IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 14, 2020, accepted March 3, 2020, date of publication March 9, 2020, date of current version March 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2979515

Physical Layer Key Generation Scheme Through Scrambling the Correlated Eavesdropping Channel

YAJUN CHEN, KAIZHI HUANG, YOU ZHOU, KEMING MA, HENGLEI JIN, AND XIAOMING XU

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 61701538, Grant 61871404, and Grant 61801435, and in part by the National Key Research and Development Program of China under Grant 2017YFB0801903.

ABSTRACT In this paper, we investigate the physical layer key generation scheme in most realistic scenarios where the correlation between the legitimate channel and the eavesdropping channel is considered. To degrade the correlation and improve the key generation capacity, a physical layer key generation scheme through scrambling the correlated eavesdropping channel is proposed. Firstly, the artificial noise is sent superimposed over pilots from the legitimate transmitter to confuse the eavesdropper. The artificial noise precoding matrix is randomly selected from decomposed unitary matrices orthogonal to the legitimate channel resulting in having no effect on legitimate channel. Then, the vector quantization algorithm and the winnow algorithm are respectively applied to quantize the channel characteristic and negotiate the generated random sequences to generate the final key. To further support the performance, we next present a power optimization scheme allocated to sending the artificial noise to maximize the generated key capacity under the total transmission power constraint. Finally, simulation results are presented to validate the effectiveness of our proposed scheme.

INDEX TERMS Physical layer key generation, channel correlation, eavesdropping key generation capacity, artificial noise, channel scrambling.

I. INTRODUCTION

Since the inherent openness of the transmission medium makes wireless information more vulnerable to being eavesdropped, secure communication is identified as a critical challenge facing wireless systems. To overcome this issue, physical layer security (PLS), as a remedy of traditional encryption techniques, has been recognized as a prominent component to realize secure communication by exploiting the physical characteristics of wireless channels. As an alternative approach of PLS, secret key generation (SKG) based on wireless fading channel has gained considerable attentions recently [1]–[3], due to its attractive features of lightweight, universality and information-theoretic security. On the other hand, higher speed and security are always the most concerned performance in wireless mobile communication. To greatly improve the capacity, multiple-antenna has been regarded as one of the most popular technologies in wireless networks. For multiple-antenna wireless networks, its key generation exploiting intrinsic characteristics of wireless channels has attracted significant attention and yielded substantial research.

The basic method and theoretical performance boundary of physical layer key generation in multi-antenna system were firstly proposed in [4] and two algorithms to improve the randomness of the generated keys were given. A key generation scheme based on the blind channel estimation in the multi-input multi-output(MIMO) system was proposed in [5], which could generate random keys through the blind channel estimation and quantization. A key generation scheme was proposed where the phase of channel response was quantified into multiple levels in the multi-antenna system [6]. However, due to some factors such as the lack of space scattering and mutual coupling between antennas, there will be correlation between different user channels. Furthermore, most existing schemes of physical layer key generation extracted channel

The associate editor coordinating the review of this manuscript and approving it for publication was Miguel López-Benítez.

features using public pilots, which is easy to obtain the similarly estimated channel by the eavesdroppers located nearby the legitimate receiver. Therefore, the eavesdropper will be able to extract channel features from received signals by public pilots, which will lead to decrease the key generation capacity and the security performance of physical layer generated key.

The authors in [7] analyzed the influence of the correlation between legitimate channels on physical layer generation key and derived its key capacity. However, they only considered the spatial correlation between legitimate channels but ignored the temporal correlation. To solve this weakness, the space-time correlation channel model in MIMO system was established and its key capacity was derived in [8]–[10]. Based on Kronecker model, the expression of the generated key rate was derived under the condition of legitimate channel correlation, and the optimal result of antenna power distribution was obtained in [11]. The authors gave the optimal pilot precoding under the correlation between legitimate channels in [12]. Two key generation models were proposed according to the correlation between the legitimate channel and the eavesdropping channel, and their closed key capacity expression were derived in [13]. The authors found that there was correlation even when the eavesdropper and legitimate user are located beyond the half-wavelength through experiments in the indoor environment in [14]. The influence of the correlation between the eavesdropping channel and legitimate channel was considered in [15]. Based on Rayleigh channel model, the authors gave the correlation model and analyzed the influence of

All the work in the above literature focused on establishing the key generation model and analyzing the security performance of the traditional key generation scheme. However, in most realistic scenarios, the legitimate channel and the eavesdropping channel will have the correlation when the eavesdropper locates nearby the legitimate receiver to eavesdrop the confidential information intended for legitimate users. Thus, the eavesdropper will obtain the similarly estimated channel and some same generated keys with the ones obtained by the legitimate receiver extracting channel features, which will degrade the key generation capacity of the existing schemes. However, there is no scheme designed to reduce the correlation between the eavesdropping channel and legitimate channel. To improve the key generation capacity, we must provide some schemes to degrade the correlation between the legitimate channel and the eavesdropping channel. From the existing schemes, we could know that the artificial-noise-assisted secure transmission scheme could confuse the eavesdropper, resulting in being difficult to estimate its real channel features between the legitimate transmitter. Thus, the eavesdropper will obtain the very different estimated channel from the main channel between the legitimate users even if the eavesdropper locates nearby the legitimate receiver because of the artificial noise (AN) sent from the legitimate transmitter. Hence, it will degrade the correlation of the estimated legitimate channel and the estimated eavesdropping channel to achieve higher key generation capacity.

Hence, in terms of the above problem, we investigate the physical layer key generation scheme in most realistic scenarios where the correlation between the legitimate channel and the eavesdropping channel is considered. To degrade the correlation and improve the key generation capacity, a physical layer key generation scheme through scrambling the eavesdropping channel is proposed. Firstly, the AN is sent superimposed over pilots from the legitimate transmitter to confuse the eavesdropper. The AN precoding matrix is randomly selected from the decomposed unitary matrices orthogonal to the legitimate channel. Then, the vector quantization algorithm and the winnow algorithm are respectively applied to quantize the channel characteristic and negotiate the generated random sequences to generate the final key. To further support the performance, we next present a transmission power optimization scheme to maximize the generated key capacity.[1] Finally, simulation results are presented to validate the effectiveness of our proposed scheme.

The rest of the paper is organized as follows. Section II describes the system model of the correlated eavesdropping channel and the problem in this model. Section III presents the proposed key generation algorithm. The performance is evaluated and transmission power optimization scheme is given in Section IV. Simulation results are given in Section V. Finally, some conclusions are given in Section VI.

Notations: We use the following notations in this paper. Bold letters denote matrices or vectors. We use $\mathcal{CN}\left(\mu, \sigma^2\right)$ to denote the noise following a circularly symmetric complex Gaussian with mean μ and covariance σ^2. In addition, the notation $\mathbb{E}\{\cdot\}$ denotes the mathematical expectation.

