)$ are independent with each other and are also independent with $h_{ab}(t)$, $h_{ba}(t)$, $h_{ae}(t)$ and $h_{be}(t)$.

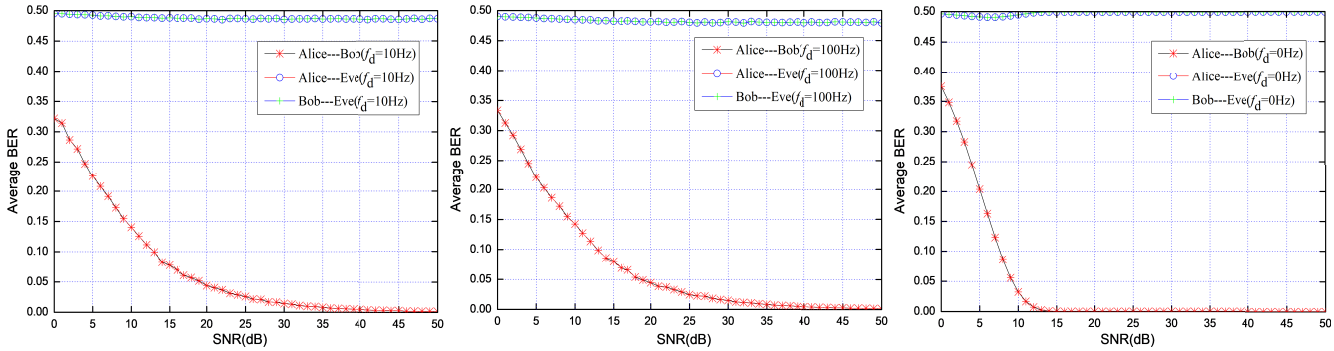
Eve demodulates $r_{ae}(t)$ and $r_{be}(t)$, and can only obtain random sequence

$$\mathbf{Y}_e = \mathbf{X}_a \oplus \mathbf{X}_b \oplus \mathbf{H}_{ae} \oplus \mathbf{H}_{be} \oplus \mathbf{N}_{ae} \oplus \mathbf{N}_{be} \tag{9}$$

where $\mathbf{H}_{ae} = [h_{ae}(1), h_{ae}(2), \ldots\ldots, h_{ae}(n)] \in (0,1)^n$ denotes errors that the wireless channel causes to the random sequence $\mathbf{X}_a$ during demodulating $r_{ae}(t)$; $\mathbf{H}_{be} = [h_{be}(1), h_{be}(2), \ldots\ldots, h_{be}(n)] \in (0,1)^n$ denotes errors that the wireless channel causes to the random sequence $\mathbf{X}_b$ during demodulating $r_{be}(t)$; $\mathbf{N}_{ae} = [n_{ae}(1), n_{ae}(2), \ldots\ldots, n_{ae}(n)] \in (0,1)^n$ indicates errors that the noise causes to the random sequence $\mathbf{X}_a$ during demodulation; $\mathbf{N}_{be} = [n_{be}(1), n_{be}(2), \ldots\ldots, n_{be}(n)] \in (0,1)^n$ indicates errors that the noise causes to the random sequence $\mathbf{Y}_b$ during demodulation.

In practical wireless network environments, there are some scattering clusters like buildings, trees and other obstructions among Alice, Bob and Eve. So the transmission between Alice and Bob experiences different multi-path effects from that of Eve. In our proposed scheme, it is assumed that Eve is more than $\lambda/2$ away from Alice and Bob, she will experience independent channel variations, hence, $h_{ae}(t)$ and $h_{be}(t)$ are sufficiently uncorrelated with $h_{ab}(t)$ and $h_{ba}(t)$.

Also, since Eve has no knowledge of $\mathbf{X}_a$, $\mathbf{X}_b$, $h_{ab}(t)$ or



(a) f_d=10Hz (b) f_d=100Hz (c) f_d=0Hz

Fig. 4 Average bit error rate under different SNR.

