IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 29, 2018, accepted January 10, 2019, date of publication January 17, 2019, date of current version March 12, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2893594

A Two-Layer Secure Quantization Algorithm for Secret Key Generation With Correlated Eavesdropping Channel

HENGLEI JIN, KAIZHI HUANG, SHUAIFANG XIAO, YANGMING LOU, XIAOMING XU, AND YAJUN CHEN

National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China

Corresponding author: Kaizhi Huang (huangkaizhi@tsinghua.org.cn).

This work was supported in part by the National Natural Science Foundation of China under Grant 61501516, Grant 61701538, Grant 61871404, and Grant 61801435, in part by the China Postdoctoral Science Foundation Project under Grant 2018M633733, in part by the Scientific and Technological Key Project of Henan Province under Grant 182102210449, in part by the Scientific Key Research Project of Henan Province for Colleges and Universities under Grant 19A510024, and in part by the National Key Research and Development Program of China under Grant 2017YFB0801903.

ABSTRACT When the eavesdropping channel has a certain correlation with the legitimate channel, the physical layer key is susceptible to eavesdroppers. To ensure the security of the secret key, we propose a two-layer secure (TLS) quantization algorithm in this paper. First, we model the correlation between the distance and the channel correlation and derive the joint probability density function of channel phase and the key capacity. Then, we describe the detail of the TLS algorithm and prove the validity of our algorithm. Finally, we evaluate the performances of the TLS quantization algorithm using two parameters–key rate and bit disagreement rate. The Simulation results verify the effectiveness of the algorithm.

INDEX TERMS Physical-layer security, key generation, quantization, secret key capacity, correlated eavesdropping channel.

I. INTRODUCTION

Physical layer key generation aims to implement the information-theory secure by exploiting the characteristics of temporal varying, spatial decorrelation, and reciprocity of wireless channels [1]–[4]. In key generation technology, two legitimate users simultaneously measure the same noise channel, through which channel parameters that are highly correlated but not completely consistent can be obtained. Next, the legitimate users quantize the measured channel parameters to bit sequences, but the sequences are usually different due to channel variations between noise and observation intervals [5], [6]. Therefore, both the sender and the receiver need to correct the disagreement bit in the sequence through information reconciliation [7]. Finally, the information leaked during the information reconciliation process is deleted through the privacy amplification process [8].

The time-varying, spatial decorrelation, and reciprocity of the wireless channel guarantee the validity of the secret key. The time-varying of the channel is the main source of randomness for the physical layer key caused by the motion of objects in the environment. Channel reciprocity means that the signals at each end of the same link have identical statistical features, and reciprocity is the basis to generate the same key. The spatial decorrelation indicates that the characteristics of the wireless channel in different spatial locations are unique and cannot be replicated, ensuring that the secret key is not wiretapped by the eavesdropper. However, some studies and experiments have shown that under certain circumstances, wireless channels may lose the characteristics of spatial decorrelation [9]–[12]. In addition, eavesdroppers may try their best to approach legitimate users in order to wiretap secret key. And the eavesdropping channel is correlated with the legitimate channel when the location of the eavesdropper is close enough, resulting in the reduction of key capacity. In [13], the influence of the statistical characteristics of the eavesdropper on the key generation scheme is tested under an indoor environment, and it is found in the experiment that the channel may still be correlated even distance between the eavesdropper and the legitimate user outside the half-wavelength. In [14], the influence of channel correlation between the legitimate channel and the eavesdropper channel on the key capacity is considered. Moreover, the channel sparsity model is proposed in this paper, and calculates the key capacity which considering the

influence of eavesdroppers. Reference [15] proposes a correlation model of eavesdropping channel based on Rayleigh channel model, and analyzes the influence of sampling delay, eavesdroppers location, Doppler spread, and pilot length on channel correlation.

Most of related studies just propose correlated channel model, and analyze the influence of eavesdropping on key capacity. But no study proposes the scheme to solve the corresponding problem. When eavesdropping channel is correlated with legitimate channel, legitimate users and eavesdroppers will extract correlated information from the channel and generate key. How to determine which information is stolen by the eavesdropper and to eliminate the information is still a problem. Most of the existing studies assume that the eavesdropper maintains passive eavesdropping state. Therefore, the location of the eavesdropper cannot be determined, and the channel correlation as well as the influence of the eavesdropper cannot be estimated. In addition, the effect of correlated eavesdropping channel on key generation scheme which based on channel phase information (CPI) and received signal strength information (RSSI) is unknown.

Aiming at the above problems, we propose a two-layer secure quantization (TLS) algorithm for physical layer key generation in this paper. Firstly, according to the actual situation of the existing research and communication system, we introduce the correlated eavesdropping channel model, and use the information theory and random signal analysis theory to derive the key capacity based on the channel phase in the model. Then we propose the idea of TLS algorithm on the basic of phase information distribution and channel correlations: Quantizing the channel phase and dividing it into two layers of bit sequences according to the risk of eavesdropping. What's more, we use the first and second layer sequence as reconciliation information and key sequence to generate secret key, respectively. Finally, we evaluate our algorithm by parameters of key rate and bit disagreement rate. The effects of eavesdropping channel correlation and signal-to-noise ratio (SNR) on the security performance of the scheme are analyzed. The results show that our algorithm improves the security performance of the secret key with correlated eavesdropping channel.

The rest of the paper is organized as follows. Section II describes the system model of correlated eavesdropping channel and proposes the problem in this model. Section III presents the proposed algorithm and evaluates the performance of algorithm. Simulation results are given in Section IV. Finally, some conclusions are given in Section V.

Notation: Lower case letters and bold lower case letters denote scalar and vector, respectively. $(\cdot)^\dagger$ denotes the conjugate transpose, and $E\{\cdot\}$ is the expectation operation.