II. SYSTEM MODEL AND KEY GENERATION CAPACITY ANALYSIS

A. SYSTEM MODEL

The correlated eavesdropping channel model is shown in Figure 1, including a transmitter Alice, a legitimate receiver Bob and an eavesdropper Eve. Alice is equipped with N antennas, Bob and Eve are both respectively equipped with one antenna. It is assumed that $\boldsymbol{h}_{ij}$ indicates the channel state information(CSI) between the transmitter i and the corresponding receiver j with $1 \times N$ dimension. Every element is a complex Gaussian random variable following the distribution with $\mathcal{CN}(0, 1)$.[2] Due to the measurement time difference and Doppler frequency shift, the uplink and downlink channel features extracted at Alice and Bob are correlated, whose correlation coefficient is denoted by ρ_{ab}.

[1] In order to improve the key generation capacity, our focus in this work is how to degrade the correlation between legitime channel and the eavesdropping channel. Hence, we mainly derive the key generation capacity to characterize the performance of this system.

[2] In this paper, we assume all the channels follow an ideal AWGN (additive White Gaussian Noise) channel model same with most existing works such as [8] and [9]. But we could easily expand our idea and the derived results to other channel models in further work.

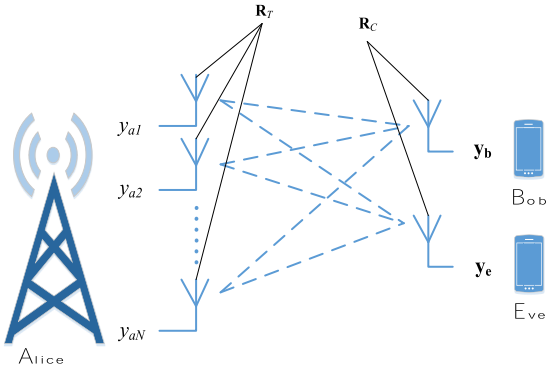


FIGURE 1. Correlation eavesdropping channel model for MISO system.

To eavesdrop the confidential information intended for Alice or Bob, Eve usually locates nearby Bob in a passive way. Hence, the eavesdropping channel and the legitimate channel is correlated. Without loss of generality, it is assumed that adjacent antennas are also correlated due to the antenna space limitation at the transmitter, the space scattering environment and other factors. According to Kronecker correlation channel model [17], we next quantitatively analyze the correlation between the transmitter and the corresponding receiver. The spatial correlation matrix of the transmitter and the receiver are respectively denoted as $\boldsymbol{R}_T$ and $\boldsymbol{R}_C$. Based on the assumption above, $\boldsymbol{R}_T$ can be expressed as:

$$\boldsymbol{R}_T = \begin{bmatrix} 1 & \rho & \rho^4 & \cdots & \rho^{(N-1)^2} \\ \rho & 1 & \rho & \cdots & \vdots \\ \rho^4 & \rho & 1 & \cdots & \rho^4 \\ \vdots & \vdots & \vdots & \ddots & \rho \\ \rho^{(N-1)^2} & \cdots & \rho^4 & \rho & 1 \end{bmatrix} \tag{1}$$

where $\rho \in [0, 1]$ denotes the correlation coefficient of the adjacent antennas.

In order to simultaneously consider the correlation between transmitter antennas, and the correlation between the eavesdropping channel and the legitimate channel, we can combine two-user MISO channels from Alice to Bob and Eve into a virtual MIMO channel. Then, the spatial correlation matrix of this virtual MIMO channel can be written as:

$$\boldsymbol{R}_C = \begin{bmatrix} 1 & \rho_{ae} \\ \rho_{ae} & 1 \end{bmatrix} \tag{2}$$

where ρ_{ae} is the correlation coefficient between the eavesdropping channel and the legitimate channel. Then, the spatial correlation matrix R is Kronecker product of $\boldsymbol{R}_C$ and $\boldsymbol{R}_T$, i.e.,

$$\boldsymbol{R} = \boldsymbol{R}_C \otimes \boldsymbol{R}_T \tag{3}$$

Then, the legitimate channel $\boldsymbol{h}_{ab}$ and the eavesdropping channel $\boldsymbol{h}_{ae}$ could be expressed as:

$$[\boldsymbol{h}_{ab}^T \boldsymbol{h}_{ae}^T] = [\tilde{\boldsymbol{h}}_{ab}^T \tilde{\boldsymbol{h}}_{ae}^T]\boldsymbol{R}^{1/2} \tag{4}$$

where $\tilde{\boldsymbol{h}}_{ab}$ and $\tilde{\boldsymbol{h}}_{ae}$ are random vectors following the same distribution with $\boldsymbol{h}_{ab}$ and $\boldsymbol{h}_{ae}$, but all random variables in $\tilde{\boldsymbol{h}}_{ab}$ and $\tilde{\boldsymbol{h}}_{ae}$ are independent to each other.

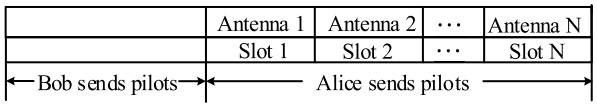


FIGURE 2. Correlation eavesdropping channel model for MISO system.

Alice, Bob and Eve estimate their corresponding channels after sending pilots to obtain their respective estimated CSI. Since Bob is only equipped a single antenna, Alice sends pilots by different antennas in different slots during a relevant time. The specific time slots allocation is shown in Figure 2.

The received signals at Alice, Bob and Eve are respectively written as:

$$\hat{\boldsymbol{h}}_a = \sqrt{P}\boldsymbol{h}_{ba}^H + \boldsymbol{n}_a \tag{5}$$

$$\hat{\boldsymbol{h}}_b = \sqrt{P}\boldsymbol{h}_{ab}^H \boldsymbol{I} + \boldsymbol{n}_b = \sqrt{P}\boldsymbol{h}_{ab}^H + \boldsymbol{n}_b \tag{6}$$

$$\hat{\boldsymbol{h}}_e = \sqrt{P}\boldsymbol{h}_{ae}^H \boldsymbol{I} + \boldsymbol{n}_e = \sqrt{P}\boldsymbol{h}_{ae}^H + \boldsymbol{n}_e \tag{7}$$

where $\boldsymbol{n}_a, \boldsymbol{n}_b$ and $\boldsymbol{n}_e$ respectively denote the additive independent complex gaussian noise at Alice, Bod and Eve with the distribution $\mathcal{CN}\left(0, {\delta_0}^2\right)$. The estimated channels for Alice, Bob and Eve can be, respectively, represented as:

$$\boldsymbol{y}_a = \boldsymbol{h}_{ba}^H + \frac{\boldsymbol{n}_a}{\sqrt{P}} \tag{8}$$

$$\boldsymbol{y}_b = \boldsymbol{h}_{ab}^H + \frac{\boldsymbol{n}_b}{\sqrt{P}} \tag{9}$$

$$\boldsymbol{y}_e = \boldsymbol{h}_{ae}^H + \frac{\boldsymbol{n}_e}{\sqrt{P}} \tag{10}$$

From the analysis above, we can get the same signal-to-noise ratio (SNR) at Alice, Bob and Eve, i.e., $\gamma = \gamma_a = \gamma_b = \gamma_e = \frac{P}{\sigma_0^2}$.