$h_{ba}(t)$, she cannot use her received signals to generate the same secret key. Moreover, since $\mathbf{X}_a$ and $\mathbf{X}_b$ are independent random signals, our proposed scheme works well even in a static situation where the fluctuation of channel characteristics changes slowly.

4.1 The Bit Error Rate

If the channel reciprocity holds, that is $h_{ab} = h_{ba} = h$, the BER between $\mathbf{Y}_a$ and $\mathbf{Y}_b$ is

$$\begin{aligned} p_m &= P_r\{\mathbf{Y}_a \neq \mathbf{Y}_b\} \\ &= P_r\{\mathbf{X}_a \oplus \mathbf{X}_b \oplus \mathbf{H}_{ba} \oplus \mathbf{N}_a\} \\ &= P_r\{\mathbf{N}_a \neq \mathbf{N}_b\} \\ &= p_{N_a}(1 - p_{N_b}) + p_{N_b}(1 - p_{N_a}) \end{aligned} \tag{10}$$

where $p_{N_a} = p(n_a = 1)$ and $p_{N_b} = p(n_b = 1)$.

The BER between $\mathbf{Y}_e$ and $\mathbf{Y}_a$ is

$$\begin{aligned} p_w &= P_r\{\mathbf{Y}_e \neq \mathbf{Y}_a\} \\ &= P_r\{\mathbf{X}_a \oplus \mathbf{X}_b \oplus \mathbf{H}_{ae} \oplus \mathbf{H}_{be} \oplus \mathbf{N}_{ae} \oplus \mathbf{N}_{be} \\ &\quad \neq \mathbf{X}_a \oplus \mathbf{X}_b \oplus \mathbf{H}_{ba} \oplus \mathbf{N}_a\} \\ &= P_r\{\mathbf{H}_{ae} \oplus \mathbf{H}_{be} \oplus \mathbf{N}_{ae} \oplus \mathbf{N}_{be} \neq \mathbf{H}_{ba} \oplus \mathbf{N}_a\} \\ &= P_r\{\mathbf{H}_{ae} \oplus \mathbf{H}_{be} \oplus \mathbf{N}_{ae} \oplus \mathbf{N}_{be} \oplus \mathbf{H}_{ba} \oplus \mathbf{N}_a = 1\} \\ &= p_{w_4}(1 - p_5) + p_5(1 - p_{w_4}) \end{aligned} \tag{11}$$

Where $p_{w_i} = p_{w_{i-1}}(1 - p_i) + p_i(1 - p_{w_{i-1}})$, $i = 1, 2, 3, 4$, $p_{w_0} = p_0$. For clear expression, here we define that $p_{H_{ae}} = p(h_{ae} = 1) = p_5$, $p_{H_{be}} = p(h_{be} = 1) = p_4$, $p_{H_{ba}} = p(h_{ba} = 1) = p_3$, $p_{N_{ae}} = p(n_{ae} = 1) = p_2$, $p_{N_{be}} = p(n_{be} = 1) = p_1$ and $p_{n_a} = p(n_a = 1) = p_0$.