II. MOTIVATION

A. SYSTEM MODEL

The key generation model based on eavesdropping channel correlation is shown in Fig.1, including two legitimate users and an eavesdropper, Alice, Bob and Eve. They are

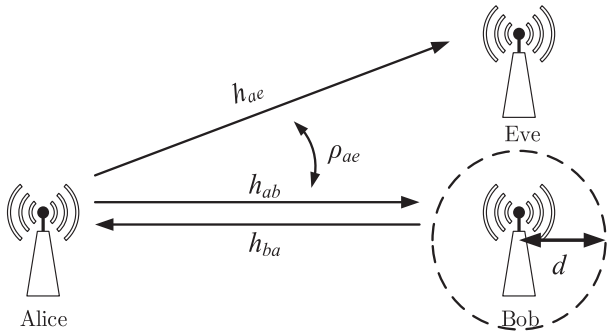


FIGURE 1. Correlated eavesdropping channel model.

all equipped with a single antenna and work in time-division duplex (TDD) mode. In this model, the channels are quasi-static Rayleigh channels, and the channel gains are invariant during the coherence time and are independent over the coherence time. The channel between Alice and Bob is called legitimate channel. According to reciprocal of channel, the uplink and downlink channel gains of legitimate channel h_{ab} and h_{ba} are identically distributed and highly correlated, $h_{ab}, h_{ba} \sim \mathcal{CN}(0, {\sigma_1}^2)$. The correlation function between h_{ab} and h_{ba} is given as

$$\rho_{ab} = \frac{E\{{h_{ab}}^\dagger h_{ba}\}}{{\sigma_1}^2} \tag{1}$$

It is assumed that Eve is located near Bob, so the eavesdropping channel between Alice and Eve is correlated with the legitimate channel. Alice and Bob cannot get the location and CSI of Eve, but they make sure there is no Eve in the circular area with Bob as the center and radius d. For the secrecy of the generated key, we consider the location of Eve in the worst point, where the correlation coefficient between eavesdropping channel and legitimate channel is highest outside the circular region. The highest correlation coefficient is $\rho_{ae}(d)$, $h_{ae} \sim \mathcal{CN}(0, {\sigma_1}^2)$. According to the definition of correlation, $\rho_{ae}(d)$ is given as

$$\rho_{ae}(d) = \frac{E\{{h_{ab}}^\dagger h_{ae}\}}{{\sigma_1}^2} = J_0(2\pi \frac{d}{\lambda}) \tag{2}$$

where $J_0(\cdot)$ is a zeroth-order Bessel function of the first kind and λ is the length of waveform.

Although Eve can rely on methods such as approaching legitimate users to make the eavesdropping channel correlated, generally speaking, the correlation is difficult to exceed the reciprocity of the main channel, that is $\rho_{ab} > \rho_{ae}(d)$. In this paper, we use the correlation between channels to analyze the performance of the scheme and the influence of eavesdropper.

For measuring the channel, Alice sends the pilot sequence S to Bob, Eve can also receive the S. The received signal at Bob and Eve can be written as

$$\begin{aligned} y_b &= h_{ab}S + n_b \\ y_e &= h_{ae}S + n_e \end{aligned} \tag{3}$$

and Bob also sends the pilot sequence to Alice. Similarly, the received signal at Alice can be written as

$$y_a = h_{ba}S + n_a \tag{4}$$

where n_a, n_b and n_e are i.i.d additive white Gaussian noise (AWGN) with variance ${\sigma_0}^2$ at the receiver Alice, Bob and Eve, respectively. Alice, Bob and Eve can then estimate the channel gain using Zero Forcing method as

$$\begin{aligned}
\hat{h}_{ab} &= y_b \frac{S^T}{||S||^2} = h_{ab} + n_b \frac{S^T}{||S||^2} \\
\hat{h}_{ba} &= y_a \frac{S^T}{||S||^2} = h_{ba} + n_a \frac{S^T}{||S||^2} \\
\hat{h}_{ae} &= y_e \frac{S^T}{||S||^2} = h_{ae} + n_e \frac{S^T}{||S||^2}
\end{aligned} \tag{5}$$

Note that $\hat{h}_{ab}$ is a zero mean Gaussian random variable with variance ${\sigma_1}^2 + \frac{{\sigma_0}^2}{||S||^2}$, and similarly $\hat{h}_{ba}$ and $\hat{h}_{ae}$ are zero mean Gaussian random variable with variance ${\sigma_1}^2 + \frac{{\sigma_0}^2}{||S||^2}$. Assuming that the transmission power is P and the length of S is L. We have $||S||^2 = PL$. And the SNR of the channel is

$$\gamma = \frac{P{\sigma_1}^2}{{\sigma_0}^2} \tag{6}$$

Then the SNR of ZF estimation is

$$\hat{\gamma} = {\sigma_1}^2 / \frac{{\sigma_0}^2}{||S||^2} = {\sigma_1}^2 / \frac{{\sigma_0}^2}{PL} = L\gamma \tag{7}$$

Because $\hat{h}_{ab}$, $\hat{h}_{ba}$ and $\hat{h}_{ae}$ are complex Gaussian variable, they can be expressed as

$$\begin{aligned}
\hat{h}_{ab} &= A_{ab}e^{j\varphi_{ab}} \\
\hat{h}_{ba} &= A_{ba}e^{j\varphi_{ba}} \\
\hat{h}_{ae} &= A_{ae}e^{j\varphi_{ae}}
\end{aligned} \tag{8}$$

where A_{ab} and φ_{ab} are the amplitude and phase of $\hat{h}_{ab}$, respectively.

B. PROBLEM PROPOSING

This paper design a quantization algorithm with the correlated eavesdropping channel based on the channel phase information (CPI). It is because the CPI has the characteristics of easy estimation and convenient quantization, most key generation schemes are designed based on CPI. However, the existing research on key generation with eavesdropping channel only analyzes the key capacity based on channel CSI, but has not studied the key capacity of RSSI, CPI and other information. In order to provide important reference for the quantization algorithm, the key capacity of the CPI with correlated eavesdropping channel is analyzed in this section.

