Encrypting Wireless Communications On the Fly Using One-Time Pad and Key Generation

Guyue Li, *Member, IEEE*, Zheying Zhang, Junqing Zhang and Aiqun Hu, *Member, IEEE*

***Abstract*—The one time pad (OTP) secure transmission relies on the random keys to achieve perfect secrecy, while the unpredictable wireless channel is shown to be a good random source. There is very few work of the joint design of OTP and key generation from wireless channels. This paper provides a comprehensive and quantitative investigation on secure transmission achieved by OTP and wireless channel randomness. We propose two OTP secure transmission schemes, i.e., Identical Key-based Physical-layer Secure Transmission (IK-PST) and Un-identical Key-based Physical-layer Secure Transmission (UK-PST). We quantitatively analyze the performance of both schemes and prove that UK-PST outperforms IK-PST. We extend the pairwise schemes to a group of users in networks with star and chain topologies. We implement prototypes of both schemes and evaluate the proposed schemes through both simulations and experiments. The results verify that UK-PST has a higher effective secret transmission rate than that of IK-PST for scenarios with both pairwise and group users.**

***Index Terms*—One time pad; secret key generation; physical-layer security; information reconciliation; group key distribution.**

I. Introduction

Information security has become the subject of scrutiny after a number of notorious cyberattacks [1], [2]. Actually, it has been taken into account as early as the communications technologies were born. Venman proposed one time pad (OTP) in 1919, which encrypts each message bit with a different key bit via exclusive OR (XOR) [3]. In 1949, Shannon mathematically proved that OTP can achieve information-theoretically security [4], i.e., perfect secrecy can be obtained even against adversaries with infinite computational power. While OTP is able to provide perfect secrecy, its application is rather limited probably because the secure and efficient provision of keys for OTP is challenging. The OTP secure transmission system requires one-time pre-shared random key which has at least the same length as the plaintext message being sent. Therefore, the realization of the OTP relies on the provision of secure keys.

Our communication and computer networks are currently protected by modern cryptography including public key cryptography and symmetric encryption [5]. Even though they are very mature, there are some concerns when quantum computer becomes available in the future. Public key cryptography relies on complicated mathematical problems such as discrete logarithm that is not scalable, which may be cracked by the quantum computer [6]. Therefore, this paper will revisit OTP which should be secure against quantum computer.

In 1993, Ahlswede *et al.* and Maurer published their seminal work of secret key agreement from common randomness [7], [8], which is an ideal candidate for generating symmetric keys for OTP. Their pioneer work has triggered extensive investigation to exploit the randomness residing in the reciprocal wireless channel [9], [10]. Various practical key generation approaches have been proposed and verified on platforms with a variety of wireless techniques, e.g., ZigBee [11], WiFi [12], [13] and LoRa [14], [15]. In practice, key generation is subject to impairments of channel measurements due to time delay in TDD systems, hardware imperfection and noise [16]. Even when various preprocessing approaches are adopted to improve the similarity between channel characteristics [16] and quantization algorithms are improved to reduce the disagreements between quantized bit sequences, they cannot guarantee to produce the same key. Hence, key generation protocol requires information reconciliation to negotiate an identical key, which requires parity information exchanged over the public channel and error correction. The generated key can be used in any scenarios where common information is required. For example, it can be used as a seed of a stream cipher for bootstrapping many higher-layer security mechanisms [10].

Key generation usually works between a pair of legitimate users, and it is later extended to a group of users with star, ring and mesh topologies [17]–[21]. This is applicable to scenarios where some confidential information needs to be shared among group users. For instance, control centres need to send confidential instructions to a group of soldiers in military operations [20].

While most of existing work investigates the key generation protocols in a given environment, very few of them focus on the joint design of key generation and OTP. A straightforward way will be cascading key generation and OTP, which is termed as Identical Key-based Physical-layer Secure Transmission (IK-PST). Two connecting wireless users firstly derive a pair of identical secret key from their channel observations, and then add each bit of the plaintext to one bit

This work was supported in part by the National Natural Science Foundation of China under Grant 61801115 and 61941115, in part by the Zhishan Youth Scholar Program of SEU, the Research Fund of National Mobile Communications Research Laboratory, Southeast University (No.2019B01) and the Fundamental Research Funds for the Central Universities (3204009415, 3209019405), in part by the Campus France PHC Cai Yuanpei 2019 project under Grant 44016XA, in part by the China Scholarship Council, and in part by the Purple Mountain Laboratory Network and Communication Security. (Corresponding author: G. Li)

G. Li and Z. Zhang are with the School of Cyber Science and Engineering, Southeast University, Nanjing, China. (e-mail: guyuelee@seu.edu.cn.)

A. Hu is with the School of Information Science and Engineering, Southeast University, Nanjing, 210096, China. (e-mail: aqhu@seu.edu.cn.)

G. Li and A. Hu are also with the Purple Mountain Laboratories for Network and Communication Security, Nanjing, 210096, China.

J. Zhang is with the Department of Electrical Engineering and Electronics, University of Liverpool, Liverpool, L69 3GJ, United Kingdom. (email: junqing.zhang@liverpool.ac.uk.)

from the OTP key using modulo-addition. Producing identical key requires sophisticated information reconciliation and this becomes more severe for group users. For example, in the work of Xu *et al.* [20], each node pair in the group need to first generate a nearly uniformly distributed pairwise key with arbitrarily small error probability. For a ring network with four users, it needs four times of the information reconciliation. Liu *et al.* used some information broadcast, joint with the observation phase in such a way that the subsequent one-way public discussion involves merely a single broadcast for information reconciliation, hence reducing the delay at the expense of some sacrifice in the key rate [18].

We further think if it is feasible to use the non-reconciled key for OTP, termed as Un-identical Key-based Physical-layer Secure Transmission (UK-PST). The challenge is to decrypt the confidential message correctly when the OTP keys of two parties are different but highly correlated. We deem the XOR encryption and decryption modules along with the physical channel as an equivalent cascade channel. Then, the tiny differences between keys can be seen as part of the transmission error, and thus can be corrected by the off-the-shelf channel coding with a stronger correction capability.

There have been some preliminary explorations on OTP with un-identical keys. Zheng *et al.* designed a modified OTP using keys generated from electrocardiogram signals for implantable medical devices [22]. There are also efforts from the wireless community. Peng *et al.* reused the error correction capability of Polar codes for the key agreement [23]. It designed an integrated wireless secret key based transmission scheme to securing pairwise M2M transmissions, and is shown to be simpler than the conventional counterpart by avoiding information reconciliation. Subsequently, the work of [24] extended the UK-PST scheme to the scenarios with four-node wireless networks to generate a shared group key.

This joint design can be applied in scenarios requiring low data rate but high security demands, as an OTP system can provide incomparable strong security but may be limited in secure transmission rate. For example, it is necessary to share the secret spreading/hopping code in spread-spectrum modulation such as CDMA or fast-frequency hopping [25]. Another potential application is to use the OTP to help distribute the quantum key from the fixed quantum endpoint to the mobile endpoints. The implementation of OTP in radio communication can protect them from disruption attacks.

Although both IK-PST and UK-PST schemes have the potential to realize the OTP secure transmission, neither of them has been well investigated yet. IK-PST is easy to understand, but its practical usage may be compromised by additional transmissions and information leakage. On the other hand, UK-PST abandons the information reconciliation and privacy amplification, but it works at the expense of a stronger correction capability of the channel coding. Besides, it needs extra keys to encrypt the syndrome of the confidential data. This paper aims to provide a comprehensive and quantitative investigation on secure transmission achieved by OTP and wireless channel randomness. The main contributions of this paper are listed as follows.

- We propose two schemes to realize OTP secure transmissions using the common randomness from wireless channels. We found that IK-PST deploys an additional identical key generation flow while UK-PST simplifies the secure transmission processes.
- We analyze the performance quantitatively and derive the closed-form expressions of three metrics, namely communication overhead, computation complexity and secure transmission rate. We prove that UK-PST outperforms IK-PST in terms of these metrics.
- We extend the OTP scheme to a group of users in networks with star and chain topologies, respectively. UK-PST does not need to produce identical pairwise keys, and thus avoids multiple sophisticated information reconciliation and privacy amplification. Therefore, system complexity and communication overhead are significantly reduced.
- We implement prototypes of the OTP system with wireless motes and evaluate the proposed schemes through both simulation and experiments. For both pairwise and group users, UK-PST is verified to achieve higher effective secret transmission rate than that of IK-PST and the gap expands with the increase of the disagreement ratio of channel quantization results. The results coincide with the theoretical analysis.

The rest of the paper is organized as follows. In Section II, we present a detailed system model and attack model. Section III proposes two OTP secure transmission protocols named IK-PST and UK-PST for a pair of users. We compare the performance of the two proposed protocols from the perspective of communication overhead, computation complexity and secure transmission rate in Section IV. Next, we extend the protocols to group communication networks with star and chain topologies in Section V. We present the simulation results and experimental results in Section VI and Section VII concludes the paper.

Notation and Outline

Unless otherwise specified, we use the following notations throughout the manuscript: Upper (lower) bold-face letters denote matrices (column vectors); $\mathbf{I}$ denotes the identity matrix. Numeral subscripts of matrices and vectors, if needed, represent their sizes. Also, matrix superscripts $(\cdot)^H, (\cdot)^T, (\cdot)^*$ denote their conjugate-transpose, transpose, and conjugate, respectively. We use $E\{\cdot\}$ to denote ensemble expectation and $|\cdot|$ to represent matrix determinant operations.

