Enhanced Message Authentication Encryption Scheme Based on Physical-Layer Key Generation in Resource-Limited Internet of Things

Zeng Xing[1], Bo Zhao[1*], Bo Xu[1*], Guangliang Ren[2], and Zhiqiang Liu[1]
[1] School of Cybersecurity, Northwestern Polytechnical University, Xi'an, Shaanxi, China
[2] School of Telecommunications Engineering, Xidian University, Xi'an, Shaanxi, China
[E-mail: bozhao@nwpu.edu.cn, nathan.xu@mail.nwpu.edu.cn]
[*]Corresponding author: Bo Zhao, Bo Xu

Received March 25, 2024; revised June 5, 2024; revised August 2, 2024; accepted August 13, 2024; published September 30, 2024

Abstract

The Internet of Things (IoT) is facing growing security challenges due to its vulnerability. It is imperative to address the security issues using lightweight and efficient encryption schemes in resource-limited IoT. In this paper, we propose an enhanced message authentication encryption (MAE) scheme based on physical-layer key generation (PKG), which uses the random nature of wireless channels to generate and negotiate keys, and simultaneously encrypts the messages and authenticates the source. The proposed enhanced MAE scheme can greatly improve the security performance via dynamic keyed primitives construction while consuming very few resources. The enhanced MAE scheme is an efficient and lightweight secure communication solution, which is very suitable for resource-limited IoT. Theoretical analysis and simulations are carried out to confirm the security of the enhanced MAE scheme and evaluate its performance. A one-bit flipping in the session key or plain texts will result in a 50%-bit change in the ciphertext or message authentication code. The numerical results demonstrate the good performance of the proposed scheme in terms of diffusion and confusion. With respect to the typical advanced encryption standard (AES)-based scheme, the performance of the proposed scheme improves by 80.5% in terms of algorithm execution efficiency.

Keywords: Internet of Things, physical-layer security, physical-layer key generation, enhanced message authentication encryption, dynamic keyed primitives construction

This work was supported in part by Natural Science Basic Research Program of Shaanxi (2023-JC-QN-0745), in part by the Science and Technology Commission of Shanghai Municipality (22YF1452200), in part by the Guangdong Basic and Applied Basic Research Foundation (2021A1515110822), in part by Basic Research Programs of Taicang (TC2022JC20), and in part by the Fundamental Research Funds for the Central Universities (D5000210589).

http://doi.org/10.3837/tiis.2024.09.005 **ISSN : 1976-7277**

1. Introduction

As a promising cyber-physical system used in various scenarios, the Internet of Things (IoT) has attracted massive attention from industry and academia. IoT integrates a large number of resource-limited devices from the physical world into a vast network to provide monitoring, positioning, and other services. Due to its open nature and large scale, IoT faces severe security threats from external attackers [1], [2]. Meanwhile, there are some potential eavesdroppers to intercept the key negotiation or message signals, and further to crack the secret key or cipher messages, which may lead to severe security issues. Therefore, efficient and lightweight secure communication schemes are needed to protect the IoT from attacks.

Conventionally, secure communication is implemented by cryptographic algorithms [3]: generating secret keys from some randomness sources, distributing or negotiating keys via asymmetric cryptography algorithms, and encrypting messages by symmetric ones, such as random number generator, Rivest-Shamir-Adleman (RSA) algorithm, and advanced encryption standard (AES) algorithm. These algorithms can achieve different secure services [3], e.g., confidentiality, integrity, source authentication, and so on. However, it is challenging to deploy these traditional application-layer cryptographic algorithms on resource-limited IoT devices because of their high computational complexity and large storage memory requirements. For example, these algorithms often perform a large number of iterative rounds to encrypt messages and at least two times to authenticate the source. Chaotic cryptographic algorithms [4], [5], [6] or elliptic curve algorithms [7] are alternative solutions, but the tremendous float-point operations make them impractical on resource-limited IoT devices.

The randomness sources are the cornerstone of the key's secrecy which also determines the security of a cryptography algorithm. Fortunately, physical layer security (PLS) can be considered a promising solution, which exploits the random nature of wireless channels to provide secrecy [8]. To this end, based on the reciprocity of the electromagnetic waves' propagation and the spatial uncorrelation of the wireless signals' statistical properties, physical-layer key generation (PKG) technologies have been proposed to efficiently and securely negotiate secret keys from wireless channels [9], [10]. The reciprocity of the electromagnetic waves' propagation and the spatial uncorrelation of the wireless signals' statistical properties result in the uniqueness and secrecy of physical characteristics of legal users, which makes it proper for randomness sources. In the past few years, various schemes of PKG have been proposed in different communication scenarios, such as vehicle Ad hoc networks [11], backscatter communications [12], in-band full-duplex multiple-input multiple-output communications [13], dynamic meta-surface antennas [14], time division duplexing system [15] and so on. However, the key generation schemes mentioned above have not yet been integrated with encryption or authentication algorithms to give a complete, secure communication solution to resource-limited IoT.

In addition to physical-layer key generation techniques, there are some other solutions to encryption or authentication for resource-limited IoT. On the one hand, current research on encryption schemes for resource-limited IoT can be generally divided into two categories: 1) conventional encryption algorithms [4], [7] with hardware special designing and 2) burgeoning cryptographic schemes such as attribute-based encryption (ABE) [16], [17]. However, these conventional algorithms are based on one-way mathematical problems, that is, problems that are easy to perform but difficult to reverse. These algorithms require specially designed hardware to accelerate on resource-limited IoT devices. At the same time, the burgeoning ABE paradigm is not suitable for large amounts of data transmission. On the other hand, the schemes dedicated only to authentication can be divided into two categories: 1) trust-based authentication, e.g., in consensus style [18] or federated style [19], and 2) characteristic-based authentication, such as physical channel characteristics [20], [21]. However, the present trust-based schemes employ complex authenticating processes, making them unsuitable for IoT with dense data transmissions. In addition, many schemes are designed in physical-layer to provide message encryption and integrity authentication. For example, these encryption schemes are schemes based on orthogonal frequency division multiplying [22], on frequency hopping spread spectrum [23], on chirp spread spectrum [24], and on phase shift keying [25], while these authentication schemes are based on received signal strength [26], on channel state information [27], on channel frequency response [28]. To achieve data confidentiality, data integrity, and source authentication simultaneously, different message authentication encryption (MAE) algorithms have been proposed to improve security and efficiency performance. These MAE schemes either artfully combine an encryption scheme and an authentication scheme [29], [30], [31] or achieve authentication based on encryption [32].

However, these schemes mentioned above generally need a second pass to authenticate messages and demand too many computational resources, so they are not suitable for resource-limited IoT devices. These problems motivate us to design a secure communication scheme that can encrypt and authenticate messages efficiently in a lightweight way and that has enough secrecy and security to defend eavesdroppers and attackers. Therefore, we propose an efficient and lightweight secret communication scheme to simultaneously implement key generation, encryption, and authentication for IoT devices, named the enhanced MAE scheme based on PKG. The main contributions are as follows:

- We proposed a new secure communication architecture integrating the PKG with the enhanced MAE. This architecture can meet the secure requirements of IoT devices. The PKG exploits the random nature of wireless channels to generate and negotiate keys, which are further utilized in the enhanced MAE to encrypt and authenticate users' data.
- An enhanced MAE algorithm is further proposed to improve the security performance in a lightweight way. On the one hand, the security of the enhanced MAE algorithm is strengthened by the PKG. On the other hand, the enhanced MAE algorithm adopts a dynamic keyed primitives construction (KPC) algorithm. The enhanced MAE takes one round and single pass structure to encrypt and authenticate messages simultaneously in a lightweight way.
- The security performance of the proposed enhanced MAE algorithm is evaluated using theoretical analysis and computer simulations. The simulation results confirm the validity and reliability of PKG. They also show that the enhanced MAE algorithm can provide data confidentiality and integrity and significantly outperform the AES algorithm by 80.5% in terms of execution efficiency. Finally, the cryptographic analysis further confirms that the enhanced MAE algorithm can resist attacks on confidentiality and authentication.