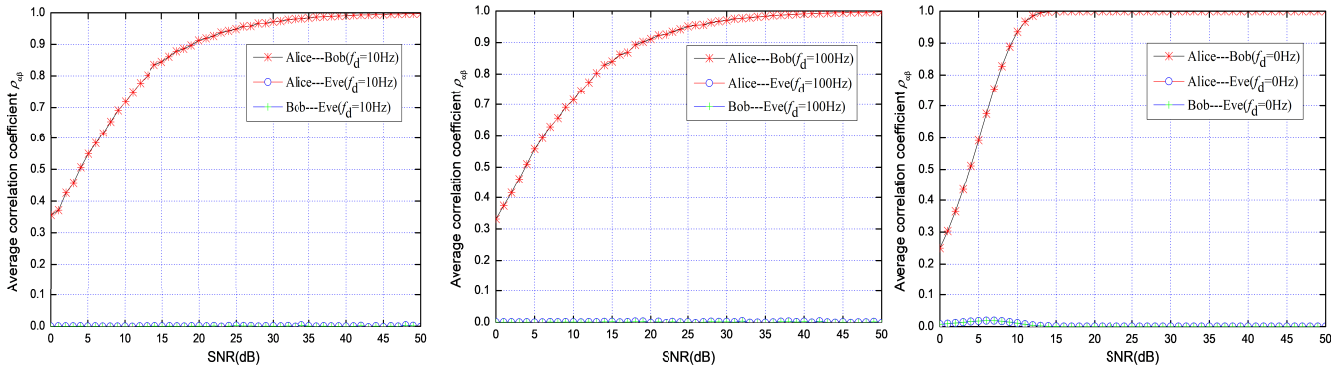
We simulate our proposed scheme for 10,000 times to estimate the average BER in both mobile (the maximum Doppler shift $f_d = 10Hz$ and $f_d = 100Hz$) and static ($f_d = 0Hz$) cases, and plot the results of average BER under different SNR in Fig. 4.

From the simulation results, it can be seen that our proposed scheme has low BER level in both static and mobile cases. For example, the average BER between $\mathbf{Y}_a$ and $\mathbf{Y}_b$ is 0.05157 when SNR=20dB and $f_d = 10Hz$, and those error bits can be easily removed through information reconciliation and a shared key can be obtained easily. Moreover, our proposed scheme can achieve a very low BER (lower than 0.00475) for a SNR higher than 40dB. Such a high SNR can be practically obtained by a recommended higher power transmission for the purpose of key generation. While the average BER between $\mathbf{Y}_a$ and $\mathbf{Y}_e$ (or between $\mathbf{Y}_b$ and $\mathbf{Y}_e$) is around 0.5, which is no better than random guess, i.e, Eve cannot obtain the secret key. Hence, our proposed scheme is efficient and secure.

4.2 Secret Bit Generation Rate

Compared to previous RSS-based schemes, our proposed scheme achieves a much higher secret key generation rate due to two major reasons: First, RSS-based methods can only get one RSS measurement from each frame/packet which limits the key generation rate. Also, not every measurement can be used to generate a key. For example, when the packet rate $f_s = 100$ packet/s and the Droppler frequency shift $f_d = 10Hz$, only one sample out of five packets at each user can be used to generate a key. Moreover, in some quantization methods, only RSS measurements above or below the threshold can be used [2], [10], all the other measurements will be discarded which will cause a large loss of bits since only one secret bit can be generated from m successive RSS measurements. Different from those exiting schemes, our proposed scheme processes the binary sequence, and no quantization is needed and thus no bit is lost. Second, for the existing RSS-based schemes, the bit generation rate cannot exceed Doppler frequency shift f_d too much [2]. However, in our proposed scheme, random sequences $\mathbf{X}_a$ and $\mathbf{X}_b$ can cause good randomness in the process of key generation, and our proposed scheme can run multiple rounds in a given coherence time to achieve a higher secret bit generate rate.

We simulate our proposed scheme under the IEEE 812.15.4 wireless network with the rate 250kbps. In our simulation, when the Droppler frequency shift $f_d = 10Hz$, each packet contains a total of 20 bytes random sequence and thus has a duration of 80μs. Processing time dominates the whole key generation process, and the random sequence is transmitted at a rate of approximately 100 packet/s, or 50 packet/user. The secret bit generation rate of our proposed scheme can achieve 8000 bit/s approximately.



(a) f_d=10Hz (b) f_d=100Hz (c) f_d=0Hz

Fig. 5 Signal correlation under different SNR.

4.3 Flexibility and Practicability

Compared to previous schemes, our proposed key generation scheme can be applied in both mobile and static environments. In previous schemes, in order to generate key bits with high average entropy, extracting bits from different "coherence time periods" is needed, which is usually realized through node mobility. However, in our proposed scheme, we do not have this constraint. Even in a static environment, the random user sequences $\mathbf{X}_a$ and $\mathbf{X}_b$ chosen in each round can cause good randomness effectively in the process of key bit generation, i.e., our proposed scheme is not constrained by the coherence time, and it can work well even in the static environment.