II. System Overview

A. System Model

This paper investigated secure transmission achieved by OTP and key generation. Specifically, a user i intends to transmit the confidential information to a user j without been known by a third party. OTP encrypts the plaintext with a random key at the transmitter via XOR operation, which can achieve perfect secrecy. The receiver decrypts the message by XORing the ciphertext with its key. The keys are the same at transmitter and receiver, which is termed as IK-PST.

The key distribution for the OTP is challenging. This paper will employ physical layer key generation from wireless channels [9]. Key generation is composed of four stages, namely channel probing, quantization, information reconciliation and privacy amplification. User i and user j will carry out bidirectional channel probing between each other, and they can collect channel measurements, $Y_{j,i}(t)$ and $Y_{i,j}(t)$, respectively, such as received signal strength (RSS) and channel state information (CSI). User i and user j collect N_T measurements with a time interval of ΔT, user i will get $\mathbf{y}_{j,i} = [Y_{j,i}(1), Y_{j,i}(2), \cdots, Y_{j,i}(N_T)]^T$ and user j will get $\mathbf{y}_{i,j} = [Y_{i,j}(1), Y_{i,j}(2), \cdots, Y_{i,j}(N_T)]^T$.

They will then perform quantization individually. For example, the mean value-based quantizer can be given as

$$Q(t_k) = \mathcal{Q}(Y(t_k)) = \begin{cases} 1, Y(t_k) \geq \theta \\ 0, Y(t_k) < \theta \end{cases}, \tag{1}$$

where θ is the mean value of $Y(t)$. Denote $\mathbf{q}_{j,i} = [Q_{j,i}(1), Q_{j,i}(2), \cdots, Q_{j,i}(N_T)]^T$ as the quantized result of user i. Similarly, $\mathbf{q}_{i,j} = \mathcal{Q}(\mathbf{y}_{i,j})$ is the quantization results of user j. The time to produce $\mathbf{q}_{j,i}$ and $\mathbf{q}_{i,j}$ with length $L_{\mathbf{q}}$ is $T = 2L_{\mathbf{q}}\Delta T$.

It is worth noting that the channel measurements should be independent, to guarantee the key randomness. In literature, various methods have been investigated to reduce the correlation among channel measurements. For example, the time interval of ΔT is set to exceed the channel coherent time, so that the adjacent channel measurements are not correlated [16]. Besides, some down-sampling and correlation reduction transforms can also be introduced to preprocess the channel measurements. Previous experiments have verified that quantization results can pass the random test, with an appropriate sampling interval or well-designed preprocessing [13], [26]. Therefore, we assume that there is no autocorrelation within the generated key bits, i.e., $\mathbf{q}_{j,i}$ ($\mathbf{q}_{i,j}$). More work related to the randomness of key generation can be found in [13], [26].

The channel measurements $Y_{i,j}(t)$ and $Y_{j,t}(t)$ are affected by the non-simultaneous sampling and noise. This issue results in un-identical keys, i.e., $\mathbf{q}_{i,j}$ and $\mathbf{q}_{j,i}$ are not the same. The disagreement ratio is defined as

$$\epsilon_{\mathbf{q}} = \frac{1}{L_{\mathbf{q}}} \left\| \mathbf{q}_{i,j} - \mathbf{q}_{j,i} \right\|_1, \tag{2}$$

where $\|\cdot\|_1$ denotes the 1-norm operator. Information reconciliation is thus used to correct the mismatches, e.g., realized by employing the error correction code (ECC) [27]. Finally, privacy amplification is adopted to eliminate any information leakage during the previous steps.

While it is intuitive to use the same key for encryption and decryption, OTP with un-identical keys at transmitter and receiver has not been explored. This is inspired by the fact that channel coding is employed to correct transmission errors and the key disagreement can be treated together with the transmission errors. When keys at the transmitter and receiver are not the same, the receiver may still be able to correctly decrypt and decode the message, termed as UK-PST. This paper will carefully examine both IK-PST and UK-PST.

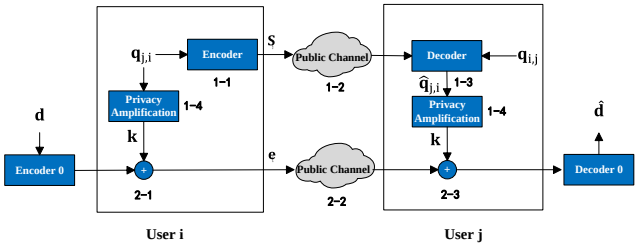

Fig. 1. Secure transmission using identical pairwise keys.

B. Attack Model

Following the assumptions in most key generation schemes [16], [28], [29], we also focus on the passive adversary. Besides, we assume the group users are all trusted, and user compromise and man-in-the-middle attacks are not considered. The eavesdropper, Eve, is assumed to be located at least half a wavelength away from legitimate users. Since wireless channel gains decorrelate over half a wavelength in multipath environments, Eve's channel is independent from that of legitimate users. Therefore, Eve cannot deduce the measurements of legitimate users merely based on her observation. However, Eve overhears all the public discussion and knows all the protocols.

III. OTP Secure Transmission for Pairwise Users

A. IK-PST Protocol

Users i and j firstly generate a string of identical secret key $\mathbf{k}$ and then use it for encrypting and decrypting the confidential message $\mathbf{d}$. Fig. 1 illustrates the protocol for secure transmission using reconciled pairwise keys, where $\mathbf{q}_{j,i}$ and $\mathbf{q}_{j,i}$ are the quantized results of channel measurements which are generated according to Section II-A.

The protocol is composed of two stages, namely identical key generation (from 1-1 to 1-4) and secure transmission (2-1, 2-2). In particular, key generation can be completed as follows.

1-1. User i generates a syndrome $\mathbf{s}$ of $\mathbf{q}_{j,i}$ by an encoder as

$$\mathbf{s} = \mathcal{E}(\mathbf{q}_{j,i}), \tag{3}$$

where $\mathcal{E}(\cdot)$ represents the generation function of a $(\mathcal{C}, n, k, t)$ ECC, e.g., BCH.

1-2. Syndrome $\mathbf{s}$ is transmitted to user j over a noiseless public channel, where error-free transmission can be realized by channel coding. For simplicity, we do not represent the channel coding process explicitly.

1-3. According to $\mathbf{s}$ and $\mathbf{q}_{i,j}$, user j recovers $\hat{\mathbf{q}}_{j,i}$ by

$$\hat{\mathbf{q}}_{j,i} = \mathcal{D}(\mathbf{q}_{i,j}, \mathbf{s}), \tag{4}$$

where $\mathcal{D}(\cdot)$ represents the decoding function of the ECC $(\mathcal{C}, n, k, t)$. $\hat{\mathbf{q}}_{j,i} = \mathbf{q}_{j,i}$ holds when the disagreement ratio $\epsilon_{\mathbf{q}}$ is within the capability of $(\mathcal{C}, n, k, t)$.

1-4. User i and j perform privacy amplification by feeding the generated keys into a hash function $\mathcal{H}(\cdot)$ as

$$\mathbf{k} = \mathcal{H}(\mathbf{q}). \tag{5}$$

Its length $L_{\mathbf{k}} = L_{\mathbf{q}} - L_{\mathbf{s}}$, where $L_{\mathbf{s}}$ is the length of $\mathbf{s}$.

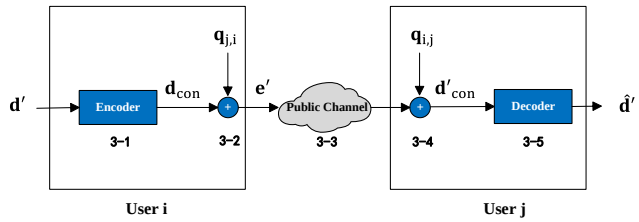

Fig. 2. Secure transmission scheme using un-identical keys.

Steps 1-1, 1-2 and 1-3 are for information reconciliation. Eve can deduce part of $\mathbf{q}_{j,i}$ by accessing $\mathbf{s}$, $\mathcal{E}(\cdot)$ and $\mathcal{D}(\cdot)$.

The rest of the steps are designed for secure transmission. User i intends to transmit confidential message $\mathbf{d}$ to user j over a public channel securely. Channel coding is used to guarantee transmission reliability, which is illustrated by the Encoder 0 and Decoder 0 modules as shown in Fig.1.

2-1. The OTP theory uses XOR operation for encrypting the data, which can be given as

$$\mathbf{e} = \mathbf{d} \oplus \mathbf{k}, \tag{6}$$

where $\oplus$ represents the bitwise XOR operator. The length of the data $\mathbf{d}$ is the same as the length of $\mathbf{k}$, i.e.,

$$L_{\mathbf{d}} = L_{\mathbf{k}}. \tag{7}$$

2-2 User i transmits the ciphertext $\mathbf{e}$ to user j over a public channel.

2-3 User j decrypts the message $\mathbf{d}$ with his key by

$$\hat{\mathbf{d}} = \mathbf{e} \oplus \mathbf{k} = \mathbf{d}. \tag{8}$$

The secure transmission is achieved.

As shown above, IK-PST scheme has a relatively complex structure to realize OTP secure transmission as it deploys an additional identical key generation flow.

B. UK-PST Protocol

Fig. 2 illustrates secure transmission using a pair of un-identical keys, which contains five steps. We also assume $\mathbf{q}_{j,i}$ and $\mathbf{q}_{i,j}$ as the quantization results of the channel measurements of user i and j and their lengths are both $L_{\mathbf{q}}$.

3-1. Private message $\mathbf{d}'$ with a length of $L_{\mathbf{d}'}$ is first fed into the channel encoder of user i and the output syndrome is

$$\mathbf{s}' = \mathcal{E}'(\mathbf{d}'), \tag{9}$$

where $\mathcal{E}'(\cdot)$ represents the generation function of a $(\mathcal{C}', n', k', t')$ ECC.