The rest of the paper is organized as follows. The system model is presented in Section II. The proposed enhanced MAE based on PKG is presented in Section III. Simulation results and analysis are presented in Section IV. Section V concludes this paper.

2. System Model

We consider an IoT network with devices having limited computing power and memory. The IoT architecture is divided into three components: core network, gateways, and sub-networks, as depicted in **Fig. 1**. Devices are grouped into sub-networks and communicate with other sub-networks via gateways. These gateways are linked together via a core network. The proposed schemes are deployed at the device end and gateway end, as shown in **Fig. 1**. The PKG is executing on the physical layer of the network protocol stack, while the enhanced MAE is executing on the application protocol layer.

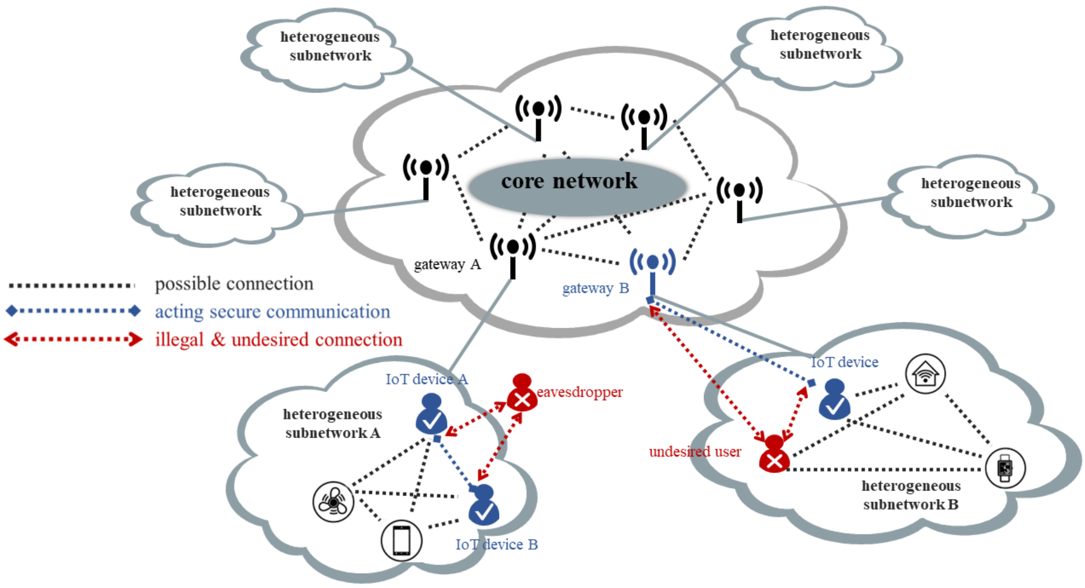

Fig. 1. The system model of the proposed scheme. Both external eavesdroppers and internal undesired users can be the attacker of a secure communication session.

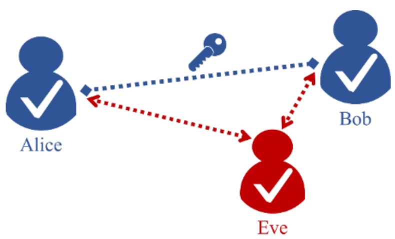

Fig. 2. The basis of physical key generation: reciprocity and spatial uncorrelation

Herein, we consider an abstract uniform attack model extracted from **Fig. 1**, as shown in **Fig. 2**. The abstraction is reasonable because we assume that Eve can move freely in space, but it is difficult to reach within a few half-wavelengths of Bob. Thus, these two cases are equivalent. We denote Alice and Bob as the legal users and Eve as the illegal user, e.g., the external eavesdropper or internal undesired user. The channel between Alice and Bob is assumed to be approximately static in a coherence duration. Alice and Bob must accomplish key negotiation and secret communication in the public wireless channel; that is, Eve can eavesdrop on their signals.

According to Kerchkoff's principle, a cipher system's security should rely only on the secrecy of keys. The secret key is generated from some randomness sources either at one end and then transmitted to another (i.e., key distribution) or derived at two ends simultaneously (i.e., key negotiation). By using the fundamental idea of PLS, the PKG technology is a good candidate for key negotiation. The PKG technology is based on the reciprocity, spatial uncorrelation and temporal variation of physical-layer channels. Reciprocity guarantees that two users can get duplicate secret keys, spatial uncorrelation provides legal users with information advantages over illegal users, and temporal variation is the randomness source. Consequently, Alice and Bob can generate strongly correlated data from channels while keeping weakly correlated to Eve's, as shown in **Fig. 2**. This information advantage is derived from the physical properties of wireless channels. We will present the proposed enhanced MAE algorithm based on physical layer key generation in the next section.

3. The Proposed Enhanced Message Authentication Encryption Based on Physical-Layer Key Generation

The security of the proposed scheme is strengthened by the PKG technology and dynamic KPC procedure. The efficiency of the proposed scheme is guaranteed by the fixed-point operations and one-round architecture of the enhanced MAE algorithm. In this section, we will explicitly show the details of the PKG technology and the enhanced MAE algorithm.

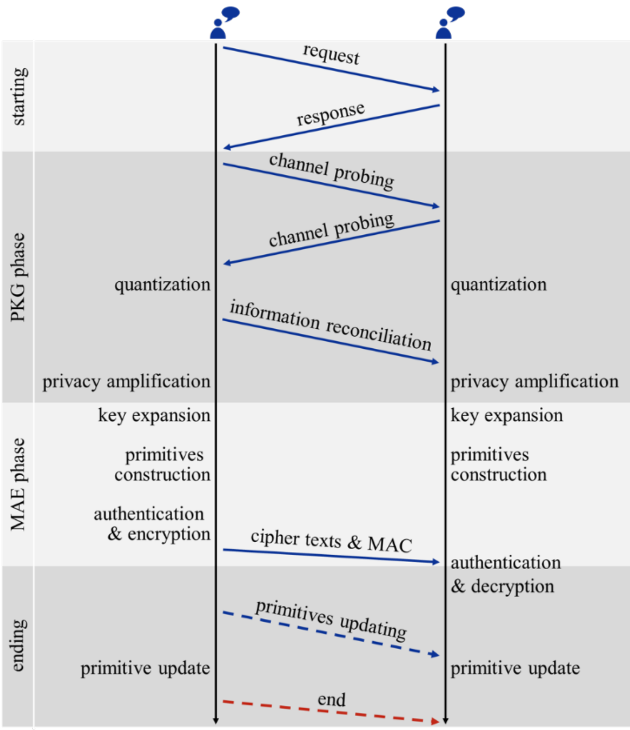

Fig. 3. The running schematic diagram of the proposed communication scheme.

