IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 8, 2019, accepted April 1, 2019, date of publication April 4, 2019, date of current version April 18, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909298

Asymmetric Physical Layer Encryption for Wireless Communications

WEI LI[1], (Member, IEEE), DES MCLERNON[2], (Member, IEEE), KAI-KIT WONG[3], (Fellow, IEEE), SHILIAN WANG[1], (Member, IEEE), JING LEI[1], (Member, IEEE), AND SYED ALI RAZA ZAIDI[2], (Member, IEEE)

[1]Department of Communication Engineering, College of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China
[2]School of Electronic and Electrical Engineering, University of Leeds, Leeds LS2 9JT, U.K.
[3]Department of Electronic and Electrical Engineering, University College London, London WC1E 7JE, U.K.

Corresponding author: Wei Li (liwei.nudt.cn@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grants 61502518, 61702536 and 61601480, and in part by the Hunan Natural Science Foundation under Grant 2018JJ3609. This work was also partly supported by the UK British Council (Newton Fund) through the project "Wireless Sensor Networks for Real Time Monitoring of Water Quality" under Grant IL3264631003 and also by the Research England Global Research Challenges Fund.

ABSTRACT In this paper, we establish a cryptographic primitive for wireless communications. An asymmetric physical layer encryption (PLE) scheme based on elliptic curve cryptography is proposed. Compared with the conventional symmetric PLE, asymmetric PLE avoids the need of key distribution on a private channel, and it has more tools available for processing complex-domain signals to confuse possible eavesdroppers when compared with upper-layer public key encryption. We use quantized information entropy to measure the constellation confusion degree. The numerical results show that the proposed scheme provides greater confusion to eavesdroppers and yet does not affect the bit error rate (BER) of the intended receiver (the information entropy of the constellation increases to 17.5 for 9-bit quantization length). The scheme also has low latency and complexity [$O(N^{2.37})$, where N is a fixed block size], which is particularly attractive for implementation.

INDEX TERMS Encryption, physical layer security, orthogonal frequency-division multiplexing (OFDM), wireless communication.

I. INTRODUCTION

Security is always an important issue in communications networks, and more so for wireless networks due to its broadcast nature. Encryption has been the technology to provide security. For example, in long-term evolution (LTE) systems, a number of symmetric cryptographic algorithms, including SNOW 3G [1], ZUC [2] and AES [3] have been applied but have faced new challenges in 5G scenarios. In particular, the application scenarios, such as enhanced mobile broadband (eMBB), massive machine type communications (mMTC), and ultra-reliable and low latency communication (URLLC), put new requirements on security, which are explained as follows.

1) **Low latency:** Low latency and high security communication technologies are required in applications such as vehicular networks and remote surgery, etc. In these scenarios, the wireless networks need to provide reliable communication with delay less than 1 millisecond.
2) **Low-power consumption and low complexity:** Due to the limited battery life of some devices such as wireless sensors and mobile phones, secure transmission technology also requires low complexity and low power algorithms.
3) **Heterogeneous access and massive users:** Heterogeneity will be one of the network functions of the next generation wireless network. Heterogeneity comes not only from the use of different access technologies (WiFi and LTE) but also from multiple network environments, which may mean that the access network architecture from different networks is different. Therefore, designers need to consider building a security architecture that is appropriate for different access technologies.
4) **Simple and robust key distribution:** In the mMTC scenario, the number of users is massive, making it difficult to manage and distribute keys.

The associate editor coordinating the review of this manuscript and approving it for publication was Md. Arafatur Rahman.

5) **Security does not rely on channel information and eavesdropper status:** Due to the variety of 5G application scenarios, the secure transmission algorithm should be adaptable to different kinds of channel environments. In addition, due to the presence of passive eavesdroppers in the network, the security algorithm should not rely on the eavesdropper channel and location information.

We are looking for a secure communication method that meets the above five features for 5G scenarios. Physical layer encryption (PLE) may be a good choice. PLE is a different approach from the bit layer cryptography and information theory based physical layer security [4]. Compared to upper-layer encryption at the bit-level, PLE facilitates processing of complex-valued signals to confuse eavesdroppers. Unlike physical layer security methods based on artificial noise and beamforming [5]–[9], PLE does not require a positive secrecy rate, nor channel state information. Therefore, PLE offers an alternative to achieve lower latency, lower complexity and higher security for secure transmission. Various PLE approaches have been proposed in systems such as orthogonal frequency-division multiplexing (OFDM) [10], [11], massive multiple-input multiple-output (MIMO) [12]–[14], untrusted relaying systems [15], IEEE 802.15.4 protocols [16], rateless codes [17] and sparse-code multiple-access (SCMA) [18]. Our previous work established mathematical models, design frameworks and cryptographic primitives for stream PLE and block PLE [19]. In [20]–[22] the keys were extracted through the wireless channel, if it satisfies some conditions such as channel reciprocity.

In the literature, most of the PLE studies considered symmetric PLE schemes. That is, the same key is used at both the transmitter and receiver. However, a symmetric PLE scheme is not suitable for multiuser scenarios, particularly when the number of users is large, and it is hard to manage a large number keys. In addition, asymmetric PLE eliminates the preliminary exchange of secret keys and allows for public keys to be shared with anyone. Therefore, we prefer the use of asymmetric PLE (APLE or public key) to reduce the complexity of key distribution and key management. There are already many mature asymmetric encryption algorithms in the upper layers [23], [24], but there is very little work in the physical layer. Of relevance is the work [12] in which a method was proposed using a massive MIMO channel as the key between the sender and the desired receiver, but this method requires the transmitter to know the channel state information for precoding which may be impractical for some scenarios.