B. KEY GENERATION CAPACITY ANALYSIS

1) SYSTEM CAPACITY ANALYSIS

The key generation capacity depends on the correlation between the legitimate channel and the eavesdropping channel, which simultaneously has close relationship with the correlation of the antennas at the transmitter. According to the spatial correlation matrix $\boldsymbol{R}_C$ at the receiver and $\boldsymbol{R}_T$ at the transmitter, the system key generation capacity can be written as:

$$C_{SK} = H(\boldsymbol{y}_a \boldsymbol{y}_e) + H(\boldsymbol{y}_b \boldsymbol{y}_e) - H(\boldsymbol{y}_a \boldsymbol{y}_b \boldsymbol{y}_e) - H(\boldsymbol{y}_e) \tag{11}$$

Since $\boldsymbol{y}_a$, $\boldsymbol{y}_b$ and $\boldsymbol{y}_e$ are both N-dimensional gaussian sources, Eq.(12) could be obtained from Eq.(11) according to the definition of the entropy of the N-dimensional gaussian sources:

$$\begin{aligned} C_{SK} &= \log_2(2\pi e)^{2N} \left|\bar{\boldsymbol{V}}_{ae}\right| + \log_2(2\pi e)^{2N} \left|\bar{\boldsymbol{V}}_{be}\right| \\ &\quad - \log_2(2\pi e)^{3N} \left|\bar{\boldsymbol{V}}_{abe}\right| - \log_2(2\pi e)^{N} \left|\boldsymbol{V}_{ee}\right| \\ &= \log_2 \left|\bar{\boldsymbol{V}}_{ae}\right| + \log_2 \left|\bar{\boldsymbol{V}}_{be}\right| - \left|\bar{\boldsymbol{V}}_{abe}\right| - \left|\boldsymbol{V}_{ee}\right| \\ &= \log_2 \frac{\left|\bar{\boldsymbol{V}}_{ae}\right| \left|\bar{\boldsymbol{V}}_{be}\right|}{\left|\boldsymbol{V}_{ee}\right| \left|\bar{\boldsymbol{V}}_{abe}\right|} \end{aligned} \tag{12}$$

where $\boldsymbol{V}_{ml}$ is the covariance matrix of the vector $\boldsymbol{y}_m$ and $\boldsymbol{y}_l (m, l \in a, b, e)$, $\bar{\boldsymbol{V}}_{ml}$ is the covariance matrix of the

combined vector $\boldsymbol{y}_m\boldsymbol{y}_l$. Hence, they could be written as:

$$\boldsymbol{V}_{ml} = \mathbb{E}\{\boldsymbol{y}_l^H \boldsymbol{y}_m\} \tag{13}$$

$$\bar{\boldsymbol{V}}_{ml} = \mathbb{E}\{[\boldsymbol{y}_m\boldsymbol{y}_l]^H [\boldsymbol{y}_m\boldsymbol{y}_l]\} \tag{14}$$

According to the definition of the spatial correlation matrix $\boldsymbol{R}_T$ at the transmitter in Eq.(1) and $\boldsymbol{R}_C$ at the receiver in Eq.(2), we could obtain the following equations:

$$\boldsymbol{V}_{aa} = \boldsymbol{V}_{bb} = \boldsymbol{V}_{ee} = \boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_N \tag{15}$$

$$\bar{\boldsymbol{V}}_{ae} = \bar{\boldsymbol{V}}_{be} = \boldsymbol{R} + \frac{1}{\gamma}\boldsymbol{I}_{2N} \tag{16}$$

$$\bar{\boldsymbol{V}}_{abe} = \bar{\boldsymbol{V}}_{be} = \begin{bmatrix} 1 & \rho_{ab} & \rho_{ae} \\ \rho_{ab} & 1 & \rho_{ae} \\ \rho_{ae} & \rho_{ae} & 1 \end{bmatrix} \otimes \boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_{3N} \tag{17}$$

Substituting Eq.(15), Eq.(16) and Eq.(17) into Eq.(12), the following equation could be obtained:

$$C_{SK} = \log_2 \frac{\left|\boldsymbol{R} + \frac{1}{\gamma}\boldsymbol{I}_{2N}\right|^2}{\left|\boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_N\right| \left|\begin{bmatrix} 1 & \rho_{ab} & \rho_{ae} \\ \rho_{ab} & 1 & \rho_{ae} \\ \rho_{ae} & \rho_{ae} & 1 \end{bmatrix} \otimes \boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_{3N}\right|} \tag{18}$$

2) EAVESDROPPING KEY GENERATION CAPACITY ANALYSIS

In this paper, we also consider the eavesdropping key generation capacity in addition to the system key generation capacity, which is the upper bound of the key information that the eavesdropper eavesdrops from received signals. The eavesdropping key generation capacity indicates how much the eavesdropper eavesdrops the extracted channel features between legitimate users. That is to say, when the eavesdropping key generation capacity is high, the generated key still has great risk of being cracked even if the system key generation capacity is high. Therefore, the eavesdropping key generation capacity should be reduced as much as possible when the key generation scheme is designed. According to its definition, the eavesdropping key generation capacity could be written as:

$$\begin{aligned} C_{Eve} &= I(\boldsymbol{y}_a; \boldsymbol{y}_e) \\ &= H(\boldsymbol{y}_a) + H(\boldsymbol{y}_e) - H(\boldsymbol{y}_a\boldsymbol{y}_e) \end{aligned} \tag{19}$$

We could extend Eq.(19) to obtain the following equation according to the definition of entropy of the N-dimensional gaussian sources:

$$\begin{aligned} C_{Eve} &= \log_2(2\pi e)^N |\boldsymbol{V}_{ee}| + \log_2(2\pi e)^N |\boldsymbol{V}_{aa}| \\ &\quad - \log_2(2\pi e)^{2N} \left|\bar{\boldsymbol{V}}_{ae}\right| \\ &= \log_2 \frac{|\boldsymbol{V}_{aa}|\,|\boldsymbol{V}_{ee}|}{\left|\bar{\boldsymbol{V}}_{ae}\right|} \\ &= \log_2 \frac{\left|\boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_N\right|^2}{\left|\boldsymbol{R} + \frac{1}{\gamma}\boldsymbol{I}_{2N}\right|} \end{aligned} \tag{20}$$

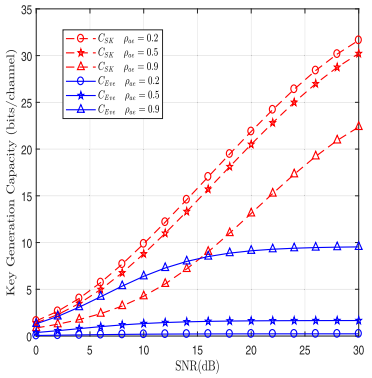


FIGURE 3. System key generation capacity C_{SK} and eavesdropping key generation capacity C_{Eve} versus SNR under different correlation coefficients ρ_{ae}.