Before analyzing the key capacity of CPI with correlated eavesdropping channel, we first introduce the key capacity of CPI which eavesdropping channel is unconsidered. In [16], the joint probability density function (PDF) of the uplink and downlink channel phases is solved by using the Jacobian determinant, and further determining the key capacity of channel phase in the narrowband channel. The joint PDF of the channel phase is

$$\begin{aligned}
f_{\rho_{ab}}(\varphi_{ab}, \varphi_{ba}) &= \frac{{D_{ab}}^{\frac{1}{2}}\left[\left(1-{\beta_{ab}}^2\right)^{\frac{1}{2}} + \beta_{ab}\left(\pi - \cos^{-1}\beta_{ab}\right)\right]}{4\pi^2{\sigma_s}^4(1-{\beta_{ab}}^2)^{\frac{3}{2}}} \\
\beta_{ab} &= \frac{\rho_{ab}\hat{\gamma}\cos(\varphi_{ab}-\varphi_{ba})}{2{\sigma_s}^4} \\
D_{ab} &= \left[{\sigma_s}^4 - \left(\left(\rho_{ab}\hat{\gamma}\right)/2\right)^2\right]^2
\end{aligned} \tag{9}$$

where ${\sigma_s}^2$ denote the variance of channel phase and ${\sigma_s}^2 = \frac{\hat{\gamma}+1}{2}{\sigma_0}^2$.

We further derive the key capacity $C_{ab}(\rho_{ab}, \hat{\gamma})$ between the φ_{ab} and φ_{ba}, because the $C_{ab}(\rho_{ab}, \hat{\gamma})$ is not considered in the eavesdropping channel correlation, which is referred to herein as the legitimate channel key capacity.

$$\begin{aligned}
&C_{ab}(\rho_{ab}, \hat{\gamma}) \\
&= I(\varphi_{ab}, \varphi_{ba}) \\
&= \iint_{\varphi_{ab}\varphi_{ba}} f_{\rho_{ab}}(\varphi_{ab}, \varphi_{ba}) log \frac{f_{\rho_{ab}}(\varphi_{ab}, \varphi_{ba})}{h(\varphi_{ab})h(\varphi_{ba})} d\varphi_{ab} d\varphi_{ba}
\end{aligned} \tag{10}$$

where $h(\varphi_{ab})$ and $h(\varphi_{ba})$ are marginal density functions of φ_{ab} and φ_{ba}, respectively. According to the nature of the complex Gaussian distribution variable, φ_{ab} and φ_{ba} are subject uniform distribution, and their marginal density functions are both expressed as $h(\varphi_{ab}) = h(\varphi_{ba}) = \frac{1}{2\pi}$.

Similarly, according to $\rho_{ae}(d)$, the joint PDF and mutual information between $h(\varphi_{ab})$ and $h(\varphi_{ae})$ can be obtained as

$$\begin{aligned}
&f_{\rho_{ae}}(\varphi_{ab}, \varphi_{ae}) \\
&\quad = \frac{{D_{ae}}^{\frac{1}{2}}\left[\left(1-{\beta_{ae}}^2\right)^{\frac{1}{2}} + \beta_{ae}\left(\pi - \cos^{-1}\beta_{ae}\right)\right]}{4\pi^2{\sigma_s}^4(1-{\beta_{ae}}^2)^{\frac{3}{2}}} \\
&\beta_{ae} = \frac{\rho_{ae}(d)\hat{\gamma}\cos(\varphi_{ab}-\varphi_{ae})}{2{\sigma_s}^4} \\
&D_{ae} = \left[{\sigma_s}^4 - \left(\left(\rho_{ae}\hat{\gamma}\right)/2\right)^2\right]^2 \\
&C_{ae}(\rho_{ae}(d), \hat{\gamma}) \\
&\quad = I(\varphi_{ab}, \varphi_{ae}) \\
&\quad = \iint_{\varphi_{ae}\varphi_{ab}} f_{\rho_{ae}}(\varphi_{ae}, \varphi_{ab}) log(4\pi f_{\rho_{ae}}(\varphi_{ae}, \varphi_{ab})) d\varphi_{ae} d\varphi_{ab}
\end{aligned} \tag{11}$$

where C_{ae} is the key capacity that is leaked to Eve, called the eavesdropping key capacity.

According to the conclusion in [15], the key capacity with correlated eavesdropping channel can be derived from (10) and (11) as

$$\begin{aligned}
C_{ab|e}(\rho_{ab}, \rho_{ae}(d), \hat{\gamma}) &= I(\varphi_{ab}, \varphi_{ba}\,|\varphi_{ae}) \\
&= C_{ab}(\rho_{ab}, \hat{\gamma}) - C_{ae}(\rho_{ae}(d), \hat{\gamma})
\end{aligned} \tag{12}$$

The effects of $\rho_{ae}(d)$ on key capacity are shown in Fig. 2. It can be seen from the figure that the key capacity is affected

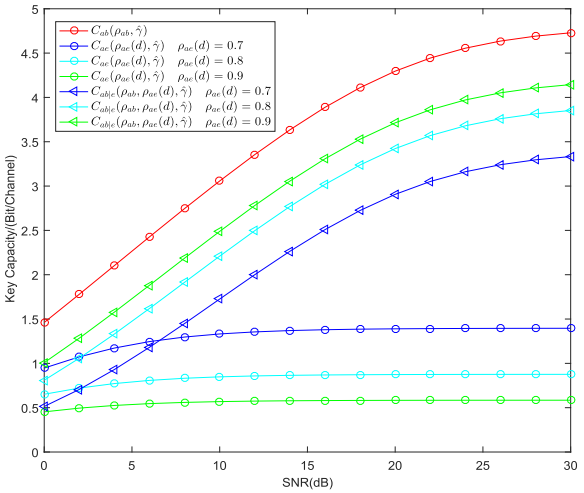


FIGURE 2. Key capacity change versus SNR γ. $\rho_{ae}(d) = 0.7, 0.8, 0.9$.

by the eavesdropping channel correlation. However, according to the assumptions of this paper, the system still is part of key capacity of security. Then we design a quantization algorithm discards the CPI eavesdropped by Eve and retains the CPI that only be extracted by Alice and Bob.