Moreover, our proposed scheme simplifies the multiplication operations to XOR, which is easy to implement and enables lightweight security in 5G IoT scenarios. Our proposed scheme neither requires special hardware nor any helper to inject noise into the system, and it can be applied to all existing communication system without alteration. Also it does not require complicated computation, and is especially suitable for 5G wireless networks with resource-constrained devices. Hence, our proposed scheme is energy efficient and practical.

4.4 Security Evaluation

To achieve a quantitive measure for the grade of reciprocity, we define $\rho_{\alpha\beta}$ as the correlation coefficient between $\mathbf{Y}_\alpha$ and $\mathbf{Y}_\beta$, respectively, with $\alpha, \beta \in \{a, b, e\}$, and $\alpha \neq \beta$, which is given as

$$\rho_{\alpha\beta} = \frac{E\{\mathbf{Y}_\alpha \mathbf{Y}_\beta\} - E\{\mathbf{Y}_\alpha\}E\{\mathbf{Y}_\beta\}}{\sigma_\alpha \sigma_\beta} \tag{12}$$

Figure 5 shows the correlation between the measurements of Alice and Bob, Alice and Eve and Bob and Eve. From Fig. 5, we can see that the reciprocity between Alice's and Bob's primitive key sequences is greatly high in terms of correlation coefficient $\rho_{\alpha\beta}$, (above 0.9 on average with SNR = 20) while the reciprocity between Alice's and Eve's sequences or Bob's and Eve's sequences is almost 0. Hence, our proposed scheme achieves good randomness and good secure results.

4.5 Active Attack Resistance

The major advantage of our proposed scheme is that it can resist the active attack introduced in Sect. 2. For instance, if an adversary inserts a large object between the Alice-Bob channel which blocks a large number of reflection or refraction signals, all RSS values observed by Alice and Bob may become very small from then on. All previous methods will extract all-0 bit sequence from the channel. While, in our proposed scheme, this can only cause some similar bit errors to Alice's and Bob's demodulated sequences, Alice and Bob still can obtain common secret sequences. Moreover, since $\mathbf{X}_a$ and $\mathbf{X}_b$ are independent random sequences, Eve has no knowledge of them and cannot identify the impact of her action on Alice's and Bob's sequences, and thus she cannot deduce information about the secret key. Comparing to previous works, our proposed scheme generates stronger secret key in a shorter time period.

5. Conclusions

Using wireless channel characteristics to establish a shared secret key is becoming a proliferate area for its high reliability, easy implementation, and low energy consumption. In this paper, we focus on the issues of ensuring the high key generation rate and correlation of the secret key under active attack, and propose a new practical secret key generation scheme with high rate key generation and correlation. In our proposed scheme, instead of transmitting known training sequences or probing signals, Alice and Bob transmit independent secret random sequences. User's random sequences together with the channel effects are used as common random source to generate the secret key, which guarantees that legitimate users are able to share secret keys with sufficient length and high security under active attack. We evaluate the proposed scheme through both analytic and simulation studies. The results show that our proposed scheme achieves

high key generation rate and key security. Also, our proposed scheme is energy efficient and practical, and it neither requires special hardware or any helper to inject noise into the system, which make it more suitable for resource-constrained devices in 5G wireless networks.

Acknowledgments

This work was partially supported by Zhejiang Province Natural Science Foundation (No. LY19F020039, No. LY18F020017), National Natural Science Foundation of China (No. 61401128, No. 61872120).

References

[1] A. Mazin, K. Davaslioglu, and R.D. Gitlin, "Secure key management for 5G physical layer security," in proc. of IEEE 18th Wireless & Microwave Technology Conference, pp.1–5, 2017.

[2] 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, 2008.