In this paper, we will present the cryptographic primitives of an APLE system. In the APLE system, encryption and decryption use different keys. The encryption key is issued as a public key, and the decryption key is stored as a private key only in the legitimate receiver. APLE has different characteristics from existing physical layer security and upper layer public key encryption technologies in that:

1) The processing objects in APLE are physical layer complex signals, while the public key cryptography processing objects are bits. Therefore, new mathematical models and tools are needed in APLE, and eavesdroppers cannot even get bit data.
2) APLE may have lower latency and complexity for lightweight applications in 5G networks.
3) In APLE the effects of wireless channels and noise can be exploited to enhance security.
4) Compared to the precoding or beamforming method [5], [25], [26], APLE does not require multiple antennas and channel information at the transmitter, and it is suitable for both single antenna systems and multi-antenna systems, which has advantages in heterogeneous networks.

In this paper, we propose an APLE design based on elliptic curve cryptography (ECC).[1] A security matrix generation algorithm is first proposed, and then the generated security matrix is used to encrypt the physical layer signal block of the transmitted signal. This method makes each input bit dispersed into the entire output signal block, thereby causing confusion at the output signal. Our design goal is to make eavesdroppers difficult to demodulate the constellation and recover the bit data while ensuring that the bit error ratio (BER) of the legitimate receiver is not degraded.

Notation: $\mathbf{X}^T$, $\mathbf{X}^*$, $\mathbf{X}^H$ and $\mathbf{X}^{-1}$ denote, respectively, the transpose, conjugate, conjugate transpose and inverse of matrix $\mathbf{X}$. In addition, $\mathbf{I}_N$ denotes the N-dimensional identity matrix, and $|x|$ denotes the absolute value of a complex scalar x. We will use $\|\cdot\|$ to denote the Euclidean norm of a vector. $\mathbb{C}^n$ represents the space of $n \times 1$ vectors with complex elements. $\mathbb{C}^{m\times n}$ and $\mathbb{R}^{m\times n}$ represent the space of all $m \times n$ matrices with complex elements and real elements respectively. For sets $\mathcal{A}$ and $\mathcal{B}$, $\mathcal{A} \times \mathcal{B} = \{(a, b) \mid a \in \mathcal{A}$ and $b \in \mathcal{B}\}$, where $\times$ is the Cartesian product between two sets. Given two positive numbers, a (the dividend) and n (the divisor), a mod n is the remainder of the Euclidean division of a by n.

II. SYSTEM MODEL AND CRYPTOGRAPHIC PRIMITIVES OF APLE

As shown in Fig. 1 the basic system model consists of a legitimate transmitter (Tx), Alice, that wants to communicate securely with a legitimate receiver (Rx), Bob, in the presence of an eavesdropper, Eve. The public key and private key are used on the Alice and Bob sides, respectively.

Definition 1: APLE system

Message space $\mathcal{M}$: the set of plaintext messages, a finite set. All input messages $S \in \mathcal{M}$.

Cipher signal space $\mathcal{C}$: the set of all possible ciphers. All cipher signals $Y \in \mathcal{C}$.

Key space $\mathcal{K}, \mathcal{K}'$: possible encryption key (public key) set $\mathcal{K}$, and possible decryption key (private key) set $\mathcal{K}'$.

[1]ECC is a public key encryption approach set on elliptic curve theory that is used to create faster, smaller, and productive cryptographic keys.

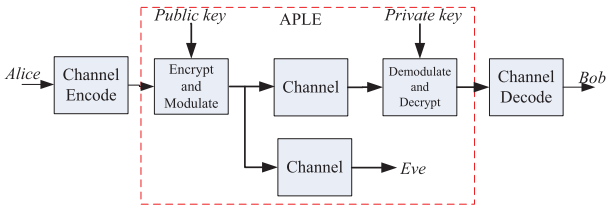

FIGURE 1. System model of APLE.

The encryption key K is chosen from $\mathcal{K}$, and the decryption key K' is chosen from $\mathcal{K}'$, and so $K \in \mathcal{K}$, $K' \in \mathcal{K}'$.

Key generation algorithm $\mathcal{G} :\rightarrow \mathcal{K} \times \mathcal{K}'$.

$\mathcal{G}$ is a probabilistic algorithm that outputs a key pair $(K, K') \in \mathcal{K} \times \mathcal{K}'$.

Encryption algorithm $\mathcal{T} : M \times \mathcal{K} \rightarrow \mathcal{C}$.

Channel function $H_B : \mathcal{C} \rightarrow \mathcal{Z}$.

$\mathcal{H}$ is the equivalent channel function between cipher signal Y and received symbol Z_B, $Z_B = H_B(Y)$. $\mathcal{Z}$ is the set of all possible Z_B, and $Z_B \in \mathcal{Z}$.

$\mathcal{K}$ is the key set and $\mathbb{C}^n$ is a $(n \times 1)$ complex vector space; for stream PLE, complex sequence $\{r_n\} = \{r_1, r_2, \ldots\} \in \mathbb{C}^n$.

Decryption algorithm $\mathcal{D} : \mathcal{Z} \times \mathcal{K}' \rightarrow \mathcal{M}$.

Note that although the above model only defines a single-user scenario, it can be easily extended to a multiuser scenario. We only need to generate a public-key private-key pair for each user. When other users want to send information to this user, they use the corresponding public key to encrypt, and the receiver can decrypt it with its own private key.

III. APLE ALGORITHM BASED ON ELLIPTIC CURVE CRYPTOGRAPHY

From the definition in the previous section, we can see that the essence of APLE is to design a mapping T from the massage space (groups of bits) to the cipher signal space (complex vectors), and an inverse mapping D. These processes involve modulation and demodulation in a standard communication system, which means that we can jointly design encryption and modulation as a whole in order to achieve joint optimization of security, reliability and transmission efficiency. However, in the design of a communication standard we also need to consider compatibility and continuity. Therefore, this paper retains the physical layer structure of existing communication system, and inserts the physical layer security as a module into the existing physical layer structure.