3.1 A Complete Communication Session

We call a complete transmission process of data as a session and a unit of bits in a transmission procedure as a message, which will carry control information or data information. The operation process of a complete communication session is described as shown in **Fig. 3**. To be specific, 1) Alice firstly sends a request message, and then Bob replies with a response message, and a communication session will be established. 2) Both Alice and Bob send known pilot frequencies for channel probing, and then they quantify their probing data individually. 3) Alice sends correcting information to Bob for information reconciliation, and then they amplify privacy separately to derive keys. Thus, Alice and Bob obtain the same key. 4) Alice transmits encrypted data to Bob with the resulting key. Specifically, Alice divides the session key into subkeys and constructs cryptographic primitives. Alice further performs encryption and authentication algorithms to generate the cipher text and message authentication code

(MAC). Finally, the cipher texts and MACs are sent to Bob. 5) Bob decrypts the cipher texts and verifies the MACs. A complete secure communication session is finished. Alice can decide whether to update the primitives and continue communicating or terminate the session.

3.2 Physical-Layer Key Generation

The proposed scheme incorporates the classical architecture of PKG, which consists of four steps: channel probing, quantization, information reconciliation, and privacy amplification.

- *Channel Probing:* First, Alice and Bob broadcast known pilot signals to enable each other to estimate the physical-layer channel characteristics [11]. In our case, received signal strength at the antenna of the radio frequency frontend is exploited since it can be measured and read directly by present IoT devices. The temporally variant electromagnetic environment gives randomness of the probing data, which is assumed in statistical channel models, such as the Rayleigh fading model or the Rician fading model.
- *Quantization:* The second step is quantization in which the bit sequences are generated from channel measurements [33]. In the proposed scheme, we perform lossless multi-level quantile-based quantization for its trade-off between computation complexity and quantization efficiency. The quantization performs as follows:

$$Quantize(h_i) = k \text{ if } Q_{k-1} < h_i \le Q_k, 1 \le k \le q, \forall i. \tag{1}$$

where $h_i \in \mathrm{H}$ is channel measurements, q is quantization level, and $Q_i, 1 \le i \le q$ is quantiles of H. Then the decimal quantization results will be coded through Gray code to reduce the mismatching ratio.
- *Information Reconciliation:* Alice and Bob need to eliminate mismatching bits due to previous steps and reconcile bit sequences they owned. In our case, we use low-density parity code (LDPC) to reconcile bit sequences because it inherently has the correcting capability and requires lower computation resources. The bit sequences will be divided into groups to be reconciled.
- *Privacy Amplification:* The final step of PKG is to extract a sequence with higher entropy and security from the previous sequences. In this paper, we offer two candidates to amplify the privacy, a 512-bit secure hash function (SHA-512) and a 128-bit photon hash function (PHOTON-128) [34], depending on the highlight of more security or more execution efficiency.

3.3 Enhanced Message Authentication Encryption

In our proposed scheme, the enhanced MAE algorithm consists of four parts: session key splitting, primitives construction, round keys expansion, and authentication and encryption/decryption algorithms. After obtaining a session key generated from PKG, the enhanced MAE first divides the session key into subkeys, then constructs cryptographic primitives such as substitution tables and permutation tables via Rivest cipher 4 keyed setup algorithm (RC4-KSA) [35]. Finally, authentication and encryption are performed using constructed primitives and expanded round keys to generate cipher texts and MACs.

3.3.1 Session Key Splitting

In each session, the enhanced MAE algorithm takes a 512-bit session key (SK) as input, and then the SK will be divided into eight parts, each with 64 bits, to construct primitives of cryptography algorithm as shown in **Table 1**. The three updating subkeys are optional: if Alice demands more security in one session, Alice can inform Bob to update primitives using these subkeys.

3.3.2 Primitives Construction

Dynamic cryptographic primitives can reduce the number of rounds to the minimum possible value of just one round, which minimizes the computational overhead without degrading the security level [36]. Therefore, RC4-KSA is performed to construct primitives. The size of the table built by RC4-KSA is 256 for S1, S2, or the length in bytes of the plain text or round keys for π, π_{RK} [35].

Table 1. The division of session key.

Subkey	Name	Primitives Constructed
KS1	Substitution	Substitution table S1
KS2	Substitution	Substitution table S2
KP	Permutation	Permutation table π
KRK	Round keys	Round keys RK
KSRK	Selection round keys	Permutation table π_{RK}
KUS	Update substitution	Substitution table S_{US}
KUP	Update permutation	Permutation table π_P
KUSRK	Update selection round keys	Permutation table π_{SRK}

3.3.3 Round Keys Expansion

Round keys expansion is the procedure that uses KRK to expand to round keys. In the proposed algorithm, the key expansion algorithm in AES is utilized for its efficiency and lightweight.

3.3.4 Authentication and Encryption Algorithm

The proposed enhanced MAE algorithm authenticates and encrypts the messages in a single-pass way. By padding zeros at the end, the Tb bytes plain text M can be divided into two equal parts with length of $n/2$ bytes. These two parts will be operated in an efficient parallel mode to generate cipher text C, as shown in Algorithm 1. MAC_{tx} is MAC generated at the transmitter, while MAC_{rx} is at the receiver. IV_0 is the initial vector to generate the final MAC. $M[\pi(i)]$ refers to the $\pi(i)$-th input plain text block, similar to $RK[\pi_{RK}(i)]$. In the i-th round ($1 \leq i \leq n/2$), two input blocks ($M[\pi(i)]$ and $M[\pi(i+n/2)]$) are encrypted and stored at the cipher text blocks $C[i]$ and $C[i+n/2]$ by doing the following operations:

- The $\pi(i)$-th plain text block $M[\pi(i)]$ is mixed (exclusive-or) with the $\pi_{\mathrm{RK}}(i)$-th round key $\mathrm{RK}[\pi_{\mathrm{RK}}(i)]$.
- Substitute $M[\pi(i)] \oplus \mathrm{RK}[\pi_{\mathrm{RK}}(i)]$ by $S1$ to produce tp1.
- Mix the plain text block $M[\pi(i+n/2)]$ with the round key $\mathrm{RK}[\pi_{RK}(i+n/2)]$ and tp1.
- Substitute $M[\pi(i+n/2)] \oplus \mathrm{RK}[\pi_{\mathrm{RK}}(i+n/2)] \oplus$ tp1 by $S2$ to produce tp2.
- Mix tp1 and tp2 to produce the i-th cipher text block $C[i]$.
- The $(i+n/2)$-th cipher text block $C[i+n/2]$ is tp2.
- Mix tp1 and tp2 and the previous IV to produce the current IV.
- The last IV block $\mathrm{IV}[n/2]$ is mixed with $(n/2)$-th cipher text block $C[n/2]$, then substituted by S1 and S2 to produce MAC_{tx}.

The decryption algorithm follows the same steps; however, 1) it uses the inverse round function RF^{-1}, which operates in reverse order and 2) RF^{-1} employs inverse substitution tables $\mathrm{S1}^{-1}$ and $\mathrm{S2}^{-1}$. The decryption algorithm is described in Algorithm 2. In particular, line 1 to 4 is to construct inverse substitution tables $\mathrm{S1}^{-1}$ and $\mathrm{S2}^{-1}$. In a single pass of encryption and decryption, the primitives keep no change.

Algorithm 1 The enhanced MAE algorithm: encryption.