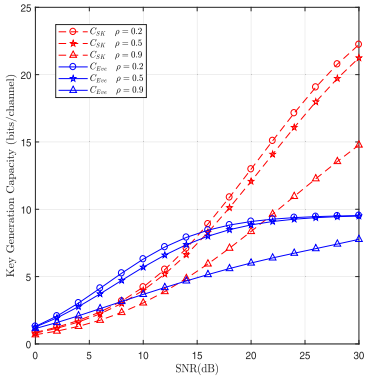


FIGURE 4. System key generation capacity C_{SK} and eavesdropping key generation capacity C_{Eve} versus SNR under different correlation coefficients ρ.

The system key generation capacity and the eavesdropping key generation capacity versus SNR is demonstrated in Figure 3 under different correlation coefficients between the eavesdropping channel and the legitimate channel. In Figure 3, the number of antenna is set as $N = 4$ and the correlation coefficient ρ_{ab} between the downlink and the uplink is 0.999, the correlation coefficient ρ between adjacent antennas is 0. From Figure 3, we can see that the key generation capacity obviously decreases when the eavesdropping channel and the legitimate channel have the correlation. C_{SK} and C_{Eve} will both increase as SNR increases. However, when the correlation coefficient ρ_{ae} approaches 1, the growing of C_{Eve} will become faster and faster, resulting in worse influence on C_{SK}.

The system key generation capacity and the eavesdropping key generation capacity versus SNR is demonstrated in Figure 4 under different correlation coefficients between adjacent antennas, where the number of antenna is set as $N = 4$, the correlation coefficient ρ_{ae} between the eavesdropping channel and the legitimate channel is 0.9. From Figure 4, we can see that the correlation between adjacent antennas could also degrade system key generation capacity, which has the same influence with the correlation between the eavesdropping channel and the legitimate channel. However, the difference is that the system key generation capacity is not zero when the correlation coefficient ρ between adjacent antennas is 1.

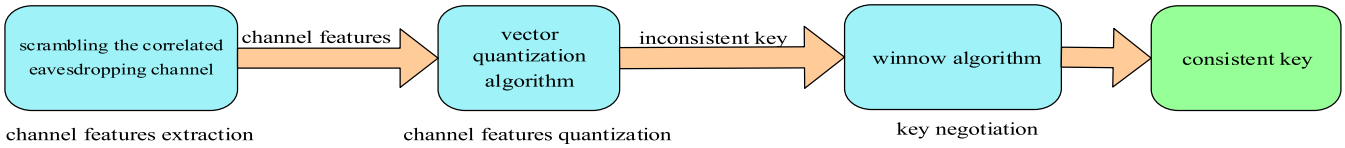


FIGURE 5. The key generation scheme through scrambling the correlated eavesdropping channel.

From the analysis above, we could come to the conclusion that the correlation between the eavesdropping channel and the legitimate channel has obvious influence on the performance of physical layer key generation capacity. From existing literature, the AN-assisted secure transmission scheme could degrade the received SNR at Eve, resulting in degrading the correlation of the estimated channel between the legitimate user and the eavesdropper to achieve higher key generation capacity. Based on the above idea, the artificial noise is superimposed over pilots within the null space of the legitimate channel. Then, the final key is obtained through the vector quantization algorithm and winnow protocol.

III. KEY GENERATION SCHEME THROUGH SCRAMBLING THE CORRELATED EAVESDROPPING CHANNEL

As shown in Figure 5, we can see that the proposed key generation scheme includes three steps such as channel features extraction, channel features quantization and random key agreement. The scrambling scheme based on the artificial-noise-assisted secure transmission scheme is proposed to degrade the correlation between the eavesdropping channel and the legitimate channel. Based on the scrambling scheme, we firstly extract channel features. Then, the vector quantization algorithm suitable for multi-correlation sources is used to quantize channel features. Furthermore, the winnow algorithm is applied to negotiate the generated key to the final consistent key.

A. CHANNEL FEATURES EXTRACTION

To degrade the correlation between the eavesdropping channel and the legitimate channel, the proposed key generation scheme through scrambling the correlated eavesdropping channel is designed based on the AN-assisted secure transmission scheme [18], [19]. To confuse the eavesdropper while having no effect on legitimate users, the artificial noise must be injected into the orthogonal space of legitimate channels. The detailed steps are listed as follow:

1) Firstly, in order to prevent Eve from obtaining the main channel features between Alice and Bob, Bob sends reverse pilots to Alice (namely, the uplink transmission from Bob to Alice) in this paper. Alice estimates the channel between Alice and Bob to obtain $\hat{\boldsymbol{y}}_a$ when it receives pilot signals from Bob;
2) Then, Alice decomposes the estimated channel $\boldsymbol{h}_{ab}^H$ by the singular value decomposition (SVD), which is denoted by $\boldsymbol{h}_{ab}^H = \boldsymbol{U}\boldsymbol{\Sigma}\boldsymbol{V}^H$. According to the matrix theory, we can know that the vectors in the right singular vector are orthogonal to $\boldsymbol{h}_{ab}^H$. In this paper, it is assumed that Alice and Bob have no information about CSI of Eve, but only know the correlation coefficient between the eavesdropping channel and the legitimate channel. Hence, the eavesdropper could not be interfered accurately by AN. However, the randomly selected AN precoding vectors orthogonal to $\boldsymbol{h}_{ab}^H$ would statistically degrade received signals at the eavesdropper. Hence, we randomly select one vector $\boldsymbol{z}$ from the right singular vector $\boldsymbol{V}^H$ as the AN precoding matrix to confuse the eavesdropper;
3) The transmission power of the AN $\boldsymbol{z}$ must hold the condition $tr(\boldsymbol{z}\boldsymbol{z}^H) \leq P_z$. Then, Alice sends pilots to Bob with the remaining power, i.e., $P_s = P - P_z$. Hence, the received signals at Bob and Eve, respectively, are written as:

$$\begin{aligned}\hat{\boldsymbol{y}}_b &= \sqrt{P - P_z}\boldsymbol{h}_{ab}^H\boldsymbol{I}_N + \sqrt{P_z}\boldsymbol{h}_{ab}^H\boldsymbol{Z} + \boldsymbol{n}_b \\ &= \sqrt{P - P_z}\boldsymbol{h}_{ab}^H + \boldsymbol{n}_b \qquad (21)\\ \hat{\boldsymbol{y}}_e &= \sqrt{P - P_z}\boldsymbol{h}_{ae}^H + \sqrt{P_z}\boldsymbol{h}_{ae}^H\boldsymbol{Z} + \boldsymbol{n}_e \qquad (22)\end{aligned}$$

where $\boldsymbol{Z}$ is a composed matrix with different vectors $\boldsymbol{z}$ when the N antennas send pilot signals. $\boldsymbol{Z} = [\boldsymbol{z}_1 \cdots \boldsymbol{z}_N]$, $\boldsymbol{z}_n$ is the selected AN precoding matrix at the n-th antenna.
4) The estimated channels can be respectively represented as:

$$\hat{\boldsymbol{y}}_b = \boldsymbol{h}_{ab}^H + \frac{\boldsymbol{n}_b}{\sqrt{P - P_z}} \qquad (23)$$

$$\hat{\boldsymbol{y}}_e = \boldsymbol{h}_{ae}^H + \frac{\sqrt{P_z}\boldsymbol{h}_{ae}^H\boldsymbol{Z}}{\sqrt{P - P_z}} + \frac{\boldsymbol{n}_e}{\sqrt{P - P_z}}. \qquad (24)$$