The basic structure of the system is shown in Fig. 2. At the transmitter, the binary information $\mathbf{S}$ is converted into a complex vector X by a mapping module. X is then converted by a block change module into a complex vector Y according to the security matrix U. Then the signal passes through the IFFT module, the cyclic prefix (CP) module and then sent to the radio frequency (RF) module for subsequent processing. The processing flow of the receiver is reversed from that of the transmitter.

The ECCM is an elliptic curve cryptographic operation module whose function is to generate a security matrix $\mathbf{U}$.

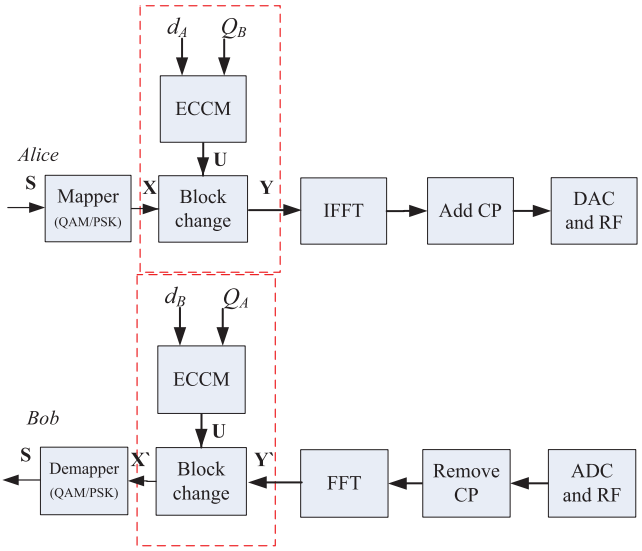

FIGURE 2. ECC based APLE.

Block change is a physical layer encryption module. d_A and d_B are the private keys of Alice and Bob, and H_A and H_B are the public keys of Alice and Bob. We will introduce each module in the following sections.

A. ELLIPTIC CURVE CRYPTOGRAPHY

Before introducing the entire algorithm, we will briefly introduce the elliptic curve cryptography. Elliptic curves were proposed for use as the basis for discrete logarithm-based cryptosystems independently by Victor Miller of IBM and Neal Koblitz of the University of Washington [27]. For the purpose of cryptography, An elliptic curve E defined over a finite field $GF(p)$ is a set of points $P = (x, y)$, where x and y are elements of $GF(p)$ that satisfy a certain equation:

$$y^2 = x^3 + ax + b, \tag{1}$$

where a and b are elements of a finite field with p elements, and p is an odd prime. a and b shall satisfy

$$4a^3 + 27b^2 \neq 0(\mod p). \tag{2}$$

There are definitions of addition, subtraction, and scalar multiplication operations on elliptic curves, which are different from operations on the ordinary number field. Detailed definitions can be found in [28]. In standard FIPS 186-4 [29], National Institute of Standards and Technology (NIST) recommends five prime fields for certain primes p of sizes 192, 224, 256, 384, and 521 bits. For each of the prime fields, one elliptic curve is recommended.

B. APLE ALGORITHM

The whole algorithm is divided into four steps: private and public key pairs generation, public keys exchange, security matrix generation, block change and secure communication.

1) PRIVATE AND PUBLIC KEY PAIRS GENERATION

First, an elliptic curve E defined over $GF(p)$ with large group of order n and a point G of large order is selected and made public to all users. Then, the following key generation primitive is used by each user to generate the individual public and private key pairs.

1) Chose a random integer d from $\{1, \cdots, n-1\}$ (where n is the order of the subgroup).
2) Compute $Q = d \times G$.
3) The private key is d and the public key is (E, G, n, Q).

Alice and Bob generate their own key pairs independently. Alice has the private key d_A and the public key $Q_A = d_A \times G$, Bob has the keys d_B and $Q_B = d_B \times G$. Note that both Alice and Bob are using the same domain parameters: the same base point G on the same elliptic curve on the same finite field $GF(p)$.

2) PUBLIC KEYS EXCHANGE

Alice and Bob exchange their public keys Q_A and Q_B over a public channel. Eve would intercept Q_A and Q_B, but will not be able to find out either d_A or d_B without solving the discrete logarithm problem.

3) SECURITY MATRIX GENERATION BY ECCM

Alice calculates $S_k = d_A \times Q_B$ (using her own private key and Bob's public key), and Bob calculates $S_k = d_B \times Q_A$ (using its own private key and Alice's public key). Here, $S_k = (x_s, y_s)$ is a point on the elliptic curve E. Then Alice and Bob need to generate a unitary matrix from S_k. Note that S_k is the same for both Alice and Bob, in fact:

$$S_k = d_A Q_B = d_A(d_B G) = d_B(d_A G) = d_B Q_A. \tag{3}$$

The eavesdropper, however, only knows Q_A and Q_B (together with the other domain parameters) and would not be able to find out the shared point S_k. We call $\mathbf{U} \in \mathbb{C}^{N \times N}$ security matrix. The security matrix generation algorithm will be demonstrated in the next subsection.

4) BLOCK CHANGE AND SECURE COMMUNICATION

After Alice and Bob generate the security matrix, they send $\mathbf{U}$ to their respective block change modules to complete the physical layer encryption and decryption. $X = \{X_1, X_2, \ldots, X_N\}$, $Y = \{Y_1, Y_2, \ldots Y_N\}$. The process of encryption on Alice is represented as

$$Y = UX. \tag{4}$$

The process of decryption on Bob is represented as

$$X' = U^H Y', \tag{5}$$

where X' and Y' recieved complex vector in Fig.2.

C. SECURITY MATRIX GENERATION ALGORITHM

The $\mathbf{U}$ matrix design needs to meet the following conditions:

- It must make the symbol module $\mathbf{X}$ fully confused and disturbed.
- It must ensure that the performance of the constellation is not changed after the transformation.

