Exploiting Redundant Randomness for Resisting Key Exposure in Encrypted Communication Systems

Longjiang Li, *Member, IEEE*, Jie Wang, Rui Zhang, Yuanchen Gao, Yonggang Li, and Yuming Mao

***Abstract*—The exposure possibility of keys poses a great threat to almost all modern cryptography, especially in wireless communications. From the adversary's point of view, a cryptographic key can be considered as a random variable in its key space, whose security level can be measured in terms of randomness. In this article, we propose a highly exposure-resilient framework, which incorporates redundant randomness of key sources into the design of cryptographic systems to resist key exposure in encrypted communications. As hardware costs continue to decrease, the deployment of redundant randomness at the same time to achieve a better security level is affordable in the future. The framework offers a way to protect the privacy of a single key by fusing multiple redundant keys. Analysis and results demonstrate that the proposed scheme can dramatically reduce the secrecy outage probability, and provides an extensible way to enhance the encrypted communication system's resistance to unknown eavesdropping or key exposure.**

***Index Terms*—Communication security, entropy-maximizing transformation, key exposure, redundant structure, secrecy outage probability.**

I. Introduction

COMMUNICATION and information security are extremely important for almost every aspect of human activities. Especially, in wireless communications [1], information leakage through the transmission of wireless signal is unavoidable. Nowadays, the mainstream methodology for ensuring security is to encrypt all transmitted information through a symmetric cryptographic protocol, such as RC4, Advanced Encryption Standard (AES), and ChaCha [2], that presumes that the entire security depends only on the privacy or unpredictability of various private keys [3]. Due to various attacks, such as side-channel attacks and cold boot attacks [4], key exposure is becoming one of the major challenges in the key lifecycle. Asymmetric cryptographic techniques are mainly used for key exchange or refreshment [5]. However, many widely used key exchange algorithms, such as RSA, are facing the risk of keys being cracked or leaked [6], due to the imminent threat of quantum computers [7]. Thus, there has been a renewed interest in information-theoretic security, widely accepted as the strictest notions of security [8], [9], which builds on Shannon's notion of perfect secrecy [10] through maximizing the entropy from the perspective of adversaries.

However, it is often extremely difficult or expensive [11], [12] to obtain a high-quality key. From the adversary's point of view, a cryptographic key can be considered as a random variable in its key space, whose security level can be measured in terms of randomness [9]. This is why many researchers [13], [14] directly use guessing probability of keys to evaluate the security of cryptographic systems. Fortunately, we found that a class of functions, called entropy-maximizing transformations (EMTs), can be utilized to improve randomness by exploiting redundancy, which inspires us to protect a single key from the threat of key exposure through EMTs.

With the continuous reduction of hardware costs, the idea of exploiting redundancy has been widely used to improve the system reliability [15] and prevent uncertain software/hardware's backdoors or occasional failures [16], [17]. Surprisingly, redundant design has almost never been considered in cryptographic systems and the effectiveness of almost all encryption algorithms is based on the privacy of a single key at every moment [18], [19], which makes the cryptosystem extremely vulnerable to unpredictable or covert key exposure. Although key-updating approaches (KUAs) [5], [18], [19] can periodically replace the potentially leaked keys by fresh keys, a key may lose its security effect before the refreshing cycle, if the amount of leaked information is unbounded.

In this article, we propose a highly exposure-resilient framework, which incorporates the redundant randomness of key sources into the design of cryptographic systems to overcome the key exposure problem in communication systems. The basic idea is based on EMTs that can be utilized to protect a single key from the threat of key exposure in the strictest sense of min-entropy [9] through fusion with other keys, even if the amount of leaked information is unbounded. We say that such a function satisfies the entropy-maximizing property. In an encrypted communication process, EMTs start working after the two communicating parties have finished exchanging secret keys and before they start communicating, as shown in Fig. 1. With the EMTs, the quality

Manuscript received August 8, 2021; revised November 18, 2021 and January 19, 2022; accepted January 30, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61871076 and Grant 61273235, in part by the Fundamental Research Funds for the Central Universities of China under Grant ZYGX2016J001, and in part by the Defence Advance Research Foundation of China under Grant 61400020109. *(Corresponding author: Longjiang Li.)*

Longjiang Li is with the Department of Network Engineering, School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: longjiangli@uestc.edu.cn).