Require: M, S1, S2, π, RK, π_{RK}, IV_0, n
Ensure: C, MAC_{tx}
$\text{IV}[0] = \text{IV}_0$;
for $i = 1 \rightarrow n/2$ **do**
  $\texttt{tp1} = \text{S1}(M[\pi(i)] \oplus \text{RK}[\pi_{\text{RK}}(i)])$;
  $\texttt{tp2} = \text{S2}(M[\pi(i + n/2)] \oplus \text{RK}[\pi_{\text{RK}}(i + n/2)] \oplus \texttt{tp1})$;
  $C[i] = \texttt{tp1} \oplus \texttt{tp2}$;
  $C[i + n/2] = \texttt{tp2}$;
  $\text{IV}[i] = \text{IV}[i-1] \oplus \texttt{tp1} \oplus \texttt{tp2}$;
end for
$\text{IV}_f = \text{IV}[n/2]$;
$\text{MAC}_{tx} = \text{S2}(\text{S1}(\text{IV}_f \oplus C[n/2]))$;
return C, MAC_{tx}

Algorithm 2 The enhanced MAE algorithm: decryption

Require: C, S1, S2, π, RK, π_{RK}, IV_0, n
Ensure: M, MAC_{rx}
for $i = 0 \rightarrow 255$ **do**
  $\text{S1}^{-1}(\text{S1}(i)) = i$;
  $\text{S2}^{-1}(\text{S2}(i)) = i$;
end for
$\text{IV}[0] = \text{IV}_0$;
for $i = 1 \rightarrow n/2$ **do**
  $\texttt{tp2} = C[i + n/2]$;
  $\texttt{tp1} = C[i] \oplus \texttt{tp2}$;
  $M[\pi(i + n/2)] = \text{S2}^{-1}(\texttt{tp2}) \oplus \texttt{tp1} \oplus \text{SK}[\pi_{\text{RK}}(i + n/2)]$;
  $M[\pi(i)] = \text{S1}^{-1}(\texttt{tp1}) \oplus \text{SK}[\pi_{\text{RK}}(i)]$;
  $\text{IV}[i] = \text{IV}[i-1] \oplus \texttt{tp1} \oplus \texttt{tp2}$;
end for
$\text{IV}_f = \text{IV}[n/2]$;
$\text{MAC}_{rx} = \text{S2}(\text{S1}(\text{IV}_f \oplus C[n/2]))$;
return C, MAC_{rx}

Compared with the AES algorithm which operates the input text block many rounds to generate cipher texts; the enhanced MAE encrypts each plain text block in one round. The MAC is produced simultaneously with the cipher texts through a single pass. The efficiency of the enhanced MAE is improved by the architecture of one round and single pass.

3.4 Complexity Analysis

The computation and memory consumption of the PKG scheme are determined after configuring the system. We analyze the complexity of the enhanced MAE algorithm. The proposed enhanced MAE takes n bytes plain texts as input, performs $n + 2$ times look-up operation, and produces n bytes cipher texts while using 3 single-byte temporary variables (IV, ~tp2 and tp2), so the computation complexity is $O(n + 2)$. In the meantime, AES algorithm will perform 10 iterations for every 16 bytes; in each iteration, there are 16 times look-up and a 16-byte state temporary variable, as well as other operations, so the computation complexity is $O(10n)$. The MAE algorithm proposed in [37] has computation complexity of $O(3n + 1)$, $O(3n + 2)$ and $O(2n + 1)$ for the three variants, respectively. In summary, the proposed enhanced MAE algorithm has low computation complexities and low memory consumption compared to AES and conventional MAE algorithms.

4. Simulation Results and Analysis

4.1 Numerical Results of PKG

We numerically simulate the PKG on the MATLAB R2023a platform in Windows 11 with 12th Gen Inter® Core™ i5-1240P CPU. We set the quantization level $q = 8$. By standard [11], We utilize LDPC with the 168×672 generation matrix, which will take $n = 672$ bit sequence as input and generate $k = 168$ bit parity code. The coding rate, by definition, is $(n - k)/n = (672 - 168)/672 = 3/4$. The generation matrix is shown in **Table 2**, and the example of the cyclic permutation matrix is in **Table 3**. Note: the -1 represents matrices with all 0s.

Table 2. The LDPC generation matrix with rate 3/4 of block size.

35	19	41	22	40	41	39	6	28	18	17	3	28	-1	-1	-1
29	30	0	8	33	22	17	4	27	28	20	27	24	23	-1	-1
37	31	18	23	11	21	6	20	32	9	12	29	-1	0	13	-1
25	22	4	34	31	3	14	15	4	-1	14	18	13	13	22	24

Table 3. Two examples of cyclic permutation matrix P_n^Z, where $Z = 4$ and $n = 0,1$.

1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1

P_0^4

0	1	0	0
0	0	1	0
0	0	0	1
1	0	0	0

P_1^4

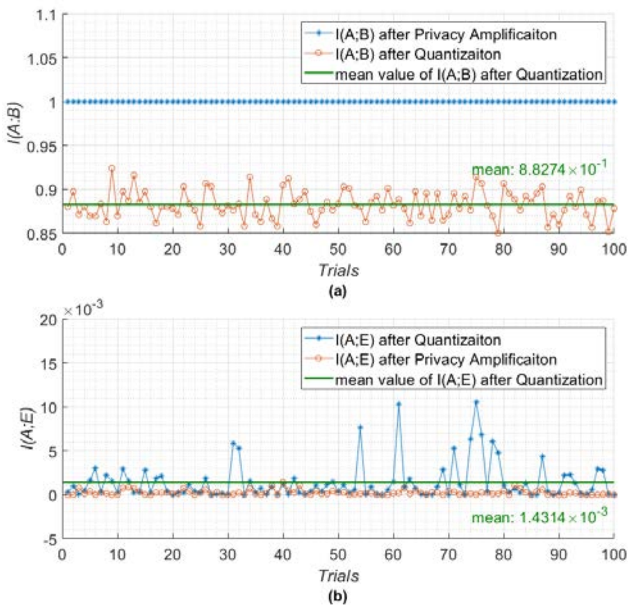

Fig. 4. Mutual information (a) between Alice and Bob, (b) between Alice and Eve.

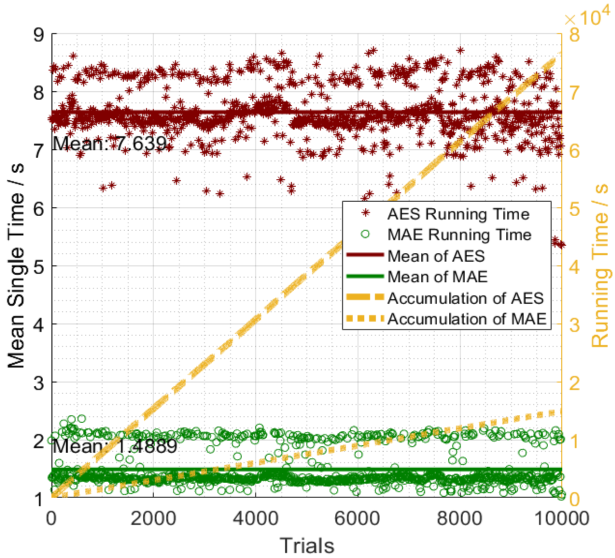

Fig. 5. Running times of enhanced MAE v.s. typical AES

The simulation is performed 100 times. **Fig. 4** shows the mutual information between Alice and Bob and between Alice and Eve at the point of quantization and privacy amplification. From **Fig. 4 (a)**, we can see that the mutual information between Alice and Bob increases to 1.000 after privacy amplification from an average of 0.883 after quantization. From **Fig. 4 (b)**, we can see that the mutual information between Alice and Eve decreased to 0.000 after amplification from an average of 1.434×10^{-3} after quantization. That is, Eve almost possesses no information about Alice's bit sequence after the process of PKG. It can be confirmed from **Fig. 4** that the PKG technology guarantees the privacy and secrecy of Alice and Bob.