In our previous work, it has been proved that the unitary matrix can well meet the above conditions [19]. We need to generate the matrix $\mathbf{U}$ to satisfy the following conditions:

In fact any $N \times N$ unitary matrix $\mathbf{U}$ has N^2 independent real phase parameters. Thus, we can generate an $N \times N$ unitary matrix $\mathbf{U}$ from a given rotation direction vector, $\boldsymbol{\theta} = \{\theta_1\theta_2, .., \theta_{N^2}\}$.

The security matrix generation algorithm is given in Algorithm 1,

Algorithm 1 Security Matrix Generation Algorithm

Require:
Shared point, $S_k = (x_s, y_s)$;
Ensure:
Security matrix, U;
1: Combine x_s and y_s to form a binary number S_0;
2: **for** i= 1 to N^2 **do**
3: $S_i = S_0 + i * q \pmod p$; // q is a prime number and $p < q$.
4: $S'_i = hash(S_i)$;
5: $\theta_i = 2\pi(S'_i \bmod \lambda)/\lambda$;
6: **end for**
7: Generate $\mathbf{U}$ from $\boldsymbol{\theta}$;
8: **return** $\mathbf{U}$;

The details of the algorithm are as follows:

1) HASH FUNCTION

The purpose of the hash function is to shuffle the data so that the distribution of the rotation angles is more uniform and random. A hash function $hash()$ is called collision free, if it maps messages of any length to strings of some fixed length, but such that finding s, y with $hash(s) = hash(y)$ is a hard problem. We can choose a mature hash function such as SHA-3 [30] to map S_i to S'_i.

2) ROTATION DIRECTION VECTOR GENERATION

Considering the range of θ_i is $[0, 2\pi)$ while the range of S'_i is $[0, 2^L - 1]$. L is the bit width of S'_i. Hence, a mapping from θ_i to S'_i has to be constructed. We use the mapping function :

$$\theta_i = 2\pi(S'_i \boldsymbol{o} d\lambda)/\lambda, \tag{6}$$

where λ is positive integer parameter which indicates phase accuracy. For example, the λ value can be 256, which means the phase accuracy is $2\pi/256$.

3) GENERATE $\mathbf{U}$ FROM θ

First construct an $N \times N$ matrix using the rotation vector $\boldsymbol{\theta}$ as

$$U' = \begin{bmatrix} e^{\theta_1}, & e^{\theta_{N+1}} & \ldots & e^{\theta_{N(N-1)+1}} \\ e^{\theta_2}, & e^{\theta_{N+2}} & \ldots & e^{\theta_{N(N-1)+2}} \\ \vdots & & & \\ e^{\theta_N}, & e^{\theta_{2N}} & \ldots & e^{\theta_{N^2}} \end{bmatrix} = [v_1, v_2, \ldots, v_N] \tag{7}$$

Then we use GramâĂ"Schmidt process to orthonormalise U' and get the unitary matrix $U = [e_1, e_2, \ldots, e_N]$.

IV. PERFORMANCE ANALYSIS AND NUMERICAL SIMULATIONS

In order to evaluate the performance of the algorithm, we analyze the security, constellation information entropy and bit error rate performance. Simulation is based on the physical layer of IEEE 802.11ac OFDM protocol which has been widely used in a wireless local area network. We consider the 256-point FFT with a cyclic prefix length of 1/4 of FFT length. The parameters are: QPSK and 16QAM modulation, FFT size = 256, a cyclic prefix length=64. We evaluate the BER performance over a practical frequency selective fading channel.

A. SECURITY ANALYSIS FROM THE PERSPECTIVE OF ATTACKERS

On the eavesdropper side, we should prevent Eve from recovering X, U or the private key d. We now consider the worst case where Eve has the following ability:

- Eve is able to correctly perform channel estimation, channel equalization, and recover the estimate of Y as $Y_e = Y + W$, where $W \in \mathbb{C}^N$ is an additive white Gaussian noise (AWGN) vector. From (4), we get
$$Y_e = UX + W. \tag{8}$$
- Eve knows the public key (E, G, n, Q).

The algorithm that we have designed need to prevent the following possible attacks by Eve.

1) RECOVER d FROM PUBLIC KEY (E,G,n,Q). (CIPHERTEXT-ONLY ATTACK)

The basis for the security of elliptic curve cryptosystems is the apparent intractability of the elliptic curve discrete logarithm problem (ECDLP). Elliptic curve cryptosystems offer the highest strength-per-key-bit of any known public-key system. With a 160-bit modulus, an elliptic curve systems offers the same level of cryptographic security as DSA or RSA with 1024-bit moduli [31].

2) RECOVER U FORM Y_e WITH THE KNOWN MESSAGE X. (KNOWN-PLAINTEXT ATTACK)

Eve's attack is equivalent to solving the equation (8) for U.

Because Eve does not know the noise $\mathbf{W}$, and the unknown $\mathbf{U}$ contains $N \times N$ variables, it is an unsolvable equation. If Eve uses brute force attack, its search space is, where is phase resolution. Take $N = 8, \lambda = 256$, as an example and its search space reaches 2^{512}. The computational complexity is certainly unaffordable for the eavesdroppers.

3) RECOVER d OR U FROM CHOSEN-PLAINTEXT

Eve can obtain the cipher signal for any specified plaintexts for the current key d (chosen-plaintext attack).

This type of attack means that Eve has a lot of plaintext ciphertext pairs (X, Y_e), and Eve trys to solve a group of equations for $\mathbf{U}$. It is obvious that the noise W plays an uncertain role in the equations, which will prevent Eve from obtaining U. In addition we also need to use PLE-block chaining operation mode in [19]. PLE-block chaining XORs the plaintext and the previous stage ciphertext, and then send the result to the PLE encryption module. This is equivalent to changing U for each block of encryption. So Eve cannot solve for $\mathbf{U}$ even if she gets enough (X, Y_e) pairs.