Jie Wang, Rui Zhang, Yuanchen Gao, and Yuming Mao are with the University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: 541056967@qq.com; 1812047438@qq.com; gyc1998@foxmail.com; ymmao@uestc.edu.cn).

Yonggang Li is with the Chongqing University of Posts and Telecommunications, Chongqing 400065, China (e-mail: lyg@cqupt.edu.cn).

Digital Object Identifier 10.1109/JSYST.2022.3149186

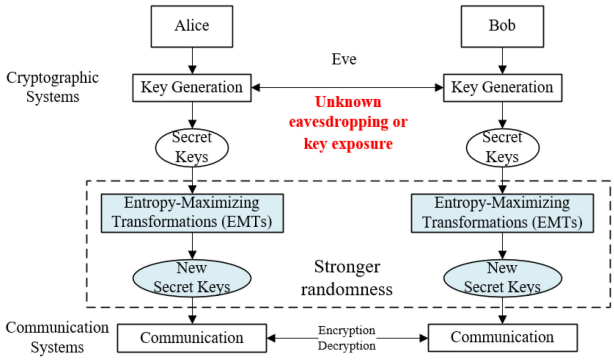

Fig. 1. Proposed exposure-resilient framework.

of the key will be improved in the sense of min-entropy. The main contributions of this article are summarized as follows.

1) A highly exposure-resilient framework for enhancing the encrypted communication system's resistance to unknown eavesdropping or key exposure by exploiting the redundant randomness in cryptographic systems.
2) A formal definition of EMTs with the entropy-maximizing property to extract a random variable with stronger randomness from a list of independent random variables.
3) A constructive proof that there are at least $(2^n!)$ instances satisfying the entropy-maximizing property for a pair of n-bit keys.
4) A closed-form formula for calculating the secrecy outage probability (SOP) based on the continuous leakage model.
5) Analysis and results demonstrating the impact of the proposed scheme on communication systems that the overall security level can be improved dramatically in terms of SOP.

The rest of this article is structured as follows. Section II reviews the related work about key exposure problems and redundant designs. Some important preliminaries are introduced in Section III. Section IV describes the core problem and presents our solution based on EMTs. Section V gives two exemplified instances for validating the entropy-maximizing property and analyzes the impact of the proposed scheme on communication systems through numerical results. Finally, Section VI concludes this article.

II. Related Work

A. Key Exposure Problems

Due to various attacks [4], key exposure is becoming one of the major challenges in the lifecycle of a key. In general, the mechanisms of generating cryptographic keys can be divided into secret key exchange or physical-layer wiretap codes [20], [21]. Most key exchange mechanisms, such as Diffie–Hellman key exchange algorithm (D-H) [22], are based on some (unproved) difficulty of mathematical problems, e.g., factoring large integers or computing discrete logarithms [23]. Although physical layer key generation mechanisms are not dependent on those unproven hypotheses [24], most of them rely on the assumption that eavesdroppers must locate at least a half a wavelength apart from legitimate users [25]. It is generally believed that quantum key distribution (QKD), as a key distribution scheme used in quantum cryptography, provides a perfect security based on quantum physics. However, there are a number of crucial challenges such as key establishment rate, distance, cost, and practical security [11], [26]. Lattice-based cryptography has the potential to resist quantum attacks [21], [27] based on some mathematical problems related to lattices, but it is still vulnerable to side channel attacks [28].