III. TWO-LAYER SECURE QUANTIZATION SCHEME

In this section, we describe the TLS quantization algorithm. First, we present the TLS quantization algorithm in detail. Then we prove the validity of our algorithm and evaluate its performance.

A. DESCRIPTION

The φ_{ae} is correlated with φ_{ab} and φ_{ba} when eavesdropping channel is correlated with legitimate channel. However, there is high probability that φ_{ab} and φ_{ba} are closer than φ_{ab} and φ_{ae}, due to $\rho_{ab} > \rho_{ae}(d)$. We propose to quantize φ_{ab} and φ_{ba} in the same interval without φ_{ae}, and the details of the algorithm as follow

1) Before transmission, Alice and Bob confirm the security distance d which means the closest distance between Eve and legitimate users. We write the d as
$$d = \min[d_1, d_2] \tag{13}$$
where d_1 and d_2 denote the security distance of Alice and Bob, respectively.
2) Both Alice and Bob send the pilot sequence to each other, then they estimate their respective CPI φ_{ab}, φ_{ba}, SNR $\hat{\gamma}$ and channel correlation ρ_{ab}.
3) Alice and Bob set two quantization levels L_1 and L_2. They first quantize φ_{ab}, φ_{ba} with quantization level L_1, which is called first layer quantization, and gets the bit sequences $\hat{X}_{L_1}$, $\hat{Y}_{L_1}$ and the remainders $\bar{\varphi}_{ab}^{L_1}$, $\bar{\varphi}_{ba}^{L_1}$.
$$\begin{aligned}\varphi_{ab} &= \hat{X}_{L_1}\frac{2\pi}{L_1} + \bar{\varphi}_{ab}^{L_1}(\hat{X}_{L_1} \in 0, 1, \cdots, L_1 - 1)\\ \varphi_{ba} &= \hat{Y}_{L_1}\frac{2\pi}{L_1} + \bar{\varphi}_{ba}^{L_1}(\hat{Y}_{L_1} \in 0, 1, \cdots, L_1 - 1)\end{aligned} \tag{14}$$
4) Then Alice and Bob quantize $\bar{\varphi}_{ab}^{L_1}$ and $\bar{\varphi}_{ba}^{L_1}$ with quantization level L_2, which is called second layer quantization, and gets the bit sequences $\hat{X}_{L_2}$, $\hat{Y}_{L_2}$.
$$\begin{aligned}\hat{X}_{L_2} &= \left[\frac{\bar{\varphi}_{ab}^{L_1}2\pi}{L_1L_2}\right](\hat{X}_{L_2} \in 0, 1, \cdots, L_2 - 1)\\ \hat{Y}_{L_2} &= \left[\frac{\bar{\varphi}_{ba}^{L_1}2\pi}{L_1L_2}\right](\hat{Y}_{L_2} \in 0, 1, \cdots, L_2 - 1)\end{aligned} \tag{15}$$
5) The 2, 3, and 4 are repeated until the length of $\hat{X}_{L_2}$ and $\hat{Y}_{L_2}$ are equal to the secret key length (fixed at 128, 256 bits, or more).
6) Alice sends the CPI estimates $\hat{X}_{L_1} = \left[\hat{X}_{L_1}(0), \hat{X}_{L_1}(1), \cdots, \hat{X}_{L_1}(K)\right]$ to Bob, where $\hat{X}_{L_1}(k)$ is the k-th ($k \in \{0, 1, \ldots, K\}$) quantization sequence and it is similar to $\hat{Y}_{L_1}(k)$, $\hat{X}_{L_2}(k)$ and $\hat{Y}_{L_2}(k)$.
7) Bob compares $\hat{X}_{L_1}$ with $\hat{Y}_{L_1}$ to find the position of disagreement sequence and discard corresponding sequence in $\hat{Y}_{L_2}$. Then Bob sends the positions to Alice.
8) Alice eliminates the corresponding sequence in $\hat{X}_{L_2}$.

B. VALIDITY OF ALGORITHM

In this section, we use the bit disagree ratio (BDR) to analyze the secure of first layer sequence and second layer sequence, and prove the TLS quantization algorithm is valid to deteriorate eavesdropper.

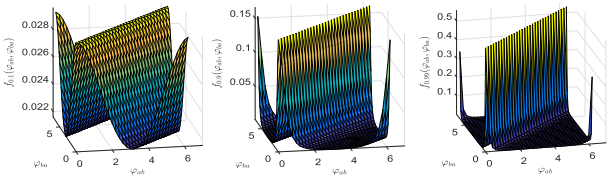


FIGURE 3. Joint PDF of φ_{ab} and φ_{ba} with correlation coefficients $\rho_{ab} = 0.1, 0.9, 0.99$.

As the analysis in Section II, that channel correlation and SNR are the two main factors affecting key capacity. Because we assume that Alice, Bob and Eve have the same environmental SNR, then the advantage of Alice and Bob is that the their channel correlation is higher than Eve. As shown in Figure 3, the surface plot of the CPI joint PDF with 0.1, 0.9 and 0.99 correlation coefficients, respectively. It can be observed from the Figure 3 that the phase combinations $(\varphi_{ab}, \varphi_{ba})$ located near the function $\varphi_{ab} = \varphi_{ba}$ is more possible if correlation coefficient is high. And the $(\varphi_{ab}, \varphi_{ba})$ located over the entire plane is more possible if correlation coefficient is low.