To compare the execution time of PKG utilizing SHA-512 and PHOTON-128 hash algorithms, we performed 10000 PKG trials, and the result is shown in **Table 2**. For the SHA-512 hash algorithm, the input length is 672, and the hash value length is 512. For the PHOTON-128 hash algorithm, the input sequence is divided into 4 168-bit subsequences to be separately hashed, and the 4 128-bit hash value is appended to a 512-bit output. Thus, if we assume the attacker can generate p messages in the lifetime of the key (a secure communication session), the collision probability of SHA-512, CP_{SHA} is

$$CP_{SHA} = \frac{p(p-1)/2}{2^{512+1}} \tag{2}$$

while the collision probability of PHOTON-128, CP_{PHOTON} is

$$CP_{PHOTON} = \frac{p(p-1)/2}{2^{128+1}} \times 4 \tag{3}$$

The latter is about $2^{512+1-(128+1-2)} = 2^{385} \approx 7.8804 \times 10^{115}$ times the former. SHA-512's security is highly more significant than that of PHOTON-128. Meanwhile, as shown in **Table 4**, SHA-512's execution time is about 119 times that of PHOTON-128. So, according to the highlight on security or efficiency, we can choose to use one of these two hash functions.

Table 4. The statistical results of execution time (seconds) of SHA-512 and PHOTON-128.

Algorithm	Min	Std	Max	Mean
SHA-512	2.4690	0.0287	3.1743	2.5111
PHOTON-128	0.0193	5.8616×10^{-4}	0.0469	0.0211

In addition, we perform the NIST SP 800-22 randomness test for keys generated by the proposed PKG scheme, and the results are shown in **Table 5**. It confirmed that our PKG scheme can produce secret keys with sufficient randomness and can be utilized in cipher algorithms.

Table 5. The results of NIST SP 800-22 randomness tests.

Test	Pass proportion	Result
Frequency	20/20	Success
BlockFrequency	20/20	Success
CumulativeSums	40/40	Success
Runs	20/20	Success
LongestRun	20/20	Success
Rank	20/20	Success
FFT	19/20	Success
NonOverlappingTemplate	2932/2960	Success
OverlappingTemplate	20/20	Success
Universal	20/20	Success
ApproximateEntropy	20/20	Success
RandomExcursionsVariant	103/104	Success
Serial	40/40	Success
LinearComplexity	20/20	Success

4.2 Numerical Results of Enhanced MAE

4.2.1 Performance Analysis

To demonstrate the efficiency, the enhanced MAE is compared with a PKG-assisted AES scheme in terms of running time. For fairness, both the enhanced MAE and AES [40] are implemented on the MATLAB platform. Both of them encrypt the same plain texts in each trial, and the simulation is performed in 10,000 trials. The running time of the two schemes is shown in **Fig. 5**. It can be seen from **Fig. 5** that the running time of the enhanced MAE is an average of 1.489 ms per encryption, while the PKG-assisted AES takes an average of 7.639 ms to perform one encryption. It can be proven from **Fig. 5** that the performance of the proposed scheme improves by 80.5% in terms of algorithm execution efficiency with respect to the typical AES scheme.

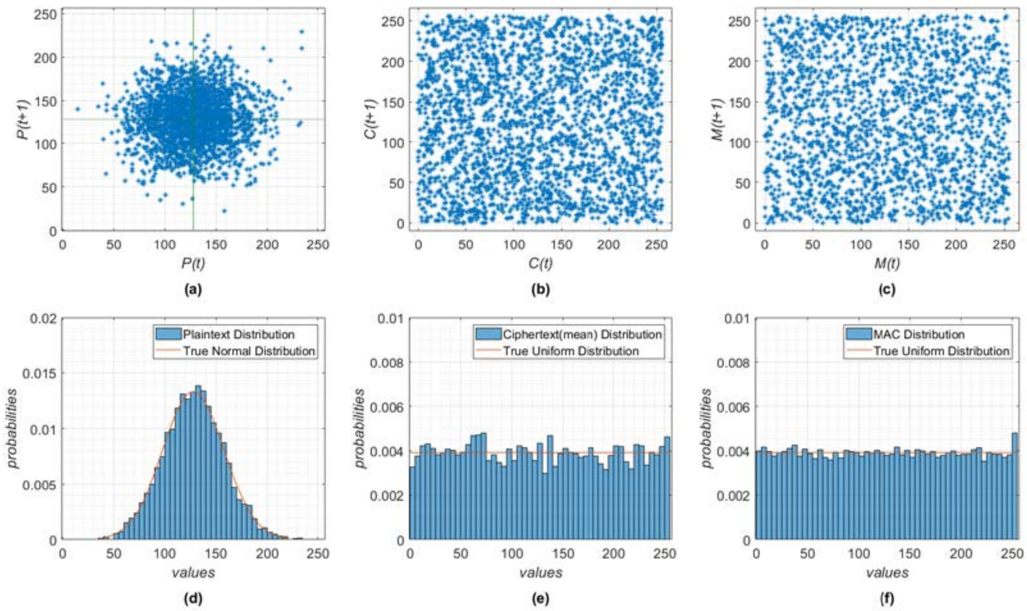

Fig. 6. Statistical analysis results: the recurrence of the plain texts(a) and cipher texts (b), the corresponding PDF of the plain texts (d) and produced cipher texts (e), and recurrence histogram distribution (c) and histogram distribution (f) of MAC in hexadecimal format.

4.2.2 Statistical Analysis

To resist statistical attacks, the occurrence probability of all symbols in the cipher texts should be close to $1/s$, where s denotes the symbols' space. The symbols' space in the enhanced MAE is 256 since the cipher texts and MACs are operated in bytes. Similarly, the occurrence probability of all symbols in the MAC should also be close to $1/s$ because the number of bytes in MAC is equal to the number in cipher text blocks. This could be assessed statistically, in particular by visualizing the probabilistic density function (PDF) of the encrypted message and the generated MACs. The same plain text is encrypted with 10,000 random session keys. The statistical results at the byte level are shown in **Table 6**, **Fig. 6** and **Fig. 7**.

Table 6. The statistical results of MAE algorithm.