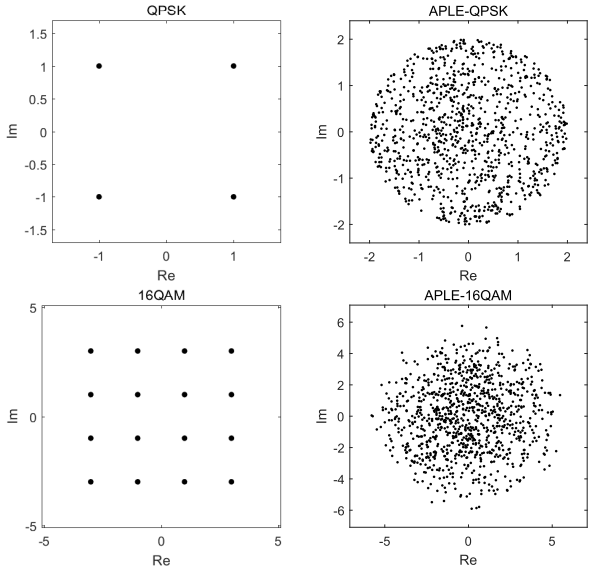

FIGURE 3. The QPSK and 16QAM constellation before and after encryption.

B. CONFUSION OF THE CONSTELLATIONS

Confusion of the constellations is an important indicator of the security of physical layer encryption. Eavesdroppers have the possibility of obtaining information by accumulating observations for constellations over a long time. In order to avoid this situation, we need more confusion in the constellations.

Fig. 3 shows the QPSK and 16QAM constellation ($Y = c + d * j$) before and after encryption. We can see that the constellation map is chaotic after encryption, there is no obvious pattern, and it looks like noise. We use quantized information entropy to measure the constellation confusion degree:

$$H^{\Delta}(Y) := -\sum_{i=-\infty}^{\infty}\sum_{j=-\infty}^{\infty} \Gamma(i,j)\log_2 \Gamma(i,j), \tag{9}$$

where $\Gamma(i,j) = \int_{i\Delta}^{(i+1)\Delta}\int_{j\Delta}^{(j+1)\Delta} p(c,d)dcdd$, $p(c,d)$ is the joint probability density function for c and d. Δ is quantification accuracy. Larger information entropy means that the constellation is highly chaotic and there is less leakage of constellation information.

Fig. 4 shows that the information entropy increases with increasing quantization length of constellation coordinates.

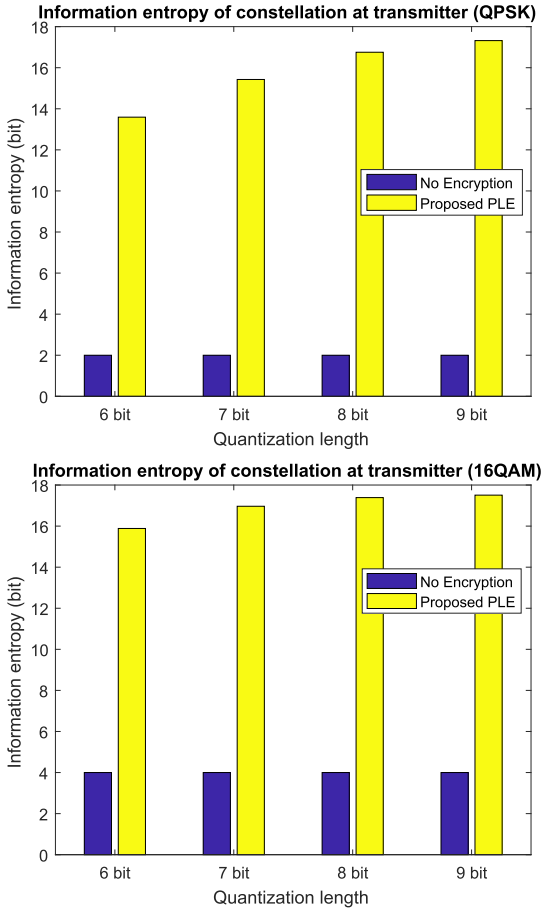

FIGURE 4. Information entropy of constellations at the transmitter.

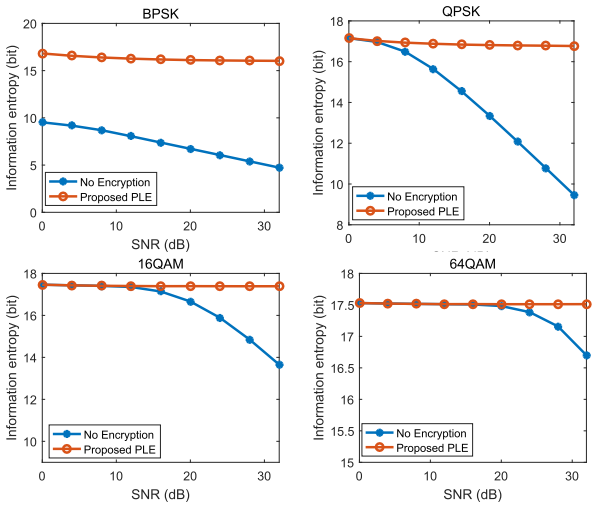

FIGURE 5. Information entropy of constellation at the receiver, quantization length = 9 bits.

It is shown that our proposed method can increase the information entropy of the constellation significantly.

Fig. 5 shows the information entropy of the BPSK, QPSK, 16QAM, and 64QAM constellation at the receiver with the change of signal to noise ratio. It can be seen that in the non-encrypted scheme with the increase of SNR, the information entropy shows a downward trend, which means that the noise can make the constellation more chaotic. When the signal-to-noise ratio of the eavesdropper increases, the information entropy decreases and the constellation becomes more and more insecure. The eavesdropper may then obtain leaked information from the statistical characteristics of the constellation. However, in the proposed PLE method, the information entropy of the constellation does not change with noise. The encrypted constellation still has great confusion at high SNR eavesdropper.