TABLE I
Advantages and Limitations of the Related Work

The related work	Advantage	Limitation
Diffie–Hellman key exchange [22]	Applicable to various scenarios including wired and wireless communications	Based on unproven hypotheses and vulnerable to quantum computer attacks
Physical-layer key generation [25] [24]	Lightweight and applicable to wireless reciprocal channel	Vulnerable to attacks of nearby eavesdroppers
Quantum Key Distribution [26] [11]	Perfectly resistant to eavesdropping based on quantum physics	Some practical limitations related to key establishment rate, distance, cost
Lattice-based cryptography [27]	Having potential to resist quantum attacks	Highly complex and vulnerable to side channel attacks
Key-updating approach [5] [18]	Able to resist the key exposure if the amount of key leakage in each period is strictly bounded	Wasting precious entropy and prone to failure when leakage is unbounded
The proposed framework	Resistant to unbounded leakage of each single key	Only useful in the situation with redundant randomness

At present, there have been extensive researches on the key exposure problem, which is typically formulated as one-time attacks [29] or continuous leakage models [30], [31]. The continuous leakage model presumes that there is a bound on the amount of leakage in each period [32], [33] so that the key exposure problem can be overcome by KUAs that replace the potentially leaked keys by fresh keys [5], [18], [19]. However, in many real-world applications, the amount of leakage may not be fixed or bounded in advance due to the concealment [34] and unpredictability [35], [36] of various attacks. So, keys have to be updated at a high frequency [18], [33] maybe far beyond what is necessary, which results in wasting a lot of precious entropy.

For greater clarity, the advantages and limitations of these existing work and the proposed framework are briefly summarized in Table I.

B. Redundant Designs

The origin of redundant technology can be traced back to 1834, when Lardner [37] proposed that different computers that execute the same instruction can ensure the reliability of results. Heterogeneous redundancy was also exploited in the flight control system for the Boeing 777 airplane to improve the reliability and security [38]. Navarro *et al.* [39], [40] investigated different redundancy mechanisms in coherent systems with possibly dependent heterogeneous components.

Wang *et al.* [41] proposed an optimal algorithm to find the minimum redundancy under the established reliability requirements.

In recent years, some research interests related to redundant designs have turned to improving system security. In 2013, Wu [17] proposed a mimic defense system based on the concept of heterogeneous redundancy to overcome uncertain threats due to unknown vulnerabilities or backdoors in the software/hardware. This work was selected on the list of China's top ten science and technology developments for the year 2013 by China's Academy of Sciences and China's Academy of Engineering. Yang *et al.* [42] proposed several common dynamic scheduling algorithms for redundant executions in mimic defense. Shamir [43] proposed a secret sharing scheme by using the redundant shares for cheater detection.

To the best of our knowledge, the idea of exploiting redundant randomness among keys is almost never considered in cryptographic systems, and almost all encryption algorithms [18], [19] are only based on the privacy of a single key at every moment, which is prone to the key exposure problem.

III. Preliminaries

A. Metrics for Measuring Key Secrecy

Shannon [10] showed that ensuring perfect secrecy requires that the key rate be at least as large as the message rate, which is impractical for real-world applications. Thus, much work is devoted to quantifying "partial" privacy. Currently, there have been five metrics for measuring the secrecy of keys: equivocation; number of expected guesses; guess probability; optimum guessing attack cost; and min-entropy.

In the following paragraphs, we will further discuss those five metrics and highlight the rationality of min-entropy as the preferred one.

In Shannon's original work, equivocation was used [10] as a "theoretical secrecy index," based on the similarity between the deciphering problem for the eavesdropper and the decoding problem for the receiver in the standard noisy communication setting [44]. Basically, equivocation is equivalent to the conditional entropy of the key sequence given the cryptogram, so Shannon's equivocation indeed describes the average unpredictability of a key from the perspective of an eavesdropper. However, Massey [45] showed that, even for arbitrarily small entropy, the expected number of guesses that need to be made for correctly guessing a random variable may be arbitrarily large.

Thus, most contemporary researchers [9], [13], [44] continue to seek more effective metrics other than Shannon's equivocation to evaluate the secrecy level of a key. Merhav and Arıkan [13] directly used the number of expected guesses that eavesdroppers need to make before finding the correct plaintext to measure secrecy level of general key sources. The guess probability corresponds to the reciprocal of the number of guesses, when the number of samples tends to infinity [44]. Wang *et al.* [14] used guess probability to measure the security of keys generated by QKD and pointed out that only the upper bound of the guessing probability really makes sense because the value in a loose bound is not all achievable.