3-2. The confidential message $\mathbf{d}'$ and syndrome $\mathbf{s}'$ are concatenated as

$$\mathbf{d}_{con} = [\mathbf{d}', \mathbf{s}'], \tag{10}$$

and encrypted using the key $\mathbf{q}_{j,i}$ into the the ciphertext $\mathbf{e}'$. The bits-stream encryption is realized by

$$\mathbf{e}' = \mathbf{d}_{con} \oplus \mathbf{q}_{j,i} = [\mathbf{d}' \oplus \mathbf{q}_{j,i}^{L}, \mathbf{s}' \oplus \mathbf{q}_{j,i}^{R}], \tag{11}$$

where $\mathbf{q}_{j,i}^{L}$ is the left $L_{\mathbf{d}'}$-bit part and $\mathbf{q}_{j,i}^{R}$ is the right $L_{\mathbf{s}'}$-bit part of $\mathbf{q}_{j,i}$. Therefore, the lengths satisfy that

$$L_{\mathbf{q}} = L_{\mathbf{d}'} + L_{\mathbf{s}'}. \tag{12}$$

3-3. The ciphertext $\mathbf{e}'$ is transmitted to user j over a public channel.

3-4. Although user j does not have the identical bit sequence for decryption, he has $\mathbf{q}_{i,j}$ which has a high similarity with $\mathbf{q}_{j,i}$. User j decrypts $\mathbf{e}'$ with $\mathbf{q}_{i,j}$ by

$$\mathbf{d}'_{con} = \mathbf{e}' \oplus \mathbf{q}_{i,j} = \mathbf{d}_{con} \oplus \Delta = [\mathbf{d}' \oplus \Delta_L, \mathbf{s}' \oplus \Delta_R], \tag{13}$$

where $\Delta = \mathbf{q}_{i,j} \oplus \mathbf{q}_{j,i}$ illustrates the difference between $\mathbf{q}_{i,j}$ and $\mathbf{q}_{j,i}$. When a bit mismatch occurs, the XOR result becomes '1' in the corresponding position of Δ.

3-5. The user j recovers the confidential message $\mathbf{d}'$ by

$$\hat{\mathbf{d}}' = \mathcal{D}'(\mathbf{d}'_{con}) = \mathbf{d}', \tag{14}$$

where $\mathcal{D}'$ is the decoding function of the ECC $(\mathcal{C}', n', k', t')$. Note that, in the practical implementation, the interleaver and de-interleaver can be exploited to reduce the impact of burst errors. The elements in $\mathbf{d}'_{con}$ are firstly permuted via an interleaver before the ECC decoding, and after the ECC decoding, the elements in $\hat{\mathbf{d}}'$ are also permuted to the original order via a de-interleaver.

As shown above, UK-PST scheme has a relatively simple structure to realize OTP secure transmission as it does not need an additional identical key generation flow.

IV. Performance Analysis of IK-PST and UK-PST

In this section, we present a contrastive analysis of both schemes in terms of communication overhead, computation complexity and secure transmission efficiency.

A. Communication Overhead

Firstly, we consider the communication overhead caused by the information transmissions from user i to user j. IK-PST needs two times of the information transmission (step 1-2 and step 2-2) while UK-PST only needs one information transmission (step 3-3). Following the previous work of [27], we measure the communication overhead by the interaction delay T_{delay}. The delays for both schemes are calculated as

$$\begin{aligned} T_{delay}^{IK} &= (\frac{L_{\mathbf{s}} + L_0}{B} + \frac{dist}{c}) + (\frac{L_{\mathbf{d}} + L_0}{B} + \frac{dist}{c}) \\ &= \frac{L_{\mathbf{q}}}{B} + 2(T_0 + \frac{dist}{c}), \end{aligned} \tag{15}$$

and

$$T_{delay}^{UK} = \frac{L_{\mathbf{q}} + L_0}{B} + \frac{dist}{c} = \frac{L_{\mathbf{q}}}{B} + T_0 + \frac{dist}{c}, \tag{16}$$

respectively, where B is the system bandwidth, $dist$ is the transmission distance, c is the velocity of light, L_0 is the indispensable overhead in a frame, e.g., the synchronization header, PHY header and frame payload and $T_0 = L_0/B$ is the time cost by transmitting these bits. As observed from (15) and (16),

$$T_{delay}^{UK} < T_{delay}^{IK}. \tag{17}$$

Fig. 3 plots the delays of both schemes as a function of L_q in a typical ZigBee scenario. The transmission range of ZigBee

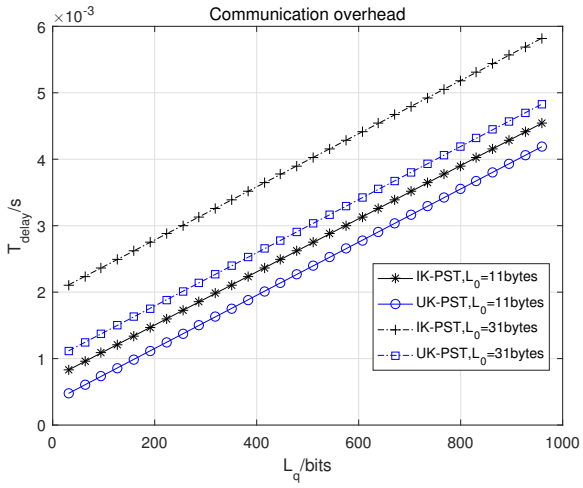

Fig. 3. The communication delays of IK-PST and UK-PST as a function of the frame overhead L_0. The bandwidth $B = 1$ MHz and $dist = 100$ meters.

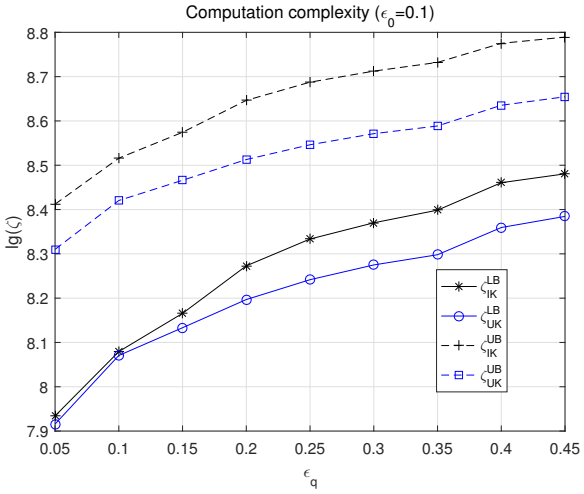

Fig. 4. The upper and lower bounds of the decoder complexity of the UK-PST and IK-PST schemes. The error probability of the channel is $\epsilon_0 = 0.1$.

is usually below 100 meters, therefore we set the distance $dist = 100$; the bandwidth $B = 1$ MHz. The propagation delay is relatively smaller than other terms. According to the frame format of IEEE 802.15.4 [30], the fixed overhead is 11 bytes and there are 0 to 20 bytes for addresses and frame payload. As observed from Fig. 3, the delay curves rise with the increase of length $L_{\mathbf{q}}$. The delays of UK-PST are smaller than that of IK-PST, which illustrates that UK-PST can reduce the communication overhead. The overhead increases linearly with the rise of $L_{\mathbf{q}}$. When the overhead L_0 is higher, both schemes have higher delays. When $L_0 = 31$ bytes, the delay of UK-PST is about half that of IK-PST.

B. Computation Complexity

Computation complexity is very important for resource-constrained systems. UK-PST does not need the sophisticated reconciliation phase, and instead uses un-identical binary sequences as the encryption and decryption keys. The disagreements between keys will bring in the errors in the recovery of $\mathbf{d}$. The errors are similar to the transmission errors caused by transmission distortion. Therefore, we can deem the errors as part of the equivalent channel errors and couple the error correction task to the existing channel coding of the system.

The computational complexity is dominated by the decoder complexity. This paper uses BCH code, as it has been widely used because of the low complexity. The decoder complexity bounds for a BCH code $(\mathcal{C}, n, k, t)$ can be given as [31]

$$\zeta^{UB}(\mathcal{C}) = (45k^2 + 4k)n^2(\log n)^2, \tag{18}$$

$$\zeta^{LB}(\mathcal{C}) = 45k^2n^2(\log n)^2. \tag{19}$$

The IK-PST scheme uses two BCH codes, $(\mathcal{C}_0, n_0, k_0, t_0)$ for the physical channel with error probability ϵ_0 and $(\mathcal{C}, n, k, t)$ for the information reconciliation with $\epsilon_{\mathbf{q}}$. Therefore, we use

$$\zeta_{IK}^{UB} = \zeta^{UB}(\mathcal{C}_0) + \zeta^{UB}(\mathcal{C}), \tag{20}$$

$$\zeta_{IK}^{LB} = \zeta^{LB}(\mathcal{C}_0) + \zeta^{LB}(\mathcal{C}). \tag{21}$$

for approximate calculation of complexity of IK-PST.

The UK-PST scheme uses only one BCH code $(\mathcal{C}', n', k', t')$ for the cascade channel with ϵ_{eq} [32], given as

$$\epsilon_{eq} = \epsilon_0 + \epsilon_{\mathbf{q}} - 2\epsilon_0\epsilon_{\mathbf{q}}. \tag{22}$$

When $\epsilon_0 = 0$, we find that $\epsilon_{eq} = \epsilon_{\mathbf{q}}$ and both schemes have the same computational complexity. When $\epsilon_0 > 0$, we use

$$\zeta_{UK}^{UB} = \zeta^{UB}(\mathcal{C}'), \tag{23}$$

$$\zeta_{LK}^{UB} = \zeta^{LB}(\mathcal{C}'). \tag{24}$$

for approximate calculation of complexity of UK-PST.