Since φ_{ab}, φ_{ba} and φ_{ae} are uniformly distributed over the $[0, 2\pi)$, we use uniform quantization algorithm to extract secret bit, and take the 2-bit uniform quantization algorithm as an example for analysis which shown in Table 1. We denote b_1 and b_2 as the high bit and the low bit of the 2-bit uniform quantization algorithm, and draw the quantization area of b_1 and b_2 as Fig.4 according to Table 1. The quantified results between Alice and Bob are bits disagreement when $(\varphi_{ab}, \varphi_{ba})$

TABLE 1. Example 2-bit quantization.

Bin i	Sequence b_1	b_2	Interval of φ_{ab},φ_{ba}
1	0	0	$(0, \pi/2]$
2	0	1	$(\pi/2, \pi]$
3	1	0	$(\pi, 3\pi/2]$
4	1	1	$(3\pi/2, 2\pi]$

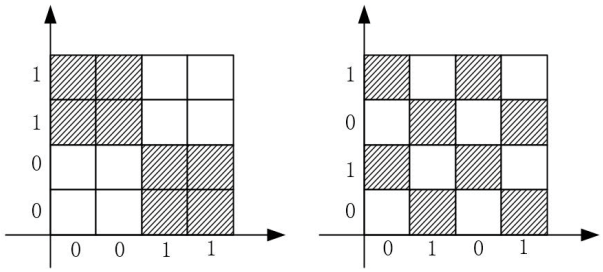


FIGURE 4. The quantization area of b_1 and b_2.

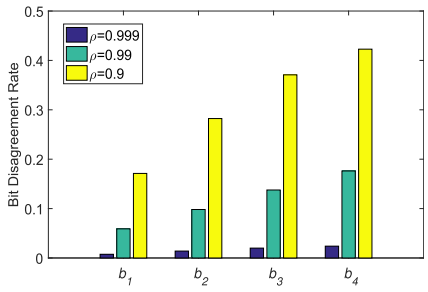


FIGURE 5. BDR of different bits in 4-bit unique quantization algorithm with 0.9, 0.99, 0.999 correlation coefficients.

located in shaded area. If we refer to the of b_1 and b_2 as A_1 and A_2, then the BDR of b_1 and b_2, denoting P_{D1} and P_{D2}, are

$$P_{D1} = \iint_{A1} f_1(\varphi_{ab}, \varphi_{ba}) d\varphi_{ab} d\varphi_{ba}$$
$$P_{D2} = \iint_{A2} f_1(\varphi_{ab}, \varphi_{ba}) d\varphi_{ab} d\varphi_{ba} \quad (16)$$

It is obviously the P_{D1} is lower than P_{D1}, and we can conclude that b_2 is more susceptible to eavesdropping than b_1. Similarly, the BDR of first layer sequences are higher than the BDR of second layer sequences, and the second layer sequences are more difficult to wiretap for the eavesdropper. Even if the BDR of second layer sequences are higher for legitimate users, as long as they are below a certain threshold, we can remove the disagreement bits through the information reconciliation process to generate the same secret key. Fig.5 shows the BDR of different bits in 4-bit unique quantization algorithm with 0.9, 0.99, 0.999 correlation coefficients and confirms our analysis.

C. ALGORITHM PERFORMANCE EVALUATION

The TLS quantization algorithm has been proposed in Section III. A, but how to select the appropriate L_1 and L_2 in different correlations and SNR is still a problem. In this section, we evaluate the performance of algorithms with different quantization levels through three performance parameters, and provide reference for TLS quantization algorithm.

1) KEY RATE

In TLS quantization algorithm, Alice and Bob extract the key from $\bar{\varphi}_{ab}^{L_1}$ and $\bar{\varphi}_{ba}^{L_1}$, and we denote their joint probability density function is $g_{\rho_{ab}}(\bar{\varphi}_{ab}^{L_1}, \bar{\varphi}_{ba}^{L_1})$. There is a many-to-one mapping between $\varphi_{ab}, \varphi_{ba}$ and $\bar{\varphi}_{ab}^{L_1}, \bar{\varphi}_{ba}^{L_1}$, so the $g_{\rho_{ab}}(\bar{\varphi}_{ab}^{L_1}, \bar{\varphi}_{ba}^{L_1})$ can be calculated by (11) as

$$g_{\rho_{ab}}(\bar{\varphi}_{ab}^{L_1}, \bar{\varphi}_{ba}^{L_1}) = \sum_{j=0}^{L_1-1} \sum_{i=0}^{L_1-1} f_{\rho_{ab}}(\varphi_{ab} + \frac{2\pi i}{L_1}, \varphi_{ba} + \frac{2\pi j}{L_1}) \quad (17)$$

Then we write the joint PDF of $\hat{X}_{L_2}$ and $\hat{Y}_{L_2}$ as

$$p_{\hat{X}_{L_2}\hat{Y}_{L_2}}(x_m, y_l) = P_{\hat{X}_{L_2}\hat{Y}_{L_2}}(\hat{X}_{L_2} = x_m, \hat{Y}_{L_2} = y_l)$$
$$= \int_{\frac{2\pi(l-1)}{L_1L_2}}^{\frac{2\pi l}{L_1L_2}} \int_{\frac{2\pi(m-1)}{L_1L_2}}^{\frac{2\pi m}{L_1L_2}} g_{\rho_{ab}}(\bar{\varphi}_{ab}^{L_1}, \bar{\varphi}_{ba}^{L_1}) d\bar{\varphi}_{ab}^{L_1} d\bar{\varphi}_{ba}^{L_1}$$
$$(m, l \in 1, 2, \ldots, L_2) \quad (18)$$

and the achievable key rate $R_{ab}(\rho_{ab}, \hat{\gamma})$ is

$$R_{ab}(\rho_{ab}, \hat{\gamma}, L_1, L_2) = I(\hat{X}_{L_2}; \hat{Y}_{L_2})$$
$$= \sum_{l=0}^{L_2} \sum_{m=0}^{L_2} p_{\hat{X}_{L_2}\hat{Y}_{L_2}}(x_m, y_l) \log \frac{p_{\hat{X}_{L_2}\hat{Y}_{L_2}}(x_m, y_l)}{p_{\hat{X}_{L_2}}(x_m) p_{\hat{Y}_{L_2}}(y_l)} \quad (19)$$