B. CHANNEL CHARACTERISTIC QUANTIZATION

The channel features $\hat{\boldsymbol{y}}_a$ and $\hat{\boldsymbol{y}}_b$ extracted by both Alice and Bob are vectors and variables in corresponding vectors are correlated. To overcome this issue, the vector quantization algorithm in [20], [21] is applied. Here are the basic steps and we can refer to [20], [21] for more details.

1) Alice and Bob divide $\hat{\boldsymbol{y}}_a$ and $\hat{\boldsymbol{y}}_b$ into vectors with the length n. Hence, they could be divided into $\lceil N/n \rceil$ groups;
2) The quantization region in the n-dimensional space is designed according to the length L_n of the generated key and the lower bound of key consistency rate ε in each vector group. Generally, it could be realized by the clustering algorithm according to a certain number of training sets. And the designed codeword corresponding to each quantization region will also be optimized with the objective of optimal key consistency rate;

TABLE 1. The key generation scheme through scrambling the correlated eavesdropping channel.

Step 1: Bob sends reverse pilots to Alice and Alice obtains the estimated channel $\hat{\boldsymbol{y}}_a$;
Step 2: Alice decomposes $\hat{\boldsymbol{y}}_a$ by SVD and sends the AN to Bob superposed over pilots;
Step 3: Bob could obtain the estimated channel $\hat{\boldsymbol{y}}_b$ from received signals;
Step 4: Divide $\hat{\boldsymbol{y}}_a$ and $\hat{\boldsymbol{y}}_b$ into vectors groups with length n ;
Step 5: Quantize each vectors with length n and output the keys K_A and K_B;
Step 6: Alice and Bob interweave the scrambled K_A and K_B to respectively get A_i and B_i;
Step 7: The parity bit is exchanged between Alice and Bob, and delete one bit in A_i and B_i;
Step 8: If parity bits are inconsistent, use Hamming code to correct errors in A_i and B_i;
Step 9: Repeat Step7 and Step8 until there is no error;
Step 10: Output the error corrected $K_A{}'$ and $K_B{}'$.

3) According to the Euclidean distance between vector groups and the center of the quantization region, Alice and Bob determine that which region the group will fall into and output the codeword as the generated key. After quantization, there will be some inconsistencies between the generated keys for Alice and Bob due to noise, Doppler shift and other factors. Then, the winnow algorithm is applied to negotiate the generation key.

Now we will summarize the detailed steps of the proposed scheme shown in Table 1.

IV. PERFORMANCE ANALYSIS AND OPTIMIZATION

In this section, the statistical channel features about received signals at Alice, Bob and Eve are analyzed to derive key generation capacity. What is more, to maximize the key generation capacity, the algorithm to obtain the optimal power ratio is presented under the security and power constraints.

A. PERFORMANCE ANALYSIS

From the analysis in section II-A, it can be seen that parameters affecting the key generation capacity have the spatial correlation coefficient ρ of the transmitter antennas, the correlation coefficient ρ_{ae} of the eavesdropping channel and legitimate channel, the number of the transmitter antenna N and the received SNR. The channel correlation coefficient and the number of antennas are inherent attributes which remain unchanged. Hence, the key generation capacity of the proposed scheme is mainly determined by received SNR and next the detailed analysis will be given.

In the proposed scheme, the received SNR at Alice is equal to the one without AN, which could be denoted as $\bar{\gamma}_a = \frac{P}{\sigma_0^2} = \gamma$. $P_z{=}\lambda P$ presents the allocated transmission power to generate AN and $(1{-}\lambda)\,P$ is the allocated transmission power to the pilot signals. Thus, $\lambda = \frac{P_z}{P} \in [0, 1]$ denotes the ratio of the total transmission power allocated to transmit AN and the received SNR at Bob can be simplified as $\bar{\gamma}_b = (1-\lambda)\gamma$. It is assumed that the covariance matrix $\boldsymbol{V}_{ml}^N$ is the covariance matrix between vectors $\hat{\boldsymbol{y}}_m$ and $\hat{\boldsymbol{y}}_l$, the covariance matrix $\bar{\boldsymbol{V}}_{ml}^N$ is the covariance matrix between the combined vectors $\hat{\boldsymbol{y}}_m$ and $\hat{\boldsymbol{y}}_l$. Then, we can give the following equations:

$$\boldsymbol{V}_{aa}^N = \boldsymbol{V}_{aa} = \boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_N \tag{25}$$

$$\boldsymbol{V}_{bb}^N = \boldsymbol{R}_T + \frac{1}{\gamma_b}\boldsymbol{I}_N = \boldsymbol{R}_T + \frac{1}{(1-\lambda)\gamma}\boldsymbol{I}_N \tag{26}$$

From the analysis above, we can know that the received SNR at Eve is both affected by the power of pilots and the interference caused by AN. Hence, the correlation of variables in $\hat{\boldsymbol{y}}_e$ is more complex. The covariance matrix of the received signal $\hat{\boldsymbol{y}}_e$ could be obtained through following steps:

$$\begin{aligned}
\boldsymbol{V}_{ee}^N &= \mathbb{E}\left\{\hat{\boldsymbol{y}}_e^H \hat{\boldsymbol{y}}_e\right\} \\
&= \mathbb{E}\left\{\begin{array}{l}\left[\boldsymbol{h}_{ae}^H + \frac{\sqrt{P_z}\boldsymbol{h}_{ae}^H\boldsymbol{Z}}{\sqrt{P-P_z}} + \frac{\boldsymbol{n}_e}{\sqrt{P-P_z}}\right]^H \\ \bullet\left[\boldsymbol{h}_{ae}^H + \frac{\sqrt{P_z}\boldsymbol{h}_{ae}^H\boldsymbol{Z}}{\sqrt{P-P_z}} + \frac{\boldsymbol{n}_e}{\sqrt{P-P_z}}\right]\end{array}\right\} \\
&= \mathbb{E}\left\{\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H + \frac{P_z\left(\boldsymbol{Z}^H\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H\boldsymbol{Z}\right)}{P-P_z} + \frac{\boldsymbol{n}_e^H\boldsymbol{n}_e}{P-P_z}\right\} \\
&= \boldsymbol{R}_T + \frac{P_z}{P-P_z}E\left(\boldsymbol{Z}^H\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H\boldsymbol{Z}\right) + \frac{\sigma_0^2}{P-P_z}\boldsymbol{I}_N
\end{aligned} \tag{27}$$