Fig. 4 shows that the bounds increase with $\epsilon_{\mathbf{q}}$ and both the decoder complexity upper bound and lower bound of UK-PST are lower than that of IK-PST, when the error probability of the physical channel is $\epsilon_0 = 0.1$.

C. Secure Transmission Rate

The secure transmission rate is defined as the length of secure transmitted information divided by the time to produce it, which is mathematically given by

$$R = \frac{L_{\mathbf{d}}}{T} = \frac{L_{\mathbf{d}}}{2\Delta T L_{\mathbf{q}}}. \tag{25}$$

According to the OTP theory [4], the upper bound of the secure transmission rate between user i and j satisfies that

$$R^{UB} = \frac{1}{T}I(\mathbf{q}_{i,j}, \mathbf{q}_{j,i}) \tag{26}$$

$$= \frac{1}{T}(H(\mathbf{q}_{i,j}) - H(\mathbf{q}_{i,j}|\mathbf{q}_{i,j})), \tag{27}$$

$$= \frac{1}{2\Delta T}(1 + \frac{1}{2}\log(1 - \epsilon_{\mathbf{q}}) + \frac{1}{2}\epsilon_{\mathbf{q}}). \tag{28}$$

The bound rate is reached through the Slepian-Wolf source encoding with random binning structure, which is complex for implementation.

Then, we focus on the secure transmission rates of the IK-PST and UK-PST schemes.

IK-PST: In the step 1-1, a $(\mathcal{C}, n, k, t)$ ECC is used to generate a syndrome $\mathbf{s}$. In this case, $k = L_{\mathbf{q}}$ and the length of $\mathbf{s}$ is denoted as $L_{\mathbf{s}} = n - k$. Besides, the disagreement ratio $\epsilon_{\mathbf{q}}$ is within the correction capability of $\mathcal{C}$, which means that $\epsilon_{\mathbf{q}} \leq \frac{t}{n}$. Plugging these components, we get the following proposition.

Proposition 1: The upper bound of secure transmission rate for IK-PST is given by

$$R_{IK}^{UB} = \frac{L_{\mathbf{d}}^{UB}}{T} = \frac{1}{2\Delta T} \frac{L_{\mathbf{q}} - 4\epsilon_{\mathbf{q}} L_{\mathbf{q}} - 1}{(1 - 2\epsilon_{\mathbf{q}}) L_{\mathbf{q}}}. \tag{29}$$

Proof: See Appendix A. ∎

Remark 1: It is observed that R_{IK}^{UB} decreases against the disagreement ratio $\epsilon_{\mathbf{q}}$, while it increases with the length $L_{\mathbf{q}}$. When $L_{\mathbf{q}}$ approaches infinity, it derives that

$$\lim_{L_{\mathbf{q}} \to +\infty} R_{IK}^{UB} = \frac{1}{2\Delta T} \left(\frac{1 - 4\epsilon_{\mathbf{q}}}{1 - 2\epsilon_{\mathbf{q}}}\right). \tag{30}$$

UK-PST: In the step 3-1, a $(\mathcal{C}', n', k', t')$ ECC is used to generate the syndrome $\mathbf{s}'$. In this case, $n' = L_{\mathbf{q}}$ and the length of $\mathbf{s}'$ is $L_{\mathbf{s}'} = n' - k'$. Besides, the disagreement ratio $\epsilon_{\mathbf{q}}$ is within the correction capability of $\mathcal{C}'$, which means that $\epsilon_{\mathbf{q}} \leq \frac{t'}{n'}$. Plugging these components, we get the following proposition.

Proposition 2: The upper bound of secure transmission rate for UK-PST is given by

$$R_{UK}^{UB} = \frac{L_{\mathbf{d}'}^{UB}}{T} = \frac{1}{2\Delta T} \frac{L_{\mathbf{q}}(1 - 2\epsilon_{\mathbf{q}}) - 1}{L_{\mathbf{q}}}. \tag{31}$$

Proof: See Appendix B. ∎

Remark 2: It is observed that R_{UK}^{UB} decreases against the disagreement ratio $\epsilon_{\mathbf{q}}$, while it increases with the length $L_{\mathbf{q}}$. When $L_{\mathbf{q}}$ approaches infinity, it derives that

$$\lim_{L_{\mathbf{q}} \to +\infty} R_{UK}^{UB} = \frac{1}{2\Delta T}(1 - 2\epsilon_{\mathbf{q}}). \tag{32}$$

We compare these two bounds of the IK-PST and the UK-PST schemes and prove the following theorem.

Theorem 1: For any $\epsilon_{\mathbf{q}} \in [0, 0.5)$ and $L_{\mathbf{q}} > 0$, the upper bounds of secure transmission rates satisfy that

$$R_{UK}^{UB} \geq R_{IK}^{UB}. \tag{33}$$

The $\Delta R = R_{UK}^{UB} - R_{IK}^{UB}$ increases with $\epsilon_{\mathbf{q}}$. The equality holds, if and only if $\epsilon_{\mathbf{q}} = 0$.

Proof: See Appendix C. ∎

Remark 3: Theorem 1 reveals that UK-PST scheme has a higher bound of secure transmission rate than that of IK-PST. In the UK-PST, the $\mathbf{s}'$ is the syndrome of $\mathbf{d}'$ and also encrypted before transmission over the public channel. In the IK-PST $\mathbf{s}$ is the syndrome of $\mathbf{q}_{j,i}$ and transmitted in cleartext. Therefore, under the same condition, UK-PST is able to provide higher efficiency for secure transmission. Besides, $\mathcal{C}'$ has a shorter code length than that of $\mathcal{C}$, which also verifies that the computation complexity of UK-PST is reduced.

Fig. 5 shows the secure transmission rates of the bounds. We set $\Delta T = 1$, which means that the secure transmission rate is calculated per quantization bit. The secure transmission rates decrease with the increase of $\epsilon_{\mathbf{q}}$, while the rate of UK-PST is closer to the bound rate and it is higher than that of IK-PST. When $\epsilon_{\mathbf{q}}$ is close to 0.25, the rate of IK-PST falls to 0 which means no secure transmission is available. While UK-PST can still provide a positive secure transmission rate.

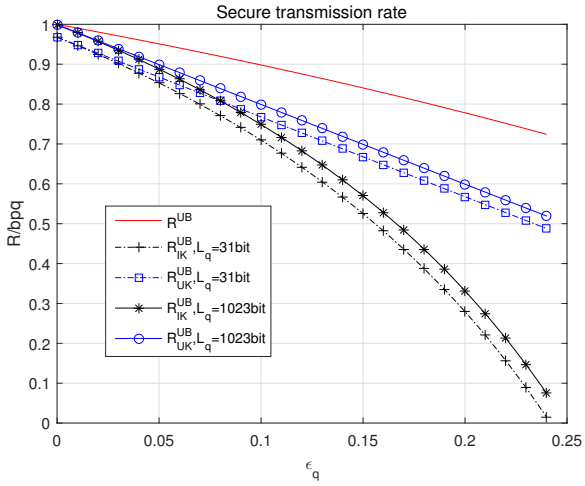

Fig. 5. The secure transmission rate of IK-PST and UK-PST as a function of the disagreement ratio $\epsilon_{\mathbf{q}}$. The time intervel between two quantization bits is set as $\Delta T = 1/2$.

In summary, UK-PST has lower communication overhead, lower computation complexity and higher secure transmission rate compared with IK-PST.

V. OTP Secure Transmission for a Group of Users

It is straightforward to extend the IK-PST scheme from two users to a group of users, which is omitted due to space limitation. In this section, we extend the pairwise UK-PST scheme to group users, which contains two phases, i.e., pairwise phase and group phase.

- **Pairwise phase**: pairwise bit sequences with high similarity are extracted from the wireless channels between every two legitimate users.
- **Group phase**: a confidential message is securely shared between group users with protection of pairwise bit sequences.

Next, we examine two typical topologies in wireless networks when performing group UK-PST for multiple users.

A. Group UK-PST in a Star Network

In a star network with N users, the central user N is wirelessly connected with child users, $1, 2, \cdots, N-1$, while every two child nodes are not directly connected. The group secure transmission protocol is summarized in Algorithm 1.

1) Pairwise Phase: Firstly, the central user N broadcasts the probe and other users collect the measurements. The measurement of the i-th user is $\mathbf{r}_{N,i}$, where $i \in \{1, 2, \cdots, N-1\}$. Next, users $1, 2, \cdots, N-1$ broadcast the probe in order and user N collects the measurements $\mathbf{r}_{i,N}$ successively. To ensure that $\mathbf{r}_{N,i}$ and $\mathbf{r}_{i,N}$ are highly correlated, the time delay should be deliberately kept smaller than the coherence time.

Algorithm 1 UK-PST algorithm in a star topology network.

Require: The confidential message $\mathbf{d}'$ at the central user N.
Ensure: The recovered messages $\hat{\mathbf{d}}_i$ at the user i, where $i \in \{1, 2, \cdots, N-1\}$.

Pairwise Phase:

1: User N broadcasts the probe and other users collect the measurements.
2: **for** $i \leftarrow 1, N-1$ **do**
3: User i broadcasts the probe, and user N collects the measurement.
4: **end for**
5: The center user N carries out quantization according to (1) and get $\{\mathbf{q}_{1,N}, \mathbf{q}_{2,N}, \cdots, \mathbf{q}_{N-1,N}\}$.
6: The user i carries out quantization according to (1) and get $\mathbf{q}_{N,i}$.