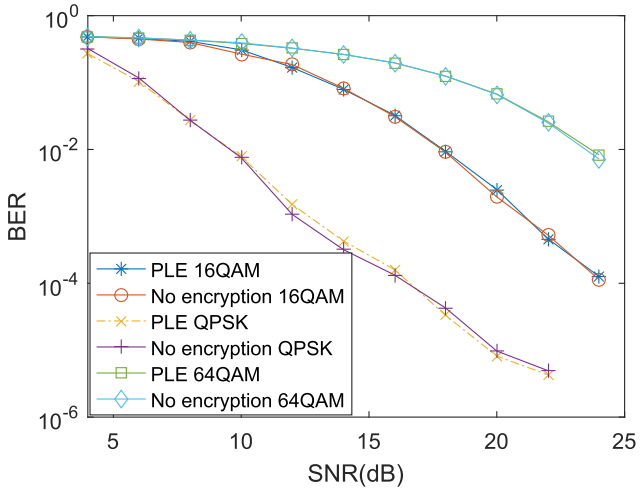

FIGURE 6. BERs of the legitimate user in an OFDM system.

C. BER PERFORMANCE

In Fig. 6 we compare the BER performance of the proposed PLE and non-encrypted systems in an OFDM system. QPSK, 16QAM, and 64QAM modulation are considered. The simulation shows that the proposed PLE encryption system has almost the same bit error rate performance as the non-encrypted system. Therefore, the proposed algorithm does not deteriorate the BER performance and meets the design requirements.

D. COMPLEXITY ANALYSIS

The computational complexity of this PLE algorithm includes two parts: one is the security matrix generation, and the other is block change and secure communication. The security matrix generation process is non-real-time and does not need to run for every signal block. Block change is a real-time encryption module that needs to run every time the signal is transferred. Therefore, the computational complexity and delay of the system are mainly generated by the block change module.

The complexity of the block change algorithm is just an $N \times N$ complex matrix multiplication added to the sender and receiver respectively. The existing low-complexity matrix multiplication algorithm is $O(N^{2.37})$ [32]. Note that N here is not the data length, but the size of the block, which is

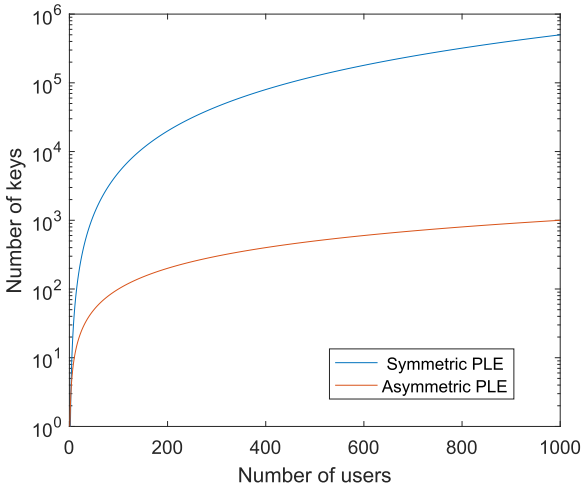

FIGURE 7. The key number of asymmetric PLE and symmetric PLE.

a constant and not very large. In fact, there are already many mature hardware implementations of matrix multiplication with lower complexity and latency [33], [34]. $N \times N$ matrix multiplication can be performed in $N^2 + 2N$ cycles using N processing elements [34]. For example if $N = 8$ and the clock is 200MHZ, then the delay is 80 clock cycles or 10^{-9} seconds. Therefore, the complexity and delay of the algorithm are not high, and it is easy to implement in hardware.

Then we consider the key number under the multi-user scenario. A comparison of the proposed asymmetric PLE with the symmetric PLE technique is given in Fig. 7. The key number for the asymmetric PLE is N_u and the key number for the symmetric PLE is $N_u(N_u - 1)/2$, where N_u is the number of users. As shown in Fig. 7, as the number of users increases, the number of keys for the symmetric PLE is very large. The number of keys for the asymmetric PLE is small. This means that the asymmetric PLE has very low key management complexity.

V. CONCLUSIONS

This paper establishes a cryptographic primitive for an asymmetric physical layer encryption system, which provides a new path for PLE system design. Further an asymmetric physical layer encryption scheme based on elliptic curve cryptography is proposed. Compared with the existing symmetric PLE scheme, the scheme does not need to perform key distribution on a private channel, and is more suitable for a multi-user communication scenario. Compared with the upper-layer public key encryption scheme, the physical layer signal can be protected and the security is enhanced. Analysis and simulation show that the proposed algorithm has a higher confusion of the constellations and has the same BER performance as the non-encrypted system. The algorithm has low latency and complexity and is easy to implement in hardware which is suitable for some 5G scenarios.

REFERENCES

[1] *Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 1: UEA2 and UIA2 Specification*, Standard ETSI/SAGE, 2006.

[2] *Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3. Document 2: ZUC Specification*, Standard ETSI/SAGE, Jan. 2011.

[3] D. Joan and R. Vincent, *The Design of Rijndael: AES-The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] N. Romero-Zurita, D. McLernon, and M. Ghogho, "Physical layer security by robust masked beamforming and protected zone optimisation," *IET Commun.*, vol. 8, no. 8, pp. 1248–1257, May 2014.

[6] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "QoS-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Trans. Signal Process.*, vol. 59, no. 3, pp. 1202–1216, Mar. 2011.

[7] W. Li, M. Ghogho, B. Chen, and C. Xiong, "Secure communication via sending artificial noise by the receiver: Outage secrecy capacity/region analysis," *IEEE Commun. Lett.*, vol. 16, no. 10, pp. 1628–1631, Oct. 2012.