[3] Y.E.H. Shehadeh, O. Alfandi, K. Tout, and D. Hogrefe, "Intelligent mechanisms for key generation from multipath wireless channels," in proc. of IEEE Wireless Telecommunications Symposium (WTS), pp.1–6, 2011.

[4] 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, 2011.

[5] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," IEEE J. Sel. Areas Commun., vol.30, no.9, pp.1666–1674, Sept. 2012.

[6] F. Marino, E. Paolini, and M. Chiani, "Secret key extraction from a UWB channel: analysis in a real environment," in proc. of IEEE International Conference on Ultra-WideBand (ICUWB), pp.80–85, 2014.

[7] M.G. Madiseh, S. He, M.L. Mcguire, S.W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in Proc. of IEEE International Conference on Communications (ICC), pp.1–5, 2009.

[8] 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, 2009.

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

[10] 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, 2009.

[11] 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 Trans. Mobile Comput., vol.12, no.5, pp.917–930, May 2013.

[12] 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), Boston, MA, USA, pp.1–5, 2015.

[13] 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), Orlando, FL, USA, pp.927–935, 2012.

[14] H. Liu, Y. Jie, W. Yan, Y.J. Chen, and C.E. Koksal, "Group secret key generation via received signal strength: Protocols, achievable rates, and implementation," IEEE Trans. Mobile Comput., vol.13, no.12, pp.2820–2835, 2014.

[15] Q. Dai, J. Liang, and K. Huang, "Adaptive key generation based on quantization of channel characteristics" in proc. of IEEE International Conference on Information Science and Technology (ICIST), pp.1512–1517, 2013.

[16] 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, 2012.

[17] R. Guillaume, S. Ludwig, A. Muller, and A. Czylwik, "Secret key generation from static channels with untrusted relays," in proc. of IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp.635–642, 2015.

[18] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in Proc. of IEEE International Conference on Computer Communications (INFOCOM), pp.3048–3056, 2013.

[19] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in Proc. of IEEE International Conference on Computer Communications (INFOCOM), pp.1–9, 2010.

[20] C. 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), Coimbra, Portugal, pp.267–272, 2015.

[21] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. "Experimental quantum cryptography," Journal of cryptology, vol.5, no.1, pp.3–28, 1992.

[22] T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol "Cascade"," IEICE Trans. Fundamentals, vol.83, no.10, pp.1987–1991, Oct. 2000.

[23] W.T. Buttler, S.K. Lamoreaux, J.R. Torgerson, G.H. Nickel, C.H. Donahue, and C.G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," Physical Review A, vol.67, no.5, pp.125–128, May 2003.

[24] 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.

[25] 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.

[26] C.H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory, vol.41, no.6, pp.1915–1923, June 1995.

[27] J.E. Hershey, A.A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," IEEE Trans. Commun., vol.43, no.1. pp.3–6, 1995.

[28] 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.

[29] J. Zhang, A. Marshall, R. Woods, and T.Q. Duong, "Secure key generation from OFDM subcarriers' channel responses," in proc. of IEEE Globecom Workshops, pp.1302–1307, 2014.

[30] J. Zhang, R. Woods, A. Marshall, and T.Q. Duong, "Verification of Key Generation from Individual OFDM Subcarrier's Channel Response," in proc. of IEEE Globecom Workshops, pp.1–6, 2016.

[31] A. Kitaura, H. Iwai, and H. Sasaoka, "A scheme of secret key agreement based on received signal strength variation by antenna switching in land mobile radio," in proc. of the 9th International Con-