Since the key negotiation information is transmitted on the channel, the quantization algorithm and the quantization levels are also publicized to Eve, so Eve can also use the TLS quantization algorithm to obtain the sequence $\hat{Y}_{Z_2}$. Similarly, we can write the eavesdropping key rate as

$$R_{ae}(\rho_{ae}(d), \hat{\gamma}, L_1, L_2)$$
$$= I(\hat{Y}_{L_2}; \hat{Z}_{L_2})$$
$$= \sum_{l=0}^{L_2} \sum_{m=0}^{L_2} p_{\hat{Y}_{L_2}\hat{Z}_{L_2}}(y_m, z_l) \log \frac{p_{\hat{Y}_{L_2}\hat{Z}_{L_2}}(y_m, z_l)}{p_{\hat{Y}_{L_2}}(y_m) p_{\hat{Z}_{L_2}}(z_l)} \quad (20)$$

where the

$$P_{\hat{Y}_{L_2}\hat{Z}_{L_2}}(\hat{Y}_{L_2} = y_m, \hat{Z}_{L_2} = z_l)$$
$$= p_{\hat{Y}_{L_2}\hat{Z}_{L_2}}(y_m, z_l)$$
$$= \int_{\frac{2\pi(l-1)}{L_1L_2}}^{\frac{2\pi l}{L_1L_2}} \int_{\frac{2\pi(m-1)}{L_1L_2}}^{\frac{2\pi m}{L_1L_2}} g_{ae}(\bar{\varphi}_{ab}^{L_1}, \bar{\varphi}_{ae}^{L_1}) d\bar{\varphi}_{ab}^{L_1} d\bar{\varphi}_{ae}^{L_1}$$
$$(m, l \in 1, 2, \ldots, L_2) \quad (21)$$

$$g_{ae}(\bar{\varphi}_{ab}^{L_1}, \bar{\varphi}_{ae}^{L_1})$$
$$= \sum_{j=0}^{L_1-1} \sum_{i=0}^{L_1-1} f_{ae}(\varphi_{ab} + \frac{2\pi i}{L_1}, \varphi_{ae} + \frac{2\pi j}{L_1}) \quad (22)$$

Similar to (12), we derive the key rate of TLS quantization algorithm as

$$R_{TLS}(\rho_{ab}, \rho_{ae}(d), \hat{\gamma}, L_1, L_2)$$
$$= R_{ab}(\rho_{ab}, \hat{\gamma}, L_1, L_2) - R_{ae}(\rho_{ae}(d), \hat{\gamma}, L_1, L_2)$$
$$= I(\hat{X}_{L_2}; \hat{Y}_{L_2}) - I(\hat{Y}_{L_2}; \hat{Z}_{L_2}) \quad (23)$$

2) ALICE-BOB BIT DISAGREEMENT RATIO AND BOB-EVE BIT DISAGREEMENT RATIO

In most related work, the BDR of initial bit is also a parameter to evaluate the performance of the quantization. The high BDR between Alice and Bob indicates that the quantization method is more susceptible to random channel noise. Meanwhile, the low BDR between Bob and Eve indicates the quantization is susceptible to eavesdropper. We denote the P_{ab} and P_{ae} as Alice-Bob BDR and Bob-Eve BDR, respectively.

$$P_{ab}(\rho_{ab}, \hat{\gamma}, L_1, L_2) = \frac{1}{\lceil \log L_2 \rceil + 1} \sum_{l=1}^{L_2} \sum_{m=1}^{L_2} p_{\hat{X}_{L_2}\hat{Y}_{L_2}}(x_m, y_l) T_{ml} \tag{24}$$

$$P_{ae}(\rho_{ae}(d), \hat{\gamma}, L_1, L_2) = \frac{1}{\lceil \log L_2 \rceil + 1} \sum_{l=1}^{L_2} \sum_{m=1}^{L_2} p_{\hat{Y}_{L_2}\hat{Z}_{L_2}}(y_m, z_l) T_{ml} \tag{25}$$

where T_{ml} is the number of error bits when sequence x_m is observed by Alice but sequence z_l is observed by Bob. Defining the distance between the m and the l as

$$d_{ml} = \min\left[\, |m-l|\,, L_2 - |m-l|\,\right] \tag{26}$$

where $d_{ml} = \min[.,.]$ chooses the smaller number, the T_{ml} can be expressed in terms of d_{ml} as

$$T_{ml} \begin{cases} d_{mn}, & if \;\; d_{ml} = 0, 1, 2 \\ 2, & if \;\; d_{ml} = 4, 8 \\ 1, & if \;\; d_{ml} = 3 \;\; and \;\; s_{ml} = 5 + 4k \\ 3, & if \;\; d_{ml} = 3 \;\; and \;\; s_{ml} \neq 5 + 4k \\ 1, & if \;\; d_{ml} = 5, 7 \;\; and \;\; s_{ml} = 9 + 8k \\ 3, & if \;\; d_{ml} = 5, 7 \;\; and \;\; s_{ml} \neq 9 + 8k \\ 2, & if \;\; d_{ml} = 6 \;\; and \\ & \quad (s_{ml} = 8 + 8k \;\; or \;\; s_{ml} = 10 + 8k) \\ 4, & if \;\; d_{ml} = 6 \;\; and \\ & \quad (s_{ml} \neq 8 + 8k \;\; and \;\; s_{ml} \neq 10 + 8k) \end{cases} \tag{27}$$

where $s_{ml} = m + l$, and k is a positive integer.