Group Phase:

7: User N encodes $\mathbf{d}'$ using (9) as described in the protocol 3-1 and gets $\mathbf{d}_{con}$.
8: User N encrypts $\mathbf{d}_{con}$ with $\mathbf{q}_{1,N}$,$\mathbf{q}_{2,N}$,$\cdots$,$\mathbf{q}_{N-1,N}$ successively as described in the step 3-2.
9: User N concatenates the ciphertexts and then broadcasts them via the public channel.
10: **for** $i \leftarrow 1, N-1$ **do**
11: User i recovers the confidential message $\hat{\mathbf{d}}_i$ using his quantized bit sequence $\mathbf{q}_{N,i}$.
12: **end for**

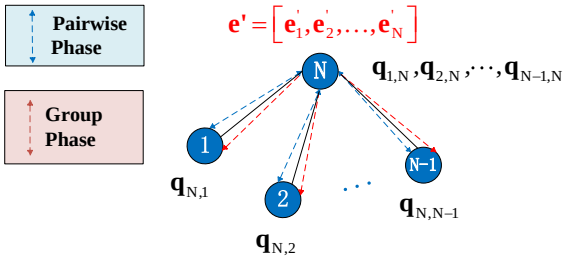

Fig. 6. The group secure transmission protocol for the star network.

Secondly, the channel measurements are converted into bit sequences using the same quantization method as shown in (1). The pairwise bit sequences $\mathbf{q}_{N,i}$ and $\mathbf{q}_{i,N}$ have high similarity but are not identical. Denotes $\Delta\mathbf{q}_i = \mathbf{q}_{N,i} \oplus \mathbf{q}_{i,N}$ as the difference between $\mathbf{q}_{N,i}$ and $\mathbf{q}_{i,N}$. Denote $\epsilon_{\mathbf{q}_i}$ as the disagreement ratio

$$\epsilon_{\mathbf{q}_i} = \frac{1}{L_{\mathbf{q}}} \left\| \mathbf{q}_{N,i} - \mathbf{q}_{i,N} \right\|_1, \tag{34}$$

and $\epsilon_{max} = \max_i \epsilon_{\mathbf{q}_i}$ represents the highest disagreement ratio among all users.

It is noteworthy that UK-PST does not contain an information reconciliation process and thus does not trigger the information leakage. The bit mismatch will be addressed in the group phase. The pairwise phase may be repeated for several times to produce long enough bit sequences with length $L_{\mathbf{q}}$. After the pairwise phase, the central user N has collected a group of sequences $\mathbf{q}_{1,N}, \mathbf{q}_{2,N}, \cdots, \mathbf{q}_{N-1,N}$. The other users have one sequence each, e.g., $\mathbf{q}_{N,i}$ for the i-th user.

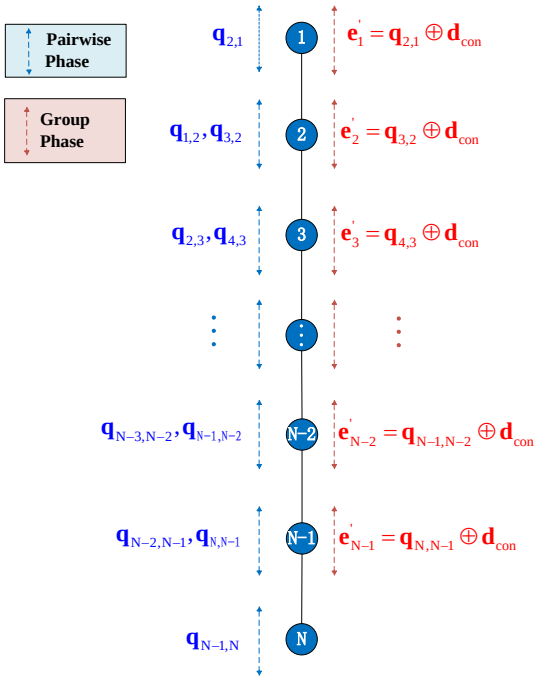

Fig. 7. The group secure transmission protocol for the chain network.

2) Group Phase: User N feeds the message $\mathbf{d}'$ into the channel encoder and the syndrome is denoted as $\mathbf{s}' = \mathcal{E}(\mathbf{d}')$. The concatenation $\mathbf{d}_{con} = [\mathbf{d}', \mathbf{s}']$ is encrypted and the ciphertexts are denoted as $\mathbf{e}' = [\mathbf{e}'_1, \mathbf{e}'_2, \cdots, \mathbf{e}'_{N-1}]$, where

$$\mathbf{e}'_i = \mathbf{d}_{con} \oplus \mathbf{q}_{i,N}. \tag{35}$$

User N broadcasts the ciphertext $\mathbf{e}'$ over the public channel. Assume that the broadcast information can be received without any errors, which can be realized through the channel coding.

The user i has the corresponding pairwise bit sequence $\mathbf{q}_{N,i}$ and can speculate $\mathbf{d}_{con}$ by

$$\hat{\mathbf{d}}^i_{con} = \mathbf{e}'_i \oplus \mathbf{q}_{N,i} = \Delta\mathbf{q}_i \oplus \mathbf{d}_{con}. \tag{36}$$

With the help of the syndrome $\mathbf{s}$, user i can correct the error bits in $\hat{\mathbf{d}}^i_{con}$ by:

$$\hat{\mathbf{d}}_i = \mathcal{D}(\hat{\mathbf{d}}^i_{con}). \tag{37}$$

To guarantee $\hat{\mathbf{d}}_i = \mathbf{d}'$ for arbitrary i, the syndrome $\mathbf{s}$ should be capable to correct all errors even in the worst case with the highest disagreement ratio of ϵ_{max}.

B. Group UK-PST in a Chain Network

In a chain network, users are connected sequentially and communications only occur between adjacent users, as shown in Fig. 11. Algorithm 2 gives an algorithm of UK-PST for a chain network with N users.

1) Pairwise Phase: Users $1 \sim N$ sound the channel in turn. First, user 1 broadcasts the probe packets and user 2 obtains the measurements $\mathbf{r}_{1,2}$. Next, user j $(2 \leq j \leq N-1)$ broadcasts, and users $j-1$ and $j+1$ obtain their measurements $\mathbf{r}_{j,j-1}$ and $\mathbf{r}_{j,j+1}$, respectively. Finally, user N broadcasts and user $N-1$ obtains the measurements $\mathbf{r}_{N,N-1}$.

Algorithm 2 UK-PST algorithm in a chain topology network.

Require: The confidential message $\mathbf{d}'$ at the central user N.
Ensure: The recovered messages $\hat{\mathbf{d}}_i$ at the user i, where $i \in \{1, 2, \cdots, N-1\}$.

Pairwise Phase:

1: Users $1 \sim N$ send the probe packets to their adjacent users and collect the measurements.
2: All of the users carry out quantization according to (1).

Group Phase:

3: User 1 encodes $\mathbf{d}'$ using (9) as described in the step 3-1and gets $\mathbf{d}_{con}$.
4: User 1 sends the encrpypted result $\mathbf{e}'_1$ to user 2.
5: **for** $i \leftarrow 2, N-1$ **do**
6: User i recovers messages $\hat{\mathbf{d}}_i$ and then broadcasts $\mathbf{e}'_i$.
7: **end for**
8: User N recovers messages $\hat{\mathbf{d}}_N$.

These measurements are converted into bit sequences, as described in (1). After the pairwise phase, user j has two bit sequences $\mathbf{q}_{j-1,j}$ and $\mathbf{q}_{j+1,j}$. For endpoint users 1 and N, each has one bit sequence, $\mathbf{q}_{2,1}$ and $\mathbf{q}_{N-1,N}$ respectively.

2) Group Phase: User 1 firstly encodes $\mathbf{d}'$ and then broadcasts the ciphertext $\mathbf{e}'_1$, which is obtained by

$$\mathbf{e}'_1 = \mathbf{q}_{2,1} \oplus \mathbf{d}_{con} = \mathbf{q}_{2,1} \oplus [\mathbf{d}', \mathbf{s}'], \tag{38}$$

where $\mathbf{s}'$ is the syndrome of $\mathbf{d}'$. We also assume that $\mathbf{e}_1$ can be received correctly. Since user 2 has the corresponding pairwise bit sequence $\mathbf{q}_{1,2}$, therefore he can speculate $\mathbf{d}'$ and $\mathbf{s}'$ by

$$\hat{\mathbf{d}}^2_{con} = \mathbf{q}_{1,2} \oplus \mathbf{e}'_1 = \Delta\mathbf{q}_{1,2} \oplus \mathbf{d}_{con}, \tag{39}$$

where $\Delta\mathbf{q}_{1,2} = \mathbf{q}_{1,2} \oplus \mathbf{q}_{2,1}$ reflects the difference between $\mathbf{q}_{1,2}$ and $\mathbf{q}_{2,1}$.