Variable	Min	Mean	Max	Std
Plain Texts	15.000	127.6094	234.000	29.8694
Cipher Texts	0.000	127.4924	255.000	73.8882
Theoretical Value	0	127.5	255	73.8297
MAC	0.000	126.9878	255.000	73.9921
Theoretical Value	0	127.5	255	73.8297

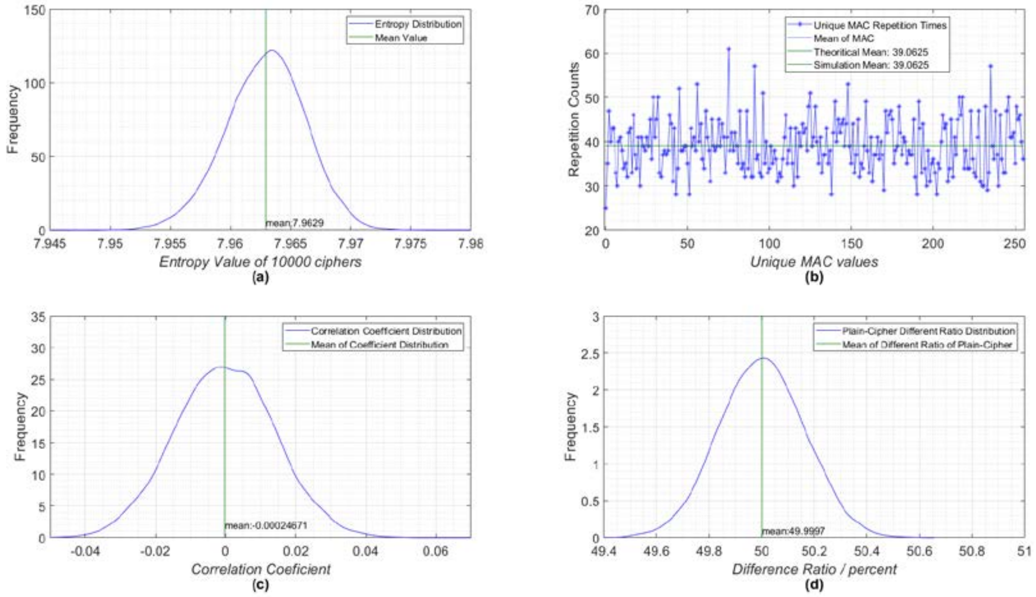

Fig. 7. Statistical analysis results: (a) PDF of the cipher texts entropy, (b) PDF of the unique MAC values, (c) PDF of the correlation coefficient, and (d) PDF of the percentage difference between plain and cipher texts.

Table 6 shows the numerical characteristics of plain texts, produced cipher texts, and MACs at the byte level, compared with theoretical values. It is seen that the produced cipher texts obey a uniform distribution from 0 to 255.

From **Fig. 6**, it is seen that the PDF of the original plain texts is not uniform, but the PDF of corresponding produced cipher texts and MACs follows the uniform distribution. At the same time, all symbols have a probability of occurrence close to $(1/256) = 0.039$.

The results are also validated by the entropy and difference ratio at the data message level. If the entropy value of the produced cipher texts is close to $(-\log_2 1/256) = 8$, the uniformity of texts is satisfied. **Fig. 7 (a)** illustrates the PDF of the entropy values of 10,000 cipher texts. The result shows clearly that the encrypted ciphers always have an entropy close to the desired value of 8. **Fig. 7 (b)** demonstrates the repetition counts of each unique symbol of the 10,000 produced MACs. The result shows that the produced MACs are arbitrarily distributed in the symbols' space.

On the other hand, in addition to the previous recurrence results, two additional tests can be performed to evaluate the randomness level of the cipher texts: 1) the correlation between plain and cipher texts and 2) the difference ratio (DR) of the original texts and the produced cipher texts. The DR between plain and cipher texts is calculated by (4).

$$\mathrm{DR}(S_A, S_B) = \frac{\sum_{i=1}^{m} D_i}{Tb} \times 100\% \tag{4}$$

where S_A, S_B is two sequences of bits, m is the length in bits of S_A, S_B, and

$$D_i = \begin{cases} 1, & S_A(i) \neq S_B(i) \\ 0, & S_A(i) = S_B(i) \end{cases} \tag{5}$$

The PDF of the correlation coefficient of plain and cipher texts is illustrated in **Fig. 7 (c)**. It is seen that the correlation coefficients concentrate highly around 0. The PDF of the DRs of plain and cipher texts is shown in **Fig. 7 (d)**. It is clear that the DR also concentrates highly around 50%. The coefficient and DR results validate the randomness of cipher texts since the desired results are derived from simulation tests.

In conclusion, **Fig. 6** and **Fig. 7** confirm the randomness and uniformity of the proposed enhanced MAE algorithm. Simulation results confirm the good diffusion and confusion properties of this scheme, which enable the enhanced MAE to resist statistical attacks.

The key avalanche effect (KAE), or the key sensitivity, refers to the effect that a 1-bit flipped in session key should result in 50% of bits changed in produced cipher texts and MACs. Similarly, the plain avalanche effect (PAE) refers to the effect that a 1-bit flipped in plain texts should result in 50% of bits changed in MACs (the cipher texts should change one block because it is a one-round algorithm). The test of KAE is performed in 5,000 trials. Within each KAE test trial, the same plain text is encrypted with a random key and another key with one bit changed in the former one. The test of PAE is also performed in 5,000 trials. Within each PAE test trial, a plain text and another plain text with one bit changed in the former one are encrypted with the same random key.

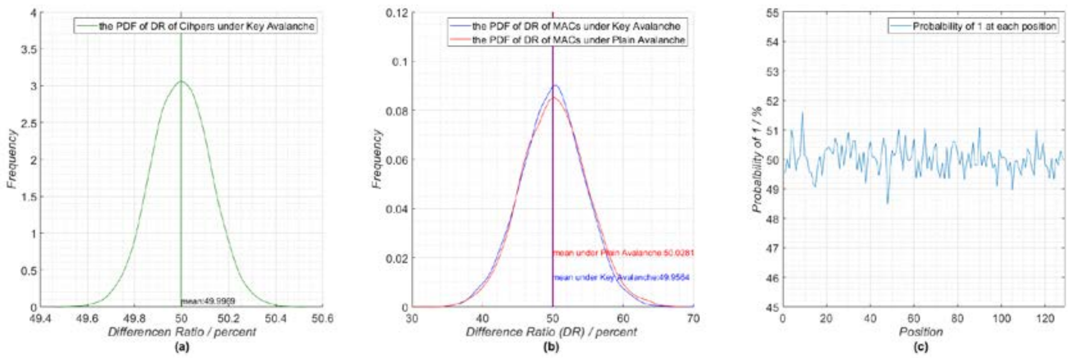

Fig. 8. The statistical results of key avalanche and plain avalanche test:(a) PDF of difference ratio of ciphers, (b) PDF of difference ratio of MACs of key and plain avalanche effect (c) the probabilities of each position in MAC with 1-bit flipping in plain.

The results of the PAE and KAE tests are shown in **Fig. 8**. **Fig. 8 (a)** illustrates the PDF of the DR of cipher texts in each KAE test trial. It is clear that the DR of cipher texts encrypted with only one-bit changed keys is 50%, i.e., totally different. **Fig. 8 (b)** illustrates the PDF of the DR of MACs in KAE and PAE tests. It shows that the DR of MACs is almost all 50%. It is seen that the produced MAC will change randomly at each bit when the input keys (KAE) or plain texts (PAE) have only one-bit change. **Fig. 8 (c)** exhibits the probability of 1 occurrence at each position in MACs produced by PAE tests. It is seen that at each position of MAC, 1 or 0 appear with equal probabilities.

In conclusion, the enhanced MAE is very sensitive to changes in input plaint texts and keys, which will strengthen its capability of resistance to statistical attacks.

4.3 Cryptographic Analysis of the Enhanced MAE

The key space of the proposed enhanced MAE algorithm is 2^{256}, which can prevent brute force attacks since it is greater than 2^{128} [41]. The proposed scheme is of great resistance against linear attacks and differential attacks, which is guaranteed by

- the independence of plain texts and cipher texts (**Fig. 6 (c)** and **(d)**), and
- the nonlinear relationship enhanced by the permutation table π and π_{RK}, and
- secret key sensitivity (**Fig. 8**) [37].