From the analysis of (23), it can be seen that there is a negative correlation between the number of quantization levels and BDR. Increasing L_1 or L_2 will result in a decrease in BDR.

D. QUANTIZATION LEVELS CALCULATION

Because there is a trade-off between key rate and bit error rate, it is impossible to find the optimal solution for these three performance indicators at the same time. Therefore, we set the key rate threshold R_1 as well as the eavesdropping rate key threshold R_{Eve}, and calculate the quantization level that minimizes the BDR under the condition that the key rate is higher than R_1 and the eavesdropping key rate is lower than R_{Eve}. The following steps describe in details of the algorithm:

1) Alice and Bob confirm the value of ρ_{ab}, $\rho_{ae}(d)$, $\hat{\gamma}$, R_1, R_{Eve}.
2) Input $L_1 = 2$.
3) Calculating the $I(\hat{X}_{L_1}; \hat{Y}_{L_1})$ and $I(\hat{X}_{L_2}; \hat{Y}_{L_2})$ when $L_2 = 2, 3, \cdots, k$ in turn, until the conditions in Eq.(28) are satisfied. Output the quantization levels L_1, L_2.

$$\begin{aligned} I(\hat{X}_{L_2}; \hat{Y}_{L_2}) &\geq R_1 \\ I(\hat{X}_{L_2}; \hat{Z}_{L_2}) &\leq R_{Eve} \end{aligned} \tag{28}$$

   If condition 1 is satisfied when condition 2 is unsatisfied, Stop the calculation and go to the next step.
4) Alice and Bob adjust the $L_1 = L_1 + 1$.
5) The steps of 3 and 4 are repeated until the quantization levels are outputed.

IV. SIMULATION RESULTS

In this section, we prepare the performances of TLS quantization algorithms with Multi-bit Adaptive Quantization (MAQ) in [17] and 4-bit, 1-bit unique quantization through simulation. We carry out the Monte Carlo simulations to demonstrate the effectiveness of theoretical analysis, and repeat 50000 times for each simulation.

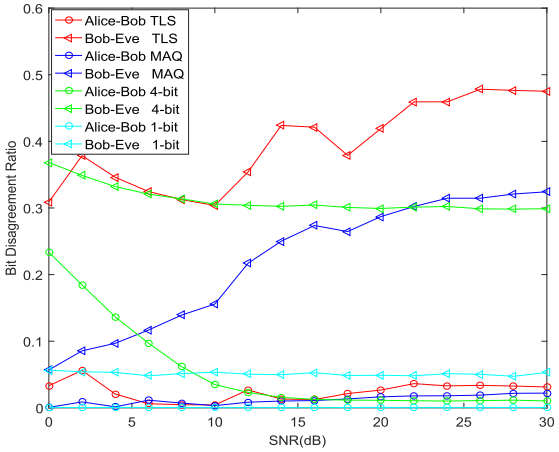


FIGURE 6. Bit Disagreement Rate of different quantization versus SNR. $\rho_{ab} = 0.999$, $\rho_{ae}(d) = 0.9$.

Fig. 6 shows a comparison of the Alice-Bob and Eve-Bob BDR between different quantization algorithms under the same channel conditions. It can be seen from the figure that the TLS quantization algorithm can effectively improve the Bob-Eve BDR and Alice-Bob BDR remaining below 0.05. The Bob-Eve BDR is close to 0.5 in high SNR, which ensures the security of the second layer sequence. Both Alice-Bob BDR and Eve-Bob BDR of 1-bit unique quantization are low, and their probability of eavesdropping is higher than other quantization algorithms. The Alice-Bob BDR of 4-bit unique quantization is so high in low SNR that error bit correction is difficult. The TLS and MAQ algorithm both dynamically change the quantization levels, but MAQ cannot classify CPI according to $\rho_{ae}(d)$ so that Bob-Eve BDR of MAQ is lower than our algorithm.

Fig. 7 shows a comparison of the key rate of different quantization algorithms under the same conditions. It can be

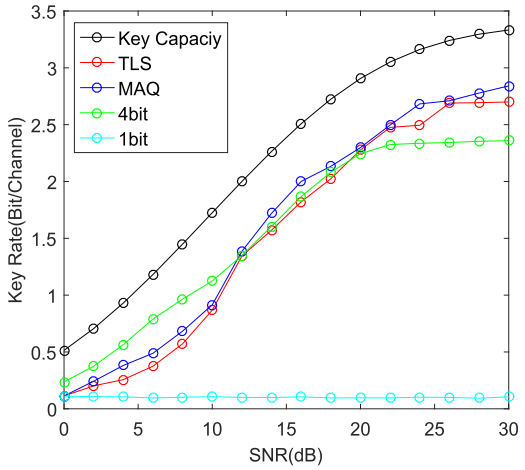


FIGURE 7. Key Rate of different quantization versus SNR. $\rho_{ab}(d) = 0.999$, $\rho_{ae}(d) = 0.9$.

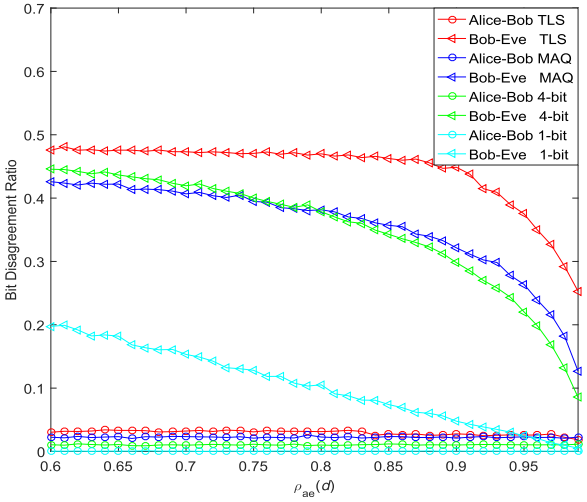


FIGURE 8. Bit Disagreement Rate of different quantization versus $\rho_{ab}(d)$. $\rho_{ab} = 0.999$, $\gamma = 30dB$.

observed from the figure that TLS quantization algorithm has a lower key rate than the MAQ because the part of key rate is discarded in the first layer sequence, but the secure performance is improved. The key rate of 1-bit unique quantization decreases only a little with the increase of SNR for the eavesdropper estimating CPI more accurately. And the rate of 4-bit unique quantization approaches the upper bound when $\gamma = 20dB$ its fixed quantization level.