Likewise, user 2 can correct the error bits in $\hat{\mathbf{d}}^2_{con}$ by:

$$\hat{\mathbf{d}}_2 = \mathcal{D}(\hat{\mathbf{d}}^2_{con}). \tag{40}$$

Subsequently, the bit sequences $\mathbf{q}_{2,1}$ is recovered by:

$$\hat{\mathbf{q}}_{2,1} = [\hat{\mathbf{d}}_2, \mathcal{E}(\hat{\mathbf{d}}_2)] \oplus \mathbf{e}'_1, \tag{41}$$

When $\Delta\mathbf{q}_{1,2}$ is within the error correction capability of the decoder, user 2 can get perfect estimations of $\mathbf{d}'$ and $\mathbf{q}_{2,1}$ that

$$\hat{\mathbf{d}}_2 = \mathbf{d}', \hat{\mathbf{q}}_{2,1} = \mathbf{q}_{2,1}. \tag{42}$$

Next, user 2 encrypts $\mathbf{d}_{con}$ with $\mathbf{q}_{3,2}$ and broadcasts $\mathbf{e}'_2 = \mathbf{q}_{3,2} \oplus \mathbf{d}_{con}$. User 3 recovers $\mathbf{d}$ using his pairwise bit sequence $\mathbf{q}_{2,3}$ and then broadcasts

$$\mathbf{e}'_3 = \mathbf{q}_{4,3} \oplus \mathbf{d}_{con}, \tag{43}$$

and so on. Finally, user $N-1$ broadcasts

$$\mathbf{e}'_{N-1} = \mathbf{q}_{N,N-1} \oplus \mathbf{d}_{con}, \tag{44}$$

and user N recovers data $\hat{\mathbf{d}}_N$ with $\mathbf{q}_{N-1,N}$. When $\Delta\mathbf{q}_{N-1,N} = \mathbf{q}_{N-1,N} \oplus \mathbf{q}_{N,N-1}$ is within the error correction capability of the ECC, user N can recover $\hat{\mathbf{d}_N} = \mathbf{d}$ correctly.

TABLE I
PERFORMANCE COMPARATION FOR GROUP SCENARIOS

Performance	IK-PST		UK-PST	
Transmissions	Star	Chain	Star	Chain
	$2N$	3N-2	$N+1$	2N-1
Reconciliation	$N-1$		0	
Secure Rate	$\frac{1}{N\Delta T}\frac{L_{\mathbf{q}}-4\epsilon_{max}L_{\mathbf{q}}-1}{(1-2\epsilon_{max})L_{\mathbf{q}}}$		$\frac{1}{N\Delta T}\frac{L_{\mathbf{q}}(1-2\epsilon_{max})-1}{L_{\mathbf{q}}}$	

C. Discussion

Table I compares the performance of IK-PST and UK-PST for group scenarios from the aspects of the number of transmissions, the number of information reconciliation and the secure transmission rate.

In a star network, IK-PST needs $2N$ transmissions, including N channel probing, $N-1$ information reconciliation and one data transmission. UK-PST reduces it to $N+1$, including N channel probing and one data transmission. Similarly, in a chain network, IK-PST needs $3N-2$ transmissions, including N channel probing, $N-1$ information reconciliation and $N-1$ data transmission. UK-PST reduces it to $2N-1$, including N channel probing and $N-1$ data transmission.

In both star and chain networks, UK-PST does not need to produce the identical pairwise key, and thus avoids sophisticated information reconciliation. This is at the cost of a stronger channel coding to correct an equivalent error rate of $\epsilon_{eq} = \epsilon_0 + \epsilon_{max} - 2\epsilon_0\epsilon_{max}$. Following (29) and (31), the secure transmission rates of IK-PST and UK-PST for a group of users are

$$R^{UB}_{IK,G} = \frac{1}{N\Delta T}\frac{L_{\mathbf{q}} - 4\epsilon_{max}L_{\mathbf{q}} - 1}{(1-2\epsilon_{max})L_{\mathbf{q}}} \tag{45}$$

and

$$R^{UB}_{UK,G} = \frac{1}{N\Delta T}\frac{L_{\mathbf{q}}(1-2\epsilon_{max}) - 1}{L_{\mathbf{q}}}, \tag{46}$$

respectively.

VI. Simulation and Experimental Validation

This section evaluated the performance of the IK-PST and UK-PST schemes through both simulations and experiments.

A. Simulations

Monte-Carlo simulation was carried out to evaluate the system performance. We did 1,000 loops per simulation, each loop with more than 10,000 bits. The quantization results between every two pairwise users were modeled as random distributed binary sequences with the disagreement ratio $\epsilon_{\mathbf{q}}$. In both schemes, the BCH code $(\mathcal{C}, n, k, t)$ is chosen and the parameters of n and k are designed according to $\epsilon_{\mathbf{q}}$ and t. For example, when $t = 1$ and $\epsilon_{\mathbf{q}} = 0.02$, the length of n must not exceed $t/\epsilon_{\mathbf{q}} = 50$. Otherwise, it does not have the capability to correct all of the disagreements. Since the code length of BCH should satisfies that $n = 2^m - 1, m \in \{3, 4, \cdots, 16\}$, we can choose $m = 5$ and use the $(31, 26, 1)$ BCH code, unless otherwise specified.

We define effective secure transmission rate as

$$R_{eff} = R(1 - \eta_f), \tag{47}$$

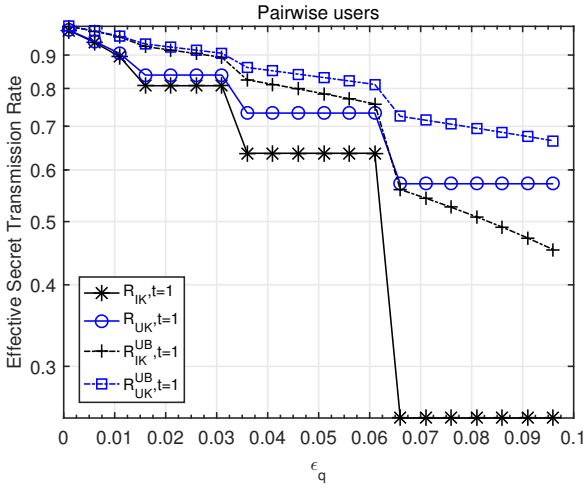

Fig. 8. Performance of effective secure transmission rates and upper bounds versus $\epsilon_{\mathbf{q}}$ for a pair of users.

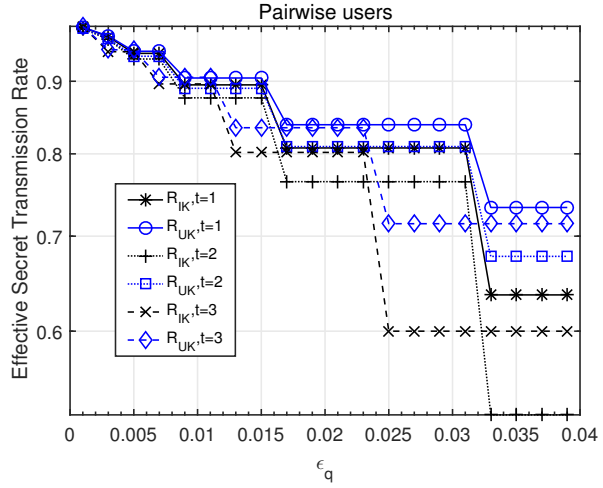

Fig. 9. Performance of effective secure transmission rate versus $\epsilon_{\mathbf{q}}$ for a pair of users with different t.

where R is the secure transmission rate defined in Section IV-C and η_f represents the probability of failure. Due to the inaccurate estimation of $\epsilon_{\mathbf{q}}$ and burst errors, the designed BCH code cannot always correct all the disagreements. Therefore, we also take the failure ratio η_f into consideration. For simplicity, the time interval between two quantization bits is set as $\Delta T = 1/2$, we can thus omit it in the calculation of secure transmission rate. Thus, (47) can be further written as

$$R_{eff} = \frac{L_{\mathbf{d}}}{L_{\mathbf{q}}}(1-\eta_f). \tag{48}$$

Fig. 8 and Fig. 9 present effective secure transmission rates of IK-PST and UK-PST as a function of the disagreement ratio of $\epsilon_{\mathbf{q}}$ for a pair of users. Following (29) and (31), the analytical upper bounds of both rates R^{UB}_{IK} and R^{UB}_{UK} are also shown in Fig. 8 as a reference. As expected, the rates decrease with $\epsilon_{\mathbf{q}}$ and the rates decrease much faster for the IK-PST scheme. The simulation curves have the same trends with that of the upper bounds, which verify the theoretical analysis in Section IV-C. Although $\epsilon_{\mathbf{q}}$ increases continuously, the rate curves have stepwise decline, caused by the limitation of available BCH codes. We also find that the effective secure transmission rates over $\epsilon_{\mathbf{q}}$ follow similar decreasing trend despite of the different set of t, as shown in Fig. 9. For $t = 1, 2, 3$, the rates of UK-PST are higher than that of IK-PST, and the gaps expand with the increase of $\epsilon_{\mathbf{q}}$. When t increases, the effective secure transmission rates decrease, because more percentage of parity bits are used. Therefore, we choose $t = 1$ for the following simulations.

Fig. 10 and Fig. 11 compare the effective secure transmission rates of IK-PST and UK-PST versus the user number in a star network and a chain network, respectively. We set that all of the users in the group have the same disagreement ratio $\epsilon_{\mathbf{q}}$. We simulate two cases of $\epsilon_{\mathbf{q}} = 0.05$ and $\epsilon_{\mathbf{q}} = 0.1$ and set $t = 1$. Group simulation results also indicate that UK-PST has higher effective secure transmission rate than that of IK-PST. When $\epsilon_{\mathbf{q}} = 0.05$, R_{UK} is about 1.15 times as much as R_{IK}, while the multiple becomes larger than 2, when $\epsilon_{\mathbf{q}} = 0.1$.

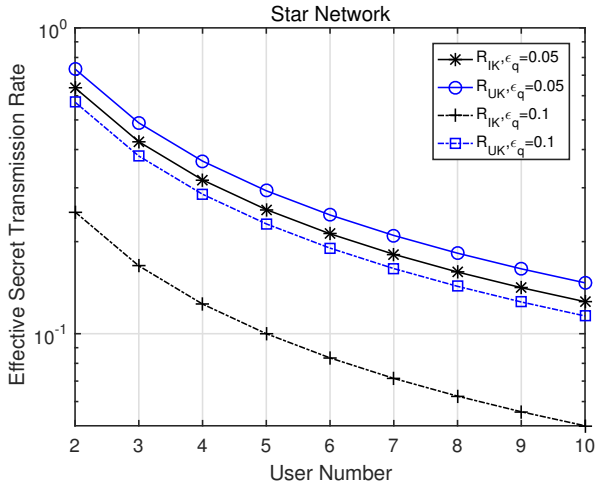

Fig. 10. Performance of effective secure transmission rate versus the user number in a star network, $t = 1$.