$\mathbb{E}\left\{\left(\boldsymbol{Z}^H\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H\boldsymbol{Z}\right)\right\}$ can be recast as:

$$\begin{aligned}
&\mathbb{E}\left\{\left(\boldsymbol{Z}^H\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H\boldsymbol{Z}\right)\right\} \\
&= [\boldsymbol{z}_1\boldsymbol{z}_2\cdots\boldsymbol{z}_N]^H\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H[\boldsymbol{z}_1\boldsymbol{z}_2\cdots\boldsymbol{z}_N] \\
&= \mathbb{E}\left[\begin{array}{cccc}
\sum_{i=1}^N\left[|z_1(i)|^2|h_{ae}(i)|^2\right] & \sum_{i=1}^N\left[|z_1(i)|\,|z_2(i)|\,|h_{ae}(i)|^2\right] & \cdots & \sum_{i=1}^N\left[|z_1(i)|\,|z_N(i)|\,|h_{ae}(i)|^2\right] \\
\sum_{i=1}^N\left[|z_2(i)|\,|z_1(i)|\,|h_{ae}(i)|^2\right] & \sum_{i=1}^N\left[|z_2(i)|^2|h_{ae}(i)|^2\right] & \cdots & \sum_{i=1}^N\left[|z_2(i)|\,|z_N(i)|\,|h_{ae}(i)|^2\right] \\
\vdots & \vdots & & \vdots \\
\sum_{i=1}^N\left[|z_N(i)|\,|z_1(i)|\,|h_{ae}(i)|^2\right] & \sum_{i=1}^N\left[|z_N(i)|\,|z_1(i)|\,|h_{ae}(i)|^2\right] & \cdots & \sum_{i=1}^N\left[|z_N(i)|^2|h_{ae}(i)|^2\right]
\end{array}\right]
\end{aligned} \tag{28}$$

where $z_1(i)$ and $h_{ae}(i)$ respectively represent the i-th element in corresponding vectors $\boldsymbol{z}_1$ and $\boldsymbol{h}_{ae}$. Since all the AN matrices are randomly selected from vectors orthogonal to $\boldsymbol{h}_{ab}^H$ and all vectors of the matrix follow the same distribution. Hence, we could further obtain:

$$\begin{aligned}
e_1 &= \mathbb{E}\left\{\sum_{i=1}^N\left[|z_1(i)|^2|h_{ae}(i)|^2\right]\right\} \\
&= \mathbb{E}\left\{\sum_{i=1}^N\left[|z_2(i)|^2|h_{ae}(i)|^2\right]\right\}
\end{aligned}$$

$$= \mathbb{E}\left\{\sum_{i=1}^{N}\left[|z_N(i)|^2|h_{ae}(i)|^2\right]\right\} \quad (29)$$

$$e_2 = \sum_{i=1}^{N}\left[z_m(i)z_n(i)|h_{ae}(i)|^2\right](m,n\in[1,N]m\neq n) \quad (30)$$

Substituting Eq.(29) and Eq.(30) into Eq.(28), we can get:

$$\mathbb{E}\left\{\left(\boldsymbol{Z}^H\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H\boldsymbol{Z}\right)\right\} = \mathbb{E}\begin{bmatrix} e_1 & e_2 & \cdots & e_2 \\ e_2 & e_1 & \cdots & e_2 \\ \vdots & \vdots & \ddots & \vdots \\ e_2 & e_2 & \cdots & e_1 \end{bmatrix} \quad (31)$$

According to Eq. (29) and Eq. (30), e_1 and e_2 could be derived as:

$$e_1 = (1-\rho_e^2)(1-\frac{\rho^2}{2}) \quad (32)$$

$$e_2 = \frac{1}{2}(1-\rho_e^2)(1-(1-\rho)^4) \quad (33)$$

Setting $\mathbb{E}\left\{\left(\boldsymbol{Z}^H\boldsymbol{h}_{ae}\boldsymbol{h}_{ae}^H\boldsymbol{Z}\right)\right\}$ as $\boldsymbol{K}$ and substituting it into Eq. (27), we will obtain:

$$\begin{aligned}\boldsymbol{V}_{ee}^N &= \mathbb{E}\left\{\hat{\boldsymbol{y}}_e^H\hat{\boldsymbol{y}}_e\right\} \\ &= \boldsymbol{R}_T + \frac{1}{1-\lambda}\boldsymbol{K} + \frac{1}{(1-\lambda)\gamma}\boldsymbol{I}_N \end{aligned} \quad (34)$$

The key generation capacity C_{SK}^N of the proposed scheme can be given by

$$\log_2 \frac{\left|\begin{bmatrix} \boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_{2N} & \rho_e\boldsymbol{R}_T \\ \rho_e\boldsymbol{R}_T & \boldsymbol{V}_{ee}^N \end{bmatrix}\right| \left|\begin{bmatrix} \boldsymbol{R}_T + \frac{1}{(1-\lambda)\gamma}\boldsymbol{I}_{2N} & \rho_e\boldsymbol{R}_T \\ \rho_e\boldsymbol{R}_T & V_{ee}^N \end{bmatrix}\right|}{\left|\boldsymbol{V}_{ee}^N\right| \left|\begin{bmatrix} \boldsymbol{R}_T + \frac{1}{\gamma}\boldsymbol{I}_N & \rho_{ab}\boldsymbol{R}_T & \rho_{ae}\boldsymbol{R}_T \\ \rho_{ab}\boldsymbol{R}_T & \frac{1}{(1-\lambda)\gamma}\boldsymbol{I}_N & \rho_{ae}\boldsymbol{R}_T \\ \rho_{ae}\boldsymbol{R}_T & \rho_{ae}\boldsymbol{R}_T & \boldsymbol{V}_{ee}^N \end{bmatrix}\right|}$$

Based on the analysis above, AN is sent superimposed over pilots from the legitimate transmitter to confuse the eavesdropper, whose precoding matrix is randomly selected from decomposed unitary matrices orthogonal to the legitimate channel resulting in having no effect on legitimate channel. Thus, Eve will obtain the very different estimated channel from the main channel between the legitimate users even if Eve locates nearby Bob. Hence, it will degrade the correlation of the estimated legitimate channel and the estimated eavesdropping channel to achieve higher key generation capacity. On the other hand, since a fraction of the transmission power will be allocated to generate AN in the proposed scheme, it will result in some power waste. However, it could improve the security performance of the considered system, which actually is our goal in this paper. Hence, in order to improve the performance of the proposed scheme as much as possible under the total transmission power constraint, we next present a power optimization scheme allocated to sending AN to maximize the generated key capacity.

TABLE 2. The iterative algorithm to obtain the optimal ratio λ.