Fig. 8 shows the relationship between the Alice-Bob BDR, Eve-Bob BDR and the eavesdropping channel correlation coefficient. It can be seen from the figure that the TLS quantization algorithm has significantly improved security in different eavesdropping channel correlation coefficients. However, as the correlation of eavesdropping channel is improved, the Eve-Bob BDR is also reduced, and the security of the key cannot be fully guaranteed. The MAQ algorithm, 1-bit and 4-bit unique quantization algorithm do not consider the eavesdropping channel correlation, so the Alice-Bob BDR remains unchanged in the same ρ_{ab} and γ. While TLS quantization algorithm changes the quantization levels as the eavesdropping channel correlation coefficient, the Alice-Bob BDR is reduced nearby $\rho_{ae}(d) = 0.83$.

V. CONCLUSION

This paper proposes the TLS quantization algorithm for the problem of secret key security decrease when eavesdropping channel is correlated with legitimate channel. The algorithm quantizes the channel phase and divides it into two layers of bit sequences according to the probability of eavesdropping. Then we use the first layer sequence which has higher probability of eavesdropping as error checking information to transmit on the public channel, and use the second layer sequence to generate secret key after information reconciliation and privacy amplification. The simulation verifies that the TLS presents better performance for key generation with correlated eavesdropping channel.

REFERENCES

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1550–1573, 3rd Quart., 2014.

[2] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[3] 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.

[4] 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.

[5] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag. (EuCAP)*, Berlin, Germany, Mar. 2009, pp. 1499–1503.

[6] C. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Proc. Workshop Wireless Commun. Secur. Phys. Layer*, Coimbra, Portugal, Jul. 2015, pp. 267–272.

[7] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, 1993, pp. 410–423.

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

[9] X. He, H. Dai, Y. Huang, D. Wang, W. Shen, and P. Ning, "The security of link signature: A view from channel models," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, San Francisco, CA, USA, Oct. 2014, pp. 103–108.

[10] X. He, H. Dai, W. Shen, P. Ning, and R. Dutta, "Toward proper guard zones for link signature," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2104–2117, Mar. 2016.

[11] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction?" in *Proc. 4th Eur. Workshop Syst. Secur.*, Salzburg, Austria, Apr. 2011, pp. 8-1–8-6.

[12] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in *Proc. 32nd IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Turin, Italy, Apr. 2013, pp. 200–204.

[13] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "The effect of eavesdropper's statistics in experimental wireless secret-key generation," *Comput. Sci.*, Dec. 2013.

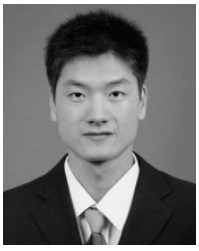
[14] T.-H. Chou, A. M. Sayeed, and S. C. Draper, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. Int. Symp. Inf. Theory*, Jun. 2010, pp. 2518–2522.

[15] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the key generation from correlated wireless channels," *IEEE Commun. Lett.*, vol. 21, no. 4, pp. 961–964, Apr. 2017.

[16] W. Cai and S. Zhang, "Research on secret key capacity based on phase of received signals in narrowband channel," *Comput. Eng.*, vol. 40, no. 7, pp. 118–122, Jul. 2014.
[17] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

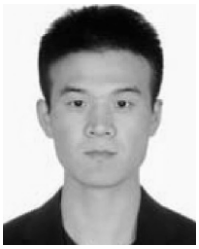
HENGLEI JIN received the B.E. degree from Sichuan University. He is currently pursuing the Ph.D. degree with National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China. His research interests include wireless communication security and secret key generation.

KAIZHI HUANG received the B.E. degree in digital communication and the M.S. degree in communication and information system from National Digital Switching System Engineering & Technological Research Center (NDSC), in 1995 and 1998, respectively, and the Ph.D. degree in communication and information system from Tsinghua University, Beijing, China, in 2003. She has been a Faculty Member of NDSC, since 1998, where she is currently a Professor and the Director of the Laboratory of Mobile Communication Networks. Her research interests include wireless network security and signal processing.



SHUAIFANG XIAO received the B.S. degree in electronic science and technology from Tsinghua University, Beijing, China, in 2011, and the Ph.D. degree in information and communication engineering with National Digital Switching System Engineering & Technological Research Center (NDSC), Zhengzhou, China, in 2018. He is currently a Research Associate with NDSC. His research interests include wireless physical layer security, cooperative communications, and the Internet of things.

YANGMING LOU received the master's degree from National Digital Switching System Engineer & Technological Research Center, Zhengzhou, in 2016. His research interests include wireless communication security and secret key generation.



XIAOMING XU received the B.S. degree in communication engineering from the College of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2011. He is currently an Instructor of the Laboratory of Mobile Communication Networks, National Digital Switching System Engineer & Technological Research Center. His research interests include stochastic geometry, cooperative communications, and physical-layer security of wireless communications.

YAJUN CHEN received the B.E. degree from University of Electronic Science and Technology of China and the Ph.D. degree from National Digital Switching System Engineer & Technological Research Center (NDSC). He is currently an Instructor of the Laboratory of Mobile Communication Networks, NDSC. His research interests include stochastic geometry, D2D communications, and the physical-layer security of wireless communications.