Besides, in both figures, the effective secure transmission rates decrease with the group size. For example, when $\epsilon_{\mathbf{q}} = 0.1$, R_{IK} drops from 0.25 with two users to 0.1 with five users and to 0.05 with ten users. The results reflect the inverse relation between the rate and group size, which is consistent with the expressions of upperbound in (45) and (46).

B. Experiments

We also verified the robustness and efficiency of IK-PST and UK-PST using a testbed with wireless motes. A wireless mote includes a STM8L101 micro-controller, a built-in antenna and a CC1101 radio chip operating at 430 MHz. We implemented half-duplex TDD for a pair of users, and used the probe packet to fulfill our needs to collect RSS measurements. We conducted experiments at the place around the No. 6 building of the Chinese Network Valley, Nanjing, China.

The experiments were carried out in three typical environments, including indoor, outdoor and corridor, as shown in Fig. 12. For the same environment, we also measured RSS

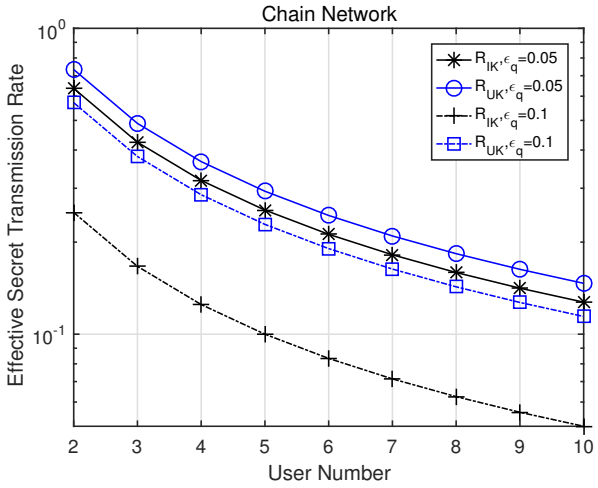

Fig. 11. Performance of effective secure transmission rate versus the user number in a chain network, $t = 1$.

Fig. 12. Three experimental environments.

TABLE II
EXPERIMENT SCENARIOS

No.	Environment	Pedestrians	Distance	LoS/NLoS	Dataset
1	Indoor	Without	1.5 m	LoS	10
2	Indoor	Without	1.5 m	NLoS	10
3	Indoor	With	4.5 m	NLoS	10
4	Corridor	Without	3.5 m	LoS	10
5	Corridor	With	3.5 m	LoS	10
6	Outdoor	Without	3.5 m	LoS	10

under different conditions, i.e., with or without pedestrians passing through, line of sight (LoS) and non line of sight (NLoS), and the communication distance between the two motes. These setups were categorized in six scenarios as listed in Table. II. For each scenario, we did ten independent tests between two wireless motes and 255 RSS measurements were collected in each test. The RSS measurements were quantized into bit sequences using order-1 quantization method as described in (1).

Fig. 13 shows the effective secure transmission rate of IK-PST and UK-PST under various scenarios. The disagreement ratio $\epsilon_{\mathbf{q}}$ is also plotted for reference. It is observed that

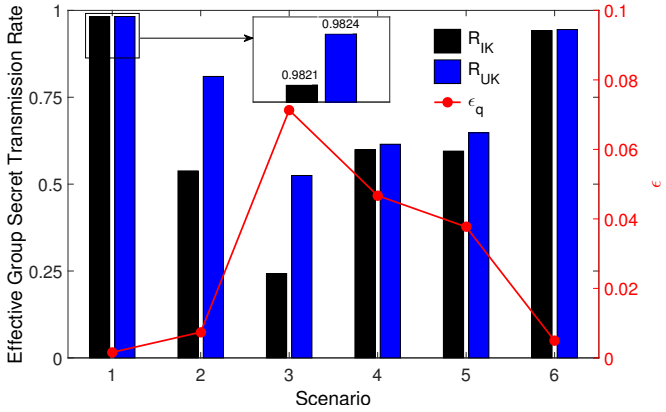

Fig. 13. Effective secure transmission rate under various scenarios.

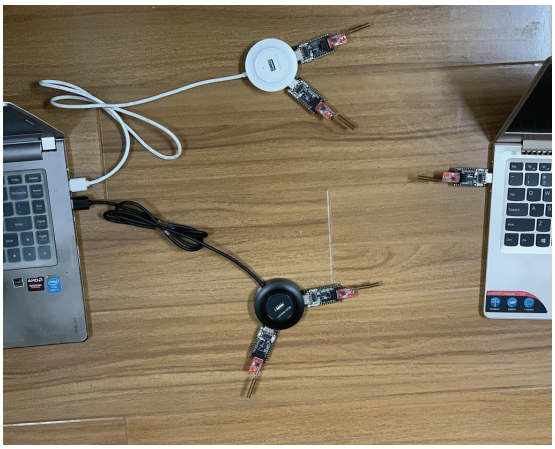

Fig. 14. Experiment platform with multiple wireless motes.

the rates are negatively correlated with $\epsilon_{\mathbf{q}}$. Scenario three achieves the highest $\epsilon_{\mathbf{q}}$ due to the longest distance of 4.5 meters, and thus the rates in this scenarios are lower. Different from the simulation, we cannot generate data with the set $\epsilon_{\mathbf{q}}$ in the experiments. Therefore, the estimation of $\epsilon_{\mathbf{q}}$ is not accurate, which may result in failure of correction. From the experimental results, R_{UK} is higher than R_{IK} for all six scenarios. In the scenario one, R_{UK} and R_{IK} are 0.9821 and 0.9824, respectively. Due to the small value of $\epsilon_{\mathbf{q}}$ in this scenario, both rates are close to 1 and the gap is small. In other scenarios with higher $\epsilon_{\mathbf{q}}$, such as the scenario three, the gap becomes significant.

We also verified the performance against a group of users with the platform shown in Fig. 14. Fig. 15 and Fig. 16 show the effective secure transmission rate versus the user number in a star and chain network, respectively. As expected, both rates fall with the increase of the user number. From Fig. 15, R_{UK} is almost twice as much as R_{IK} for two users, and the multiple reduces to 1.5 with six users. In Fig. 16, R_{UK} is about 1.15 times as much as R_{IK}. The results show that the UK-PST schemes can provide higher secure transmission rate for a group of users with both star and chain topologies.

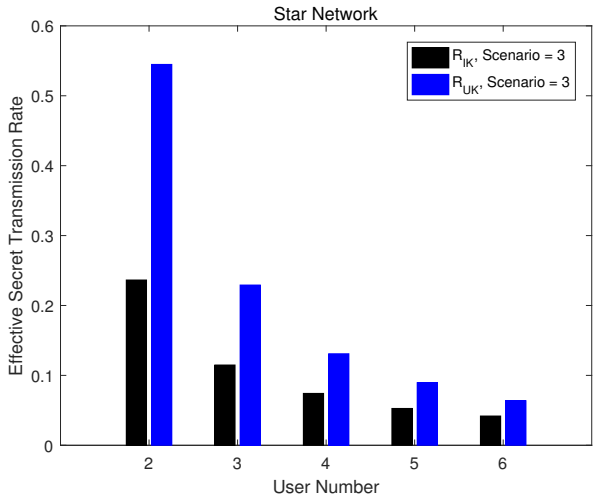

Fig. 15. Effective secure transmission rate versus the user number in a star network, $t = 1$.

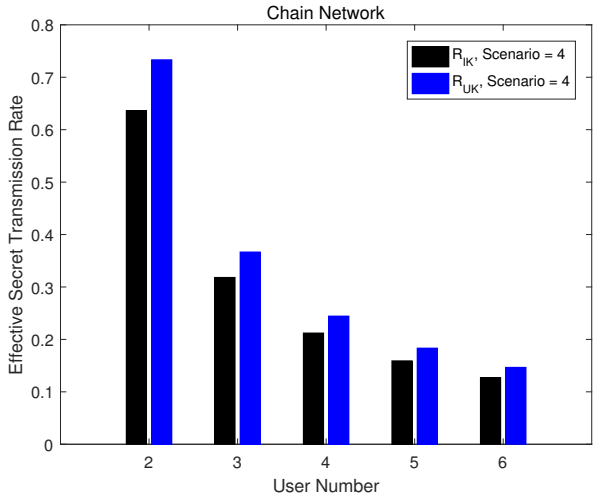

Fig. 16. Effective secure transmission rate versus the user number in a chain network, $t = 1$.

VII. Conclusion

This paper investigated the OTP secure transmission by exploiting the randomness residing in the reciprocal wireless channel. We proposed two approaches, IK-PST and UK-PST. IK-PST uses the same pairwise key at both ends while UK-PST employs un-identical keys. Although IK-PST is intuitive to understand, its performances are inferior to UK-PST from the perspective of communication overhead, computation complexity and secure transmission rate. The performance gap expands when both schemes are extended to a group of users. We conducted simulations and implemented prototypes of the two schemes. Both simulation and experimental results show that UK-PST can achieve higher effective secret transmission rate than that of IK-PST and the gap expands with the increase of the disagreement ratio of channel quantization results, which verify the theoretical analysis.