Step1: Initialize λ, and set it as $\lambda = \sqrt{C_{Eve}/C_{SK}}$;
Step2: Solve the optimization problem in Eq. 36 and get the optimal power ratio λ^*;
Step3: Update the optimal power ratio $\lambda \leftarrow \lambda^*$;
Step4: Repeat Step2-Step3 until λ^* remains almost invariable.

B. PERFORMANCE OPTIMIZATION

From results in Section IV-A, it can be seen that when the total power and channel parameters are fixed, the AN transmission power ratio optimization problem could be formulated as:

$$\begin{aligned}\max_{\lambda} C_{SK}^N &= \log_2\left|\bar{\boldsymbol{V}}_{ae}^N\right| + \log_2\left|\bar{\boldsymbol{V}}_{be}^N\right| \\ &\quad - \log_2\left|\boldsymbol{V}_{ee}^N\right| - \log_2\left|\bar{\boldsymbol{V}}_{abe}^N\right| \\ s.t.\ 1 &\geq \lambda \geq 0, \end{aligned} \quad (35)$$

where $\left|\bar{\boldsymbol{V}}_{ae}^N\right|$, $\left|\bar{\boldsymbol{V}}_{be}^N\right|$ and $\left|\bar{\boldsymbol{V}}_{abe}^N\right|$ are diagonal matrices with λ. Hence, we only analyze the matrix $\boldsymbol{V}_{ee}^N$ and $\boldsymbol{R}_T + \frac{1}{(1-\lambda)\gamma}\boldsymbol{I}_N$ to know that the impact of the transmission power ratio λ on the key generation capacity C_{SK}^N. Next, we will analyze it according to the entropy of sources with N dimension.

It is assumed that $\boldsymbol{X} = (X_1X_2\cdots X_n)$ is uniformly distributed variables following $\mathcal{CN}\left(0,{\delta_0}^2\right)$. Then, the entropy of the source $\boldsymbol{X}$ can be expressed as:

$$H(\boldsymbol{X}) = \frac{1}{2}\log_2(2\pi e)^N|\boldsymbol{C}| \quad (36)$$

where $\boldsymbol{C}$ is the covariance matrix of $\boldsymbol{X}$ and the diagonal elements of $\boldsymbol{C}$ are all σ_0^2. $\boldsymbol{X}$ could be denoted by $\hat{\boldsymbol{X}} = (\hat{X}_1\hat{X}_2\cdots\hat{X}_n)$ because of noise, whose variance is $\sigma^2+\sigma_0^2$. But the covariance between different variables remains unchanged, then the covariance matrix could be written as $\hat{\boldsymbol{C}} = \boldsymbol{C} + \sigma_0^2\boldsymbol{I}_N$. That is to say, the entropy of each variable $(\hat{X}_1\hat{X}_2\cdots\hat{X}_n)$ in the N-dimensional gaussian source increases under the influence of noise, but the covariance between different variables remains unchanged. Hence, the joint entropy $H(\hat{\boldsymbol{X}})$ of the N-dimensional gaussian source will also increase. What is more, the larger the noise variance σ_0^2 is, the greater the entropy will be.

Then, the determinant of the matrix $\boldsymbol{R}_T + \frac{1}{(1-\lambda)\gamma}\boldsymbol{I}_N$ will gradually increase with λ increasing. That is to say, with the increase of the AN power, the entropy of the received signal $\hat{\boldsymbol{y}}_b$ at Bob will increase. Similarly, the entropy of the received signal $\hat{\boldsymbol{y}}_e$ at Eve will also increase. Hence, $\left|\bar{\boldsymbol{V}}_{ae}^N\right|$, $\left|\bar{\boldsymbol{V}}_{be}^N\right|$, $\left|\bar{\boldsymbol{V}}_{abe}^N\right|$ and $\left|\bar{\boldsymbol{V}}_{ee}^N\right|$ in Eq. (35) are monotonic increasing functions with λ. From the analysis above, we can come to the conclusion that C_{SK}^N is a convex function about λ. Because the closed expression C_{SK}^N is difficult to be obtained, the iterative algorithm is presented to obtain the optimal ratio λ in this section. The detailed steps are shown in Table 2.

V. SIMULATION RESULTS

Figure 6 reveals the key generation capacity of the proposed scheme with the correlation coefficient of the eavesdropping channel under a low SNR ($\gamma = 5dB$). The values 0.2, 0.5 and

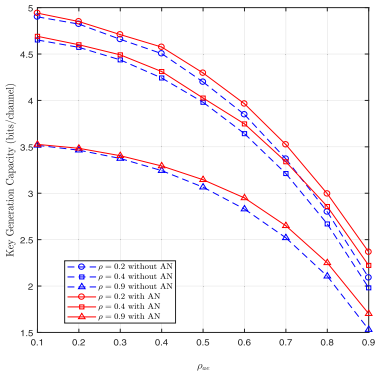


FIGURE 6. The key generation capacity with the correlation coefficient ρ_{ae} of eavesdropping channel under $\gamma = 5dB$.

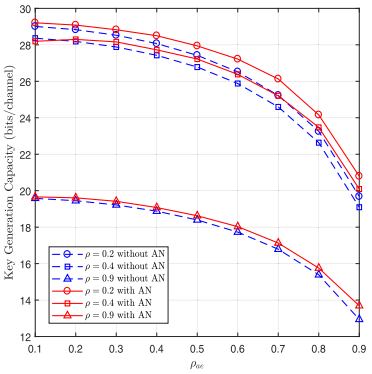


FIGURE 7. The key generation capacity with the correlation coefficient ρ_{ae} of eavesdropping channel under $\gamma = 25dB$.

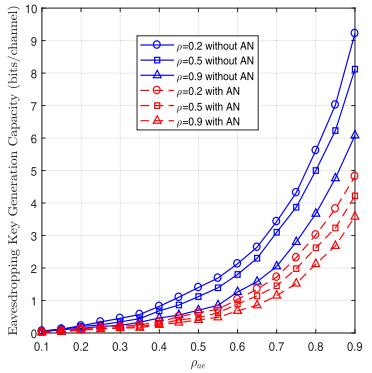


FIGURE 8. The key generation capacity with the correlation coefficient ρ_{ae} of eavesdropping channel under $\gamma = 25dB$.

0.9 respectively represent different correlation coefficients of adjacent antennas. As shown in Figure 6, the channel gain of the proposed scheme is not high when the correlation coefficient of the eavesdropping channel is low. As the correlation coefficient of the eavesdropping channel increases, the proposed scheme can significantly improve the key generation capacity. This is because when the correlation coefficient of the eavesdropping channel is lower, the eavesdropper can eavesdrop less information related to legitimate users. That is to say, the key generation capacity gain will be smaller because the impact of the AN on the eavesdropper is less. With the correlation coefficient of the eavesdropping channel increasing, eavesdroppers could eavesdrop more information. From the analysis above, we could come to the conclusion that the AN will improve the key generation capacity. In addition, it can be seen that the increase of the correlation coefficient of the transmitter antenna will reduce the key generation capacity of the proposed scheme.