At the same time, the key-related attacks are tough to perform since a one-bit change in the session key will produce enormously different ciphers and MACs. In Summary, the proposed encryption algorithm is secure enough to resist attacks on confidentiality.

The resistance against attacks on authentication of the proposed scheme is ensured by 1) that the MAC is produced by all the plain texts and session keys, 2) that the dynamic primitives and variable session keys of each new session, and 3) that each MAC incorporates all the nonlinear tables as the compressive function. Given a message with n blocks and Tb bytes per block, $M = [m_1, m_2, \ldots, m_{n\times Tb}]$. The birthday attack seeks two messages with identical MAC values in less than $2^{8\times Tb/2}$ trials [37], but Tb can be easily expanded to make brute force attacks impossible. The *meet-in-the-middle* attack is to find a plain text block m_i to be replaced without changing the produced MAC value [42]. According to **Fig. 8 (b)** and **(c)**, the plain text sensitivity of the enhanced MAE will resist meet-in-the-middle attack. Moreover, the number of bytes per block Tb and the length of plain text n are large in practice. The space to find collisions for MACs is vast, making the meet-in-the-middle attack extremely difficult. In conclusion, the proposed enhanced MAE algorithm can resist attacks on authentication.

5. Conclusion

In this paper, a lightweight and efficient PKG-based enhanced MAE algorithm has been proposed to ensure the security of resource-limited IoT. On the one hand, the PKG has been used to improve the security performance in a lightweight way. On the other hand, the low-complexity variant of the MAE algorithm has been proposed and further strengthened by the PKG. The enhanced MAE algorithm is based on the keyed primitives construction, in which we construct permutation tables and substitution tables by the RC4-KSA algorithm. The statistical results of simulations proved that the PKG technology meets the secure and secret demand. The quantitative statistical results and qualitative cryptography analysis confirm the security of the enhanced MAE algorithm in resistance against attacks on confidentiality and authentication. Compared to the benchmark, i.e., the PKG-based AES scheme, the proposed scheme improves by 80.5% in terms of execution efficiency. The lightweight and high efficiency of the proposed scheme make it applicable for resource-limited IoT networks.

References

[1] S. Javanmardi, M. Shojafar, R. Mohammadi, M. Alazab, and A. M. Caruso, "An SDN perspective IoT-Fog security: A survey," *Computer Networks*, vol.229, Jun. 2023. Article(CrossRefLink)

[2] M. B. Mohamad Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," *Computer Networks*, vol.148, pp.283-294, Jan. 2019. Article(CrossRefLink)

[3] D. Chawla and P. S. Mehra, "A roadmap from classical cryptography to post-quantum resistant cryptography for 5G-enabled IoT: Challenges, opportunities and solutions," *Internet of Things*, vol.24, Dec. 2023. Article(CrossRefLink)

[4] M. Kumar and D. Kalra, "Efficient and lightweight data encryption scheme for embedded systems using 3D-LFS chaotic map and NFSR," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol.5, Sep. 2023. Article(CrossRefLink)

[5] S. Liu and G. Ye, "Asymmetric image encryption algorithm using a new chaotic map and an improved radial diffusion," *Optik*, vol.288, Oct. 2023. Article(CrossRefLink)

[6] M. Tanveer, A. K. Bashir, B. A. Alzahrani, A. Albeshri, K. Alsubhi, and S. A. Chaudhry, "CADF-CSE: Chaotic map-based authenticated data access/sharing framework for IoT-enabled cloud storage environment," *Physical Communication*, vol.59, Aug. 2023. Article(CrossRefLink)

[7] C. Chauhan, M. K. Ramaiya, A. S. Rajawat, S. B. Goyal, C. Verma, and M. S. Raboaca, "Improving IoT Security Using Elliptic Curve Integrated Encryption Scheme with Primary Structure-Based Block Chain Technology," *Procedia Computer Science*, vol.215, pp.488-498, 2022. Article(CrossRefLink)
[8] B. Li, Z. Fei, C. Zhou, and Y. Zhang, "Physical-Layer Security in Space Information Networks: A Survey," *IEEE Internet Things J.*, vol.7, no.1, pp.33-52, Jan. 2020. Article(CrossRefLink)
[9] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol.39, no.3, pp.733-742, May 1993. Article(CrossRefLink)
[10] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inform. Theory*, vol.39, no.4, pp.1121-1132, Jul. 1993. Article(CrossRefLink)
[11] Z. Wang et al., "A Reliable Physical Layer Key Generation Scheme Based on RSS and LSTM Network in VANET," *IEEE Internet Things J.*, pp.692-707, 2024. Article(CrossRefLink)
[12] J. Li, P. Wang, L. Jiao, Z. Yan, K. Zeng, and Y. Yang, "Security Analysis of Triangle Channel-Based Physical Layer Key Generation in Wireless Backscatter Communications," *IEEE Transactions on Information Forensics and Security*, vol.18, pp.948-964, 2023. Article(CrossRefLink)
[13] H. Luo, N. Garg, and T. Ratnarajah, "A Channel Frequency Response-Based Secret Key Generation Scheme in In-Band Full-Duplex MIMO-OFDM Systems," *IEEE J. Select. Areas Commun.*, vol.41, no.9, pp.2951-2965, Sep. 2023. Article(CrossRefLink)
[14] Z. Wan et al., "Physical-layer key generation based on multipath channel diversity using dynamic metasurface antennas," *China Commun.*, vol.20, no.4, pp.153-166, Apr. 2023. Article(CrossRefLink)
[15] S. Zhang, L. Jin, Y. Lou, and Z. Zhong, "Secret key generation based on two-way randomness for TDD-SISO system," *China Commun.*, vol.15, no.7, pp.202-216, Jul. 2018. Article(CrossRefLink)
[16] Q. He, N. Zhang, Y. Wei, and Y. Zhang, "Lightweight attribute based encryption scheme for mobile cloud assisted cyber-physical systems," *Computer Networks*, vol.140, pp.163-173, Jul. 2018. Article(CrossRefLink)
[17] M. Rasori, M. L. Manna, P. Perazzo, and G. Dini, "A Survey on Attribute-Based Encryption Schemes Suitable for the Internet of Things," *IEEE Internet Things J.*, vol.9, no.11, pp.8269-8290, Jun. 2022. Article(CrossRefLink)
[18] A. Haj-Hassan, Y. Imine, A. Gallais, and B. Quoitin, "Consensus-based mutual authentication scheme for Industrial IoT," *Ad Hoc Networks*, vol.145, Jun. 2023. Article(CrossRefLink)
[19] C. Gonçalves, B. Sousa, M. Vukovic, and M. Kusek, "A federated authentication and authorization approach for IoT farming," *Internet of Things*, vol.22, Jul. 2023. Article(CrossRefLink)
[20] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," *IEEE Internet Things J.*, vol.2, no.1, pp.72-83, Feb. 2015. Article(CrossRefLink)
[21] C. Zhao, M. Huang, L. Huang, X. Du, and M. Guizani, "A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks," *Computer Networks*, vol.128, pp.164-171, Dec. 2017. Article(CrossRefLink)
[22] J. Liu, A. Ren, R. Sun, X. Du, and M. Guizani, "A Novel Chaos-Based Physical Layer Security Transmission Scheme for Internet of Things," in *Proc. of 2019 IEEE Global Communications Conference (GLOBECOM)*, pp.1-6, Waikoloa, HI, USA, Dec. 2019. Article(CrossRefLink)
[23] A. Alsadi and S. Mohan, "A New Frequency Hopping Scheme to Secure the Physical Layer in The Internet of Things (IoT)," in *Proc. of 2020 Wireless Telecommunications Symposium (WTS)*, pp.1-8, Washington, DC, USA, Apr. 2020. Article(CrossRefLink)
[24] F. A. Taha and S. Althunibat, "Improving Data Confidentiality in Chirp Spread Spectrum Modulation," in *Proc. of 2021 IEEE 26th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pp.1-6, Porto, Portugal, Oct. 2021. Article(CrossRefLink)