ference on Advanced Communication Technology, pp.1763–1767, 2007.
[32] M. Wilhelm, I. Martinovic, and J.B. Schmitt, "Secure key generation in sensor networks based on frequency-selective channels," IEEE J. Sel. Areas Commun., vol.31, no.9, pp.1779–1790, 2013.
[33] P. Huang and X. Wang, "Fast secret key generation in static wireless networks: A virtual channel approach," in Proc. of 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM), Turin, Italy, pp.2292–2300, April 2013.
[34] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-layer secret key agreement in two-way wireless relaying systems," IEEE Trans. Inf. Forensics Security, vol.6, no.3, pp.650–660, 2011.
[35] L. Lai, Y. Liang, and W. Du, "Cooperative key generation in wireless networks," IEEE J. Sel. Areas Commun., vol.30, no.8, pp.1578–1588, 2012.
[36] S. Yasukawa, H. Iwai, and H. Sasaoka, "A secret key agreement scheme with multi-level quantization and parity check using fluctuation of radio channel property," in IEEE International Symposium on Information Theory, pp.732–736, 2008.
[37] U.M. Maurer, "Secret key agreement by public discussion from common information," IEEE Trans. Inf. Theory, vol.39, no.3, pp.733–742, 1993.
[38] M.G. Madiseh, S.W. Neville, and M.L. McGuire, "Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation," IEEE Trans. Inf. Forensics Security, vol.7, no.4, pp.1278–1287, 2012.
[39] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in Proc. of 30th IEEE Int. Conf. Comput. Commun. (INFOCOM), Shanghai, China, pp.1125–1133, April 2011.
[40] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, "Smokegrenade: An efficient key generation protocol with artificial interference," IEEE Trans. Inf. Forensics Security, vol.8, no.11, pp.1731–1745, 2013.
[41] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," IEEE Commun. Mag., vol.53, no.6, pp.33–39, 2015.
[42] A. Khisti, "Secret-Key Agreement Over Non-Coherent Block-Fading Channels With Public Discussion," IEEE Trans. Inf. Theory, vol.62, no.12, pp.7164–7178, 2016.
[43] S. Zhang, L. Jin, Y. Lou, and Z. Zhong, "Secret key generation based on two-way randomness for TDD-SISO system," China Communications, vol.15, no.7, pp.202–216, 2018.

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 network security, security issues in wireless networks, key management and physical layer security, etc.

Mingyang Kang was born in Xiaoxian, Anhui Province, China in 1994. He received his B.S. degree in Metal Material Engineering from North University of China, Taiyuan, China, in 2017. He is currently pursuing the master degree in the School of Cyberspace, Hangzhou Dianzi University. His research interests include network security, physical layer security, information security, etc.

Guohua Wu received the B.S. degree from Shandong University of Technology, Jinan, China, in 1992, the M.S. degree from National Institute of Metrology, Beijing, China, in 1995, and the Ph.D. degree from Zhejiang University, Hangzhou, China, in 1998, where he was a Lecturer with the Department of Biomedical Engineering, from 1998 to 2000, and became an Associate Professor, in 2001. Since 2002, he has been with the Department of Computer Science and Engineering, Hangzhou Dianzi University, and was appointed as a Professor, in 2009. He is currently a Professor with the School of Cyberspace, Hangzhou Dianzi University, Hangzhou, Zhejiang, China. He is also an Executive Director of the Information Security Laboratory. His current research interests include information system, model driven architecture, data mining, and digital heath.

Yizhi Ren received his PhD in Computer software and theory from Dalian University of Technology, China in 2011. From 2008 to 2010, he was a research fellow at Kyushu University, Japan. He is currently an associate professor with School of Cyberspace, Hangzhou Dianzi University, China. His current research interests include: network security, complex network, and trust management. Dr. REN has published over 60 research papers in refereed journals and conferences. He won IEEE Trustcom2018 Best Paper Award, CSS2009 Student Paper Award and AINA2011 Best Student paper Award.

Chunhua Su received his PhD of computer science from Faculty of Engineering, Kyushu University, Japan in 2009. He is currently working as Senior Associate Professor in Division of Computer Science, University of Aizu. He has worked as a research scientist in Cryptography & Security Department of the Institute for Infocomm Research, Singapore from 2011–2013. From 2013–2016, he has worked as an Assistant professor in School ofInformation Science, Japan Advanced Institute of Science and Technology. From 2016–2017, he worked as Assistant Professor in Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in data mining and IoT security & privacy.