Figure 7 demonstrates the key generation capacity of the proposed scheme with the eavesdropping channel correlation coefficient under a high SNR ($\gamma = 25dB$). As shown in Figure 7, we can see that the proposed scheme could improve the key generation capacity more obviously under a high SNR. This is because with the increase of SNR, the quality of the eavesdropping channel becomes better and better. And the eavesdropper will obtain more information between legitimate users, resulting in the lower key generation capacity. Hence, it is more obvious that the AN has a significant impact on the eavesdropper with a higher SNR.

The eavesdropping key generation capacity with the correlation coefficient of eavesdropping channel under a high SNR ($\gamma = 25dB$) is presented in Figure 8. As shown in Figure 8, the eavesdropping key generation capacity of the proposed scheme under different ρ_{ae} is lower compared with the traditional key generation scheme using public pilots, which shows that the proposed scheme has an effective interference on received signals at the eavesdropper. With the increase of the correlation of eavesdropping channel, the eavesdropping key generation capacity of the traditional key generation scheme and the proposed scheme will both increase. However, because the eavesdropping key generation capacity of the proposed scheme is smaller, its security is higher.

VI. CONCLUSION

This paper proposes a key generation scheme through scrambling the correlated eavesdropping channel in MISO system to overcome the issue that it will decrease the key generation capacity because of the correlation channel between the eavesdropper and legitimate user. In the proposed scheme, the artificial noise is superimposed over pilot signals to interfere received signals at eavesdroppers. Firstly, the legitimate transmitter and receiver will extract the channel reciprocity features from their corresponding received signals. Then, we could obtain the key after vector quantization and key agreement. Furthermore, the security performance of the proposed scheme is analyzed. Finally, to improve its security performance, we give an iterative algorithm optimizing the power allocation between pilot signals and the artificial noise. Simulation results show that the proposed scheme could effectively improve the physical key generation capacity for MISO system.

REFERENCES

[1] P. Gacs and J. Körner, "Common information is far less than mutual information," *Problems Control Inf. Theory*, vol. 2, pp. 149–162, Jan. 1973.

[2] 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.

[3] H. Jin, K. Huang, S. Xiao, Y. Lou, X. Xu, and Y. Chen, "A two-layer secure quantization algorithm for secret key generation with correlated eavesdropping channel," *IEEE Access*, vol. 7, pp. 26480–26487, 2019.

[4] J. W. Wallace, C. Chen, and M. A. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. Eur. Conf. Antennas Propag.*, Mar. 2009, pp. 1499–1503.
[5] R. Shetty, "Blind channel estimation based robust physical layer key generation in MIMO networks," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2010, pp. 2522–2525.
[6] V. Zeinali and H. K. Bizaki, "Shared secret key generation protocol in wireless networks based on the phase of MIMO fading channels," *Wireless Pers. Commun.*, vol. 89, no. 4, pp. 1315–1334, Aug. 2016.
[7] R. K. Sharma and J. W. Wallace, "Measured statistics of reciprocal channel key generation of indoor MIMO channels," in *Proc. IEEE Antennas Propag. Soc. Int. Symp.*, Jul. 2010, pp. 1–4.
[8] G. Pasolini and D. Dardari, "Secret key generation in correlated multi-dimensional Gaussian channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2171–2177.
[9] G. Pasolini and D. Dardari, "Secret information of wireless multi-dimensional Gaussian channels," *IEEE Trans. Wireless Commun.*, vol. 14, no. 6, pp. 3429–3442, Jun. 2015.
[10] X. Wang, L. Jin, and H. Song, "Physical layer secret key capacity based on wireless channel parameters," *J. Electron. Inf. Technol.*, vol. 38, no. 10, pp. 2612–2618, 2016.
[11] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2013, pp. 1245–1250.
[12] S. Engelmann, A. Wolf, and E. A. Jorswieck, "Precoding for secret key generation in multiple antenna channels with statistical channel state information," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2014, pp. 1592–1595.
[13] Y. Chen, H. Vogt, and A. Sezgin, "Gaussian wiretap channels with correlated sources: Approaching capacity region within a constant gap," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, Jun. 2014, pp. 794–799.
[14] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "The effect of eavesdropper's statistics in experimental wireless secret-key generation," *Comput. Sci.*, vol. 14, no. 5, pp. 1304–1312, 2014.
[15] T.-H. Chou, S. C. Draper, and A. M. Sayeed, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2518–2522.
[16] 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.
[17] J. P. Kermoal, L. Schumacher, K. I. Pedersen, P. E. Mogensen, and F. Frederiksen, "A stochastic MIMO radio channel model with experimental validation," *IEEE J. Sel. Areas Commun.*, vol. 20, no. 6, pp. 1211–1226, Aug. 2002.
[18] R. Negi and S. Goel, "Secure communications using artificial noise," in *Proc. IEEE Int. Conf. Vehicle Technol.*, Sep. 2005, pp. 1906–1910.
[19] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[20] H.-T. Li and Y.-W. P. Hong, "Secret key generation over correlated wireless fading channels using vector quantization," in *Proc. IEEE Int. Conf. Signal Inf. Process. Assoc.*, 2012, pp. 1–7.
[21] C. K. Sung, H. Suzuki, and I. B. Collings, "Channel quantization using constellation based codebooks for multiuser MIMO-OFDM," *IEEE Trans. Commun.*, vol. 62, no. 2, pp. 578–589, Feb. 2014.

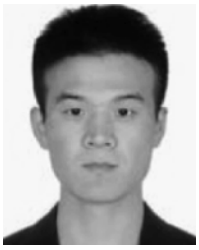
YAJUN CHEN received the B.E. degree from UESTC University, and the M.S. and Ph.D. degrees from the National Digital Switching System Engineering and Technological R&D Center (NDSC), Zhengzhou, China. He has been a Faculty Member of NDSC, since 2017. His research interests include physical layer security, wireless location, and resource management in 5G networks.

KAIZHI HUANG received the B.E. degree in digital communication and the M.S. degree in communication and information system from the National Digital Switching System Engineering and 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. She received the Best Symposium Paper Award from the Electromagnetic Compatibility Society, in 2011.

YOU ZHOU received the B.E. degree from PLA Information Engineering University, Zhengzhou, China, and the Ph.D. degree from the National Digital Switching System Engineering and Technological Research Center (NDSC). He has been a Faculty Member of NDSC, since 2013. His research interest includes wireless location.

KEMING MA received the B.E. degree from PLA Information Engineering University, Zhengzhou, China, and the M.S. degree from the National Digital Switching System Engineering and Technological Research Center (NDSC). He has been a Faculty Member of NDSC, since 2014. His research interest includes wireless location.

HENGLEI JIN received the B.E. degree from Sichuan University. He is currently pursuing the Ph.D. degree with the National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China. 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 Engineering and Technological Research Center. His research interests include stochastic geometry, cooperative communications, and physical layer security of wireless communications.