[25] S. V. Pechetti, A. Jindal, and R. Bose, "Channel-based mapping diversity for enhancing the physical layer security in the Internet of Things," in *Proc. of 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, pp.1-6, Montreal, QC, Canada, Oct. 2017. Article(CrossRefLink)

[26] J. Wang, Y. Shao, Y. Wang, Y. Ge, and R. Yu, "Physical Layer Authentication Based on Nonlinear Kalman Filter for V2X Communication," *IEEE Access*, vol.8, pp.163746-163757, 2020. Article(CrossRefLink)

[27] X. Lu, J. Lei, Y. Shi, and W. Li, "Improved Physical Layer Authentication Scheme Based on Wireless Channel Phase," *IEEE Wireless Commun. Lett.*, vol.11, no.1, pp.198-202, Jan. 2022. Article(CrossRefLink)

[28] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," in *Proc. of 2007 IEEE International Conference on Communications*, pp.4646-4651, Glasgow, UK, Jun. 2007. Article(CrossRefLink)

[29] F. De Santis, A. Schauer, and G. Sigl, "ChaCha20-Poly1305 authenticated encryption for high-speed embedded IoT applications," in *Proc. of Design, Automation & Test in Europe Conference & Exhibition (DATE), 2017*, pp.692-697, Lausanne, Switzerland, Mar. 2017. Article(CrossRefLink)

[30] S. Kumari, M. Singh, R. Singh, and H. Tewari, "A post-quantum lattice based lightweight authentication and code-based hybrid encryption scheme for IoT devices," *Computer Networks*, vol.217, Nov. 2022. Article(CrossRefLink)

[31] Z. Zhang and S. Zhou, "A decentralized strongly secure attribute-based encryption and authentication scheme for distributed Internet of Mobile Things," *Computer Networks*, vol.201, Dec. 2021. Article(CrossRefLink)

[32] K. S. Patil, I. Mandal, and C. Rangaswamy, "Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT based applications using hybrid encryption," *Pervasive and Mobile Computing*, vol.82, Jun. 2022. Article(CrossRefLink)

[33] I. Charlier, D. Paindaveine, and J. Saracco, "QuantifQuantile: An R Package for Performing Quantile Regression Through Optimal Quantization," *The R Journal*, vol.7, no.2, pp.65-80, Dec. 2015. Article(CrossRefLink)

[34] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON Family of Lightweight Hash Functions," in *Proc. of 31st Annual Cryptology Conference, Advances in Cryptology – CRYPTO 2011, Lecture Notes in Computer Science*, vol.6841, pp.222-239, Berlin, Heidelberg, 2011. Article(CrossRefLink)

[35] H. Noura, A. Chehab, L. Sleem, M. Noura, R. Couturier, and M. M. Mansour, "One round cipher algorithm for multimedia IoT devices," *Multimed. Tools Appl.*, vol.77, no.14, pp.18383-18413, Jul. 2018. Article(CrossRefLink)

[36] H. N. Noura, A. Chehab, and R. Couturier, "Efficient & secure cipher scheme with dynamic key-dependent mode of operation," *Signal Processing: Image Communication*, vol.78, pp.448-464, Oct. 2019. Article(CrossRefLink)

[37] H. N. Noura, O. Salman, R. Couturier, and A. Chehab, "A Single-Pass and One-Round Message Authentication Encryption for Limited IoT Devices," *IEEE Internet Things J.*, vol.9, no.18, pp.17885-17900, Sep. 2022. Article(CrossRefLink)

[38] "IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*, pp.1-4379, 2021. Article(CrossRefLink)

[39] Khitish, "Secure Hash Algorithms 160,224,256,384.512," SHA Algorithms 160,224,256,384.512, 2011. Article(CrossRefLink)

[40] H. David, "Advanced Encryption Standard (AES)-128,192, 256," Advanced Encryption Standard (AES)-128,192, 256, 2021. Article(CrossRefLink)

[41] W. Stallings, Cryptography and network security: principles and practice, Seventh edition. Boston: Pearson, 2017. Article(CrossRefLink)

[42] X. Wang and H. Yu, "How to Break MD5 and Other Hash Functions," in *Proc. of 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques Advances in Cryptology – EUROCRYPT 2005, Lecture Notes in Computer Science*, vol.3494, pp.19-35, Berlin, Heidelberg, 2005. Article(CrossRefLink)

Zeng Xing received the B.S. degree from School of Cybersecurity, Northwestern Polytechnical University, Xi'an, China, in 2022. He is currently pursuing the M.S. degree in Cyberspace Security with the School of Cybersecurity, Northwestern Polytechnical University. His current research interests include physical layer security, message encryption authentication in Internet of Things.

Bo Zhao received the B.S. degree in communications engineering from Shandong University of Science and Technology, Qingdao, China, in 2015. He received the Ph.D. degree in communications and information systems from Xidian University, Xi'an, China. He is currently an Associate Professor with the School of Cybersecurity, Northwestern Polytechnical University, Xi'an, China. His research interests include random multiple access techniques, resource allocation, physical layer security, and machine learning in satellite terrestrial integrated networks.

Bo Xu received the B.S. and M.S. degree from School of Software, Northwestern Polytechnical University, Xi'an, China, in 2013 and 2016. He is currently pursuing the Ph.D. degree in Cyberspace Security with the School of Cybersecurity, Northwestern Polytechnical University. His current research interests include system-of-systems combat simulation, time series analysis and forecasting, fault diagnosis and data privacy protection.

Guangliang Ren received the B.S. degree in communications engineering from Xidian University, Xi'an, China, in 1993, the M.S. degree in signal processing from the Academy of China Ordnance, Beijing, China, in 1996, and the Ph.D. degree in communications and information systems from Xidian University, in 2006. He is currently a Professor with the School of Telecommunications Engineering, Xidian University. He is the author of more than 40 research papers in journals and conference proceedings, such as IEEE Transactions on Wireless Communications, IEEE Transactions on Communications, IEEE Transactions on Vehicular Technology and an author or coauthor of three books. His research interests include wireless communications and digital signal processing, particularly multiple-input-multiple-output systems, WiMax, LTE, etc.

Zhiqiang Liu received the Ph.D degree from the School of Computer Science, Northwestern Polytechnical University, Xi'an, China, in 2008. He visited University of Illinois at Urbana Champaign (UIUC) and Portland State University (PSU) from December 2012 to January 2014. He is currently a Professor, doctoral supervisor with the School of Cybersecurity, Northwestern Polytechnical University. His current research interests include system-of-systems combat simulation, modeling and security of engine control software, data analysis and security for the full life cycle of engine and its application in health monitoring.