[8] W. Li, Y. Tang, M. Ghogho, J. Wei, and C. Xiong, "Secure communications via sending artificial noise by both transmitter and receiver: Optimum power allocation to minimise the insecure region," *IET Commun.*, vol. 8, no. 16, pp. 2858–2862, 2014.

[9] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Outage probability based power distribution between data and artificial noise for physical layer security," *IEEE Signal Process. Lett.*, vol. 19, no. 2, pp. 71–74, Feb. 2012.

[10] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Design of an OFDM physical layer encryption scheme," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2114–2127, Mar. 2017.

[11] M. Sakai, H. Lin, and K. Yamashita, "Intrinsic interference based physical layer encryption for OFDM/OQAM," *IEEE Commun. Lett.*, vol. 21, no. 5, pp. 1059–1062, May 2017.

[12] T. R. Dean and A. J. Goldsmith, "Physical-layer cryptography through massive MIMO," *IEEE Trans. Inf. Theory*, vol. 63, no. 8, pp. 5419–5436, Aug. 2017.

[13] B. Chen, C. Zhu, W. Li, J. Wei, V. C. M. Leung, and L. T. Yang, "Original symbol phase rotated secure transmission against powerful massive MIMO eavesdropper," *IEEE Access*, vol. 4, pp. 3016–3025, 2016.

[14] S. Wang, W. Li, and J. Lei, "Physical-layer encryption in massive MIMO systems with spatial modulation," *China Commun.*, vol. 15, no. 10, pp. 159–171, Oct. 2018.

[15] H. Xu and L. Sun, "Encryption over the air: Securing two-way untrusted relaying systems through constellation overlapping," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8268–8282, Dec. 2018.

[16] A. K. Nain *et al.*, "A secure phase-encrypted IEEE 802.15.4 transceiver design," *IEEE Trans. Comput.*, vol. 66, no. 8, pp. 1421–1427, Aug. 2017.

[17] Y. Huang, W. Li, and J. Lei, "Concatenated physical layer encryption scheme based on rateless codes," *IET Commun.*, vol. 12, no. 12, pp. 1491–1497, Jul. 2018.

[18] K. Lai, J. Lei, L. Wen, G. Chen, W. Li, and P. Xiao, "Secure transmission with randomized constellation rotation for downlink sparse code multiple access system," *IEEE Access*, vol. 6, pp. 5049–5063, 2018.

[19] W. Li, D. McLernon, J. Lei, M. Ghogho, S. A. R. Zaidi, and H. Hui, "Mathematical model and framework of physical layer encryption for wireless communications," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Aug. 2018, pp. 1–7.

[20] L. Cheng, W. Li, D. Ma, J. Wei, and X. Liu, "Moving window scheme for extracting secret keys in stationary environments," *IET Commun.*, vol. 10, no. 16, pp. 2206–2214, 2016.

[21] J. Zhang, A. Marshall, R. Woods, and T. Q. Duong, "Efficient key generation by exploiting randomness from channel responses of individual OFDM subcarriers," *IEEE Trans. Commun.*, vol. 64, no. 6, pp. 2578–2588, Jun. 2016.

[22] L. Cheng, W. Li, L. Zhou, C. Zhu, J. Wei, and Y. Guo, "Increasing secret key capacity of OFDM systems: A geometric program approach," *Concurrency Comput., Pract. Exper.*, vol. 29, no. 16, p. e3966, 2017.

[23] G. S. Quirino, A. R. L. Ribeiro, and E. D. Moreno, "Asymmetric encryption in wireless sensor networks," in *Wireless Sensor Networks*, M. A. Matin, Ed. Rijeka, Croatia: InTech, 2012, ch. 10. doi: 10.5772/48464.

[24] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, "An ElGamal-like cryptosystem for enciphering large messages," *IEEE Trans. Knowl. Data Eng.*, vol. 14, no. 2, pp. 445–446, Mar. 2002.
[25] N. Romero-Zurita, M. Ghogho, and D. McLernon, "Physical layer security of mimo frequency selective channels by beamforming and noise generation," in *Proc. 19th Eur. Signal Process. Conf.*, Aug. 2011, pp. 829–833.
[26] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas I: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088–3104, Jul. 2010.
[27] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology-CRYPTO Proceedings*, H. C. Williams, Ed. Berlin, Germany: Springer, 1986, pp. 417–426.
[28] *IEEE Standard Specifications for Public-Key Cryptography*. IEEE Standard 1363-2000, Aug. 2000, pp. 1–228.
[29] *Fips Pub 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS)*, Standard FIPS PUB 186-4, National Institute of Standards and Technology Standard, Jul. 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
[30] M. J. Dworkin, "SHA-3 standard: Permutation-based hash and extendable-output functions," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep., Jul. 2015.
[31] A. Jurišic and A. J. Menezes, "Elliptic curves and cryptography," *Dr. Dobb's J.*, vol. 22, pp. 26–36, Apr. 1997.
[32] F. Le Gall, "Powers of tensors and fast matrix multiplication," in *Proc. 39th Int. Symp. Symbolic Algebraic Comput. (ISSAC)*. New York, NY, USA: ACM, 2014, pp. 296–303. doi: 10.1145/2608628.2608664.
[33] N. Boullis and A. Tisserand, "Some optimizations of hardware multiplication by constant matrices," *IEEE Trans. Comput.*, vol. 54, no. 10, pp. 1271–1282, Oct. 2005.
[34] J. Jang, S. B. Choi, and V. K. Prasanna, "Energy- and time-efficient matrix multiplication on FPGAs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 13, no. 11, pp. 1305–1319, Nov. 2005.