Appendix A
Proof of Proposition 1

For the ECC $(\mathcal{C}, n, k, t)$, it should satisfies that $n - k \geq 2t + 1$, which indicates that

$$L_{\mathbf{s}} = n - k \geq 2t + 1. \tag{49}$$

Assuming that $\mathcal{C}$ reaches the bound of the correction capability, then

$$\epsilon_{\mathbf{q}} = \frac{t}{n} \leq \frac{t}{k + 2t + 1}, \tag{50}$$

which means that

$$t \geq \frac{\epsilon_{\mathbf{q}}(1 + L_{\mathbf{q}})}{1 - 2\epsilon_{\mathbf{q}}}. \tag{51}$$

Futher, we can derive that

$$L_{\mathbf{s}} \geq 2t + 1 = \frac{2\epsilon_{\mathbf{q}} L_{\mathbf{q}} + 1}{1 - 2\epsilon_{\mathbf{q}}} \tag{52}$$

and then

$$L_{\mathbf{d}} \leq L_{\mathbf{q}} - L_{\mathbf{s}} = \frac{L_{\mathbf{q}} - 4\epsilon_{\mathbf{q}} L_{\mathbf{q}} - 1}{1 - 2\epsilon_{\mathbf{q}}}. \tag{53}$$

Therefore, the upper bound of the secure transmission rate of the IK-PST scheme is

$$R_{IK}^{UB} = \frac{L_{\mathbf{d}}^{UB}}{T} = \frac{1}{\Delta T} \frac{L_{\mathbf{q}} - 4\epsilon_{\mathbf{q}} L_{\mathbf{q}} - 1}{(1 - 2\epsilon_{\mathbf{q}}) L_{\mathbf{q}}}. \tag{54}$$

Appendix B
Proof of Proposition 2

For the ECC $(\mathcal{C}', n', k', t')$, it should satisfies that $n' - k' \geq 2t' + 1$, which indicates that

$$k' = L_{\mathbf{d}'}, n' = L_{\mathbf{q}}. \tag{55}$$

Assuming that $\mathcal{C}$ reaches the bound of the correction capability, then

$$\epsilon_{\mathbf{q}} = \frac{t'}{n'} = \frac{t}{L_{\mathbf{q}}}, \tag{56}$$

which means that

$$t' = \epsilon_{\mathbf{q}} L'_{\mathbf{q}}. \tag{57}$$

Futher, we can derive that

$$L_{\mathbf{s}'} \geq 2t' + 1 = 2\epsilon_{\mathbf{q}} L_{\mathbf{q}} + 1, \tag{58}$$

and

$$L_{\mathbf{d}'} \leq L_{\mathbf{q}} - L_{\mathbf{s}'} = L_{\mathbf{q}}(1 - 2\epsilon_{\mathbf{q}}) - 1. \tag{59}$$

Therefore, the upper bound of the secure transmission rate of the UK-PST scheme is

$$R_{UK}^{UB} = \frac{L_{\mathbf{d}'}^{UB}}{T} = \frac{1}{\Delta T} \frac{L_{\mathbf{q}}(1 - 2\epsilon_{\mathbf{q}}) - 1}{L_{\mathbf{q}}}. \tag{60}$$

APPENDIX C
PROOF OF THEOREM 1

$$\begin{aligned}\Delta R &= R_{UK}^{UB} - R_{IK}^{UB} \qquad (61)\\ &= \frac{1}{\Delta T}\left(\frac{L_{\mathbf{q}}(1-2\epsilon_{\mathbf{q}})-1}{L_{\mathbf{q}}} - \frac{L_{\mathbf{q}}-4\epsilon_{\mathbf{q}}L_{\mathbf{q}}-1}{(1-2\epsilon_{\mathbf{q}})L_{\mathbf{q}}}\right)\\ &= \frac{1}{\Delta T}\left(\frac{(L_{\mathbf{q}}(1-2\epsilon_{\mathbf{q}})^2-1+2\epsilon_{\mathbf{q}})-(L_{\mathbf{q}}-4\epsilon_{\mathbf{q}}L_{\mathbf{q}}-1)}{(1-2\epsilon_{\mathbf{q}})L_{\mathbf{q}}}\right)\\ &= \frac{1}{\Delta T}\left(\frac{2\epsilon_{\mathbf{q}}+4\epsilon_{\mathbf{q}}^2 L_{\mathbf{q}}}{(1-2\epsilon_{\mathbf{q}})L_{\mathbf{q}}}\right)\end{aligned}$$

Since $\epsilon_{\mathbf{q}} \in [0, 0.5)$ and $L_{\mathbf{q}} > 0$, we can get $R_{UK}^{UB} - R_{IK}^{UB} \geq 0$ and when $\epsilon_{\mathbf{q}} = 0$, the equality holds. The first-order partial derivative

$$\frac{\partial \Delta R}{\partial \epsilon_{\mathbf{q}}} = -2 + \frac{2(1+L_{\mathbf{q}})}{L_{\mathbf{q}}(1-2\epsilon_{\mathbf{q}})} > 0 \qquad (62)$$

Therefore, the gap of $\Delta R = R_{UK}^{UB} - R_{IK}^{UB}$ increases with $\epsilon_{\mathbf{q}}$.

REFERENCES

[1] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proc. 32nd Annual Conf. Computer Security Applications*, Los Angeles, CA, USA, Dec. 2016, pp. 226–236.

[2] E. Ronen, A. Shamir, A.-O. Weingarten, and C. O'Flynn, "IoT goes nuclear: Creating a ZigBee chain reaction," in *Proc. 2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 195–212.

[3] G. S. Vernam, "Secret signaling system," U.S. Patent 1 310 719, Jul. 12, 1919.

[4] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical J.*, vol. 28, no. 4, pp. 656–715, 1949.

[5] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 6th ed. Prentice Hall, 2013.

[6] C. Cheng, R. Lu, A. Petzoldt, and T. Takagi, "Securing the internet of things in a quantum world," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 116–120, 2017.

[7] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography – Part I: Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[8] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

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

[10] G. Li, C. Sun, J. Zhang, E. Jorswieck, B. Xiao, and A. Hu, "Physical layer key generation in 5G and beyond wireless communications: Challenges and opportunities," *Entropy*, vol. 21, p. 497, 2019.

[11] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

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

[13] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, Aug. 2016.

[14] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12 462–12 466, 2018.

[15] H. Ruotsalainen, J. Zhang, and S. Grebeniuk, "Experimental investigation on wireless key generation for low power wide area networks," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1745 – 1755, Mar. 2020.

[16] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, 2018.

[17] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Shanghai, China, Jun. 2011, pp. 1422–1430.

[18] H. Liu, J. Yang, Y. Wang, 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.

[19] H. Liu, Y. Jie, W. Yan, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. IEEE INFOCOM*, Orlando, FL, USA, May 2013, pp. 927–935.

[20] P. Xu, K. Cumanan, Z. Ding, X. Dai, and K. K. Leung, "Group secret key generation in wireless networks: algorithms and rate optimization," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1831–1846, 2016.

[21] C. D. T. Thai, J. Lee, J. Prakash, and T. Q. S. Quek, "Secret group-key generation at physical layer for multi-antenna mesh topology," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 1, pp. 18–33, 2019.

[22] G. Zheng, G. Fang, R. Shankaran, and M. A. Orgun, "Encryption for implantable medical devices using modified one-time pads," *IEEE Access*, vol. 3, pp. 825–836, 2015.

[23] L. Peng, G. Li, J. Zhang, and A. Hu, "Securing M2M transmissions using nonreconciled secret keys generated from wireless channels measurements," in *Proc. IEEE GLOBECOM Workshop Trusted Commun. with Physical Layer Security (TCPLS)*, Abu Dhabi, UAE, Dec. 2018, pp. 1–6.

[24] G. Li, L. Hu, and A. Hu, "Lightweight group secret key generation leveraging non-reconciled received signal strength in mobile wireless networks," in *Proc. IEEE ICC Workshops WPLS*, Shanghai, China, May. 2019, pp. 1–6.

[25] M. Zafer, D. Agrawal, and M. Srivatsa, "Limitations of generating a secret key using wireless fading under active adversary," *IEEE/ACM Trans. Netw.*, vol. 20, no. 5, pp. 1440–1451, 2012.

[26] L. Peng, G. Li, J. Zhang, R. Woods, M. Liu, and A. Hu, "An investigation of using loop-back mechanism for channel reciprocity enhancement in secret key generation," *IEEE Trans. Mobile Comput.*, vol. 18, no. 3, pp. 507–519, 2019.

[27] G. Li, Z. Zhang, Y. Yu, and A. Hu, "A hybrid information reconciliation method for physical-layer key generation," *Entropy*, vol. 21, no. 7, p. 688, 2019.

[28] 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. IEEE VTC*, Boston, MA, USA, Jan. 2015, pp. 1–5.

[29] G. Li, A. Hu, C. Sun, and J. Zhang, "Constructing reciprocal channel coefficients for secret key generation in FDD systems," *IEEE Commun. Lett.*, vol. 22, no. 12, pp. 2487 – 2490, 2018.

[30] E. Karapistoli, F.-N. Pavlidou, I. Gragopoulos, and I. Tsetsinas, "An overview of the IEEE 802.15. 4a standard," *IEEE Commun. Mag.*, vol. 48, no. 1, pp. 47–53, 2010.

[31] B. G. Bajoga and W. Walbesser, "Decoder complexity for BCH codes," in *Proceedings of the Institution of Electrical Engineers*, vol. 120, no. 4. IET, 1973, pp. 429–431.

[32] T. M. Cover and J. A. Thomas, *Elements of information theory*. John Wiley & Sons, 2012.