WEI LI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in communication engineering from the National University of Defence Technology (NUDT), Changsha, China, in 2002, 2006, and 2012, respectively. He is currently a Lecturer with the Department of Communication Engineering, School of Electronic Science and Engineering, NUDT. He is also a Visiting Researcher with the University of Leeds. His research interests include wireless communications, wireless network resource allocation, and physical layer security. He received the Exemplary Reviewer Award from the IEEE COMMUNICATIONS LETTERS, in 2014.

DES MCLERNON received the B.Sc. degree in electronic and electrical engineering and the M.Sc. degree in electronics from the Queen's University of Belfast, U.K. He is currently pursuing the Ph.D. degree in signal processing from the Imperial College, University of London. He then worked on radar systems research and development at Ferranti Ltd., Edinburgh, U.K. He joined the Imperial College, University of London. His research interests are broadly within the domain of signal processing for wireless communications. He has published more than 320 journals and conference papers in these areas. He has supervised more than 45 Ph.D. students. His current research projects include PHY layer security, M2M communications, energy harvesting, robotic communications, machine learning for security in SDNs, distributed sensing, stochastic geometry, multi-packet reception, and drone small-cell communications. He plays jazz piano (with a singer in bars/restaurants) and was recently runner up in the 2018 Leeds Pub Piano Competition. Recent conference organisation includes the IEEE SPAWC 2010, the European Signal Processing Conference (EUSIPCO) 2013, the IET Conference on Intelligent Signal Processing, London, in 2013, 2015, and 2017, and the IEEE GLOBECOM, in 2014, 2015, and 2016 (Workshop on Trusted Communications with Physical Layer Security). He is an Associate Editor of the *IET Signal Processing*.

KAI-KIT WONG (M'01–SM'08–F'16) received the B.Eng., M.Phil., and Ph.D. degrees in electrical and electronic engineering from The Hong Kong University of Science and Technology, Hong Kong, in 1996, 1998, and 2001, respectively. After graduation, he took up academic and research positions at The University of Hong Kong, Lucent Technologies, Bell-Labs, Holmdel, the Smart Antennas Research Group, Stanford University, and the University of Hull, U.K. He is the Chair of wireless communications with the Department of Electronic and Electrical Engineering, University College London, U.K. His current research interests include around 5G and beyond mobile communications, including topics such as massive multiple-input multiple-output, full-duplex communications, millimeter-wave communications, edge caching and fog networking, physical layer security, wireless power transfer and mobile computing, V2X communications, and, of course, cognitive radios. There are also a few other unconventional research topics that he has set his heart on, including, for example, fluid antenna communications systems, remote ECG detection, and so on. He was a co-recipient of the 2013 IEEE Signal Processing Letters Best Paper Award and the 2000 IEEE VTS Japan Chapter Award from the IEEE Vehicular Technology Conference, Japan, in 2000, and a few other international best paper awards. He is a Fellow of IET and is also on the editorial board of several international journals. He has been serving as a Senior Editor for the IEEE COMMUNICATIONS LETTERS, since 2012, and also for the IEEE WIRELESS COMMUNICATIONS LETTERS, since 2016. He has been an Area Editor for Wireless Communication Theory and Systems I of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, since 2018. He served as an Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, from 2005 to 2011, and as an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS, from 2009 to 2012. He was also a Guest Editor of the IEEE JSAC Special Issue on Virtual MIMO, in 2013. He is a Guest Editor of the IEEE JSAC Special Issue on Physical Layer Security for 5G.

SHILIAN WANG received the B.S. and Ph.D. degrees in information and communication engineering from the National University of Defense Technology (NUDT), China, in 1998 and 2004, respectively. Since 2004, he has been continued research in wireless communications with NUDT, where he became a Professor. From 2008 to 2009, he was a Visiting Scholar with the Department of Electronic and Electrical Engineering, Columbia University, New York, NY, USA. He is currently the Head of the Laboratory of Advanced Communication Technology, School of Electronic Science, NUDT. He has authored or co-authored two books, 26 journal papers, and 20 conference papers. His research interests include wireless communications and signal processing theory, including chaotic spread spectrum and LPI communications, CPM and STC, underwater acoustic communication and networks, and deep learning and its applications in communication sensing.

JING LEI received the B.Sc., M.Sc., and Ph.D. degrees from the National University of Defence Technology (NUDT), Changsha, China, in 1990, 1994, and 2009, respectively. She is currently a Distinguished Professor with the Department of Communications Engineering, College of Electronic Science, National University of Defence Technology, and the Leader of the Communication Coding Group. She was a Visiting Scholar with the School of Electronics and Computer Science, University of Southampton, U.K. She has published many papers in various journals and conference proceedings and five books. Her research interests include information theory, LDPC, space-time coding, advanced multiple access technology, physical layer security, and wireless communication technology.

SYED ALI RAZA ZAIDI received the Ph.D. degree from the School of Electronic and Electrical Engineering, University of Leeds, Leeds. From 2011 to 2013, he was with the International University of Rabat, as a Lecturer. From 2013 to 2015, he was with the SPCOM Research Group, U.S. Army Research Laboratory, funded project in the area of network science. In 2013, he was a Visiting Research Scientist with the Qatar Innovations and Mobility Centre, where he was involved in QNRF funded project QSON. He is currently a University Academic Fellow (Assistant Professor) in wireless communication and sensing systems with the University of Leeds. He has published over 90 papers in leading IEEE conferences and journals. He is also an Active Member of the EPSRC Peer Review College. During his Ph.D. degree, he received the G. W. Carter Prize and the F. W. Carter Prize for best thesis and best research paper, respectively. He is a EURASIP Local Liaison for U.K., and also a General Secretary of the IEEE Technical Subcommittee on Backhaul and Fronthaul networks. From 2014 to 2015, he served as an Editor for the IEEE COMMUNICATION LETTERS. He was also a Lead Guest Editor of *IET Signal Processing Journal*'s Special Issue on Signal Processing for Large-Scale 5G Wireless Networks. He is currently an Associate Technical Editor of IEEE *Communication Magazine*.