The main criticism regarding the number of expected guesses and guessing probability is that there are various guessing strategies that may lead to different calculation results [46]. When the probability distribution of a random variable is known to the attacker, guessing the most probable key first should be more likely to succeed, which corresponds to the optimum guessing attack cost [47]. Here, the guessing strategy for determining at least one of several secret keys is to guess a maximum of k possibilities for a given key, and move on to a new key value when either a guess is correct, or k incorrect guesses have been made for the current value. Then, the optimum guessing attack cost is obtained by choosing k that minimize the average number of guesses per success.

Definition 1 (Optimum guessing attack cost [47]): Given a set of keys $\{X\}$ independently chosen from a set of M possibilities, with probability distribution $P = \{p_1, p_2, \ldots, p_M\}$, where these probabilities are sorted so that $p_1 \geq p_2 \geq \ldots \geq p_M$, the expected work per success for the attack is

$$W_k(X) = \frac{\sum_{j=1}^{k-1}(j \times p_j) + k(1 - \sum_{j=1}^{k-1} p_j)}{\sum_{j=1}^{k} p_j} \tag{1}$$

where the numerator is the expected number of guesses for the attack and the denominator is the reciprocal of the expected number of times that the attack must be performed until the first success. Then, the optimum guessing attack cost is defined as $W_{k*}(X)$.

$$W_{k*}(X) = \min_{1 \leq k \leq M} W_k(X). \tag{2}$$

B. Definition of Min-Entropy

Although $W_{k*}(X)$ can be calculated numerically for any given distribution of X, but it is not convenient for analysis. Fortunately, min-entropy can provide an accurate approximation to $W_{k*}(P)$. The National Institute of Standards and Technology (NIST) has formally defined min-entropy in the 2018 release of Special Publication 800-90B [48].

Definition 2 (Min-entropy [9]): For a cryptographic key expressed as a random variable $X \in (0,1)^n$, its min-entropy is defined as follows:

$$\begin{aligned} H_\infty(X) &\stackrel{\text{def}}{=} \min_{x \leftarrow X} \log_2 \left(\frac{1}{Pr[X = x]} \right) \\ &= -\log_2 \left(\max_{x \leftarrow X} Pr[X = x] \right) \end{aligned} \tag{3}$$

where $x \leftarrow X$ denotes the operation of sampling a random x according to X.

Lemma 1 (An accurate approximation [47]): Min-entropy provides an approximation to $W_{k*}(P)$ with the error bounded as follows:

$$0 \leq H_\infty(X) - \log_2(W_{k*}(X)) \leq 1 - \log_2(p_1 + 1). \tag{4}$$

For a detailed proof, please refers to the Special Publication 800-90B [48], although some notations are rewritten here. For a noise source that is not independent and identically distributed(i.i.d.), NIST also provides an estimation formula for

calculating the min-entropy as follows [47]:

$$H_\infty(X) = -\log_2\left(\min(1, \hat{p} + 2.576\sqrt{\frac{\hat{p}(1-\hat{p})}{L-1}})\right) \quad (5)$$

where L is the length of the dataset X extracted from the source and $\hat{p}$ is the proportion of the most common value in the dataset. Lemma 1 means that the min-entropy either exactly corresponds to the optimum guess work performed by Eve or overestimates the work by at most one bit if the work is measured in bits. Recently, many contemporary researchers [9], [31], [49] have adopted min-entropy to measure the difficulty or unpredictability of any adversary guessing a key in the worst case. Based on the concept of min-entropy, many modern cryptographic methods such as privacy amplification and entropy accumulation have been widely applied in leakage-resilient cryptography [29] and quantum cryptography [11]. Dodis and Smith [50] showed that the output keys are guaranteed to be almost uniformly distributed measured in bits as long as the min-entropy of key source is above some threshold l. Aggarwal *et al.* [51] called this type of key source as (n, l)-source defined as follows.

Definition 3 ((n, l)-key-source [51]): X is an (n, l)-source iff $X \in \{0, 1\}^n$ and $H_\infty(X) \geq l$.

Note that the min-entropy is always less than or equal to the Shannon entropy $H(X)$ and the range of $H_\infty(X)$ and $H(X)$ are both $[0, n]$. Moreover, keeping min-entropy always maximum is essentially equivalent to protecting the unpredictability of keys [51], which greatly reduces the possibility of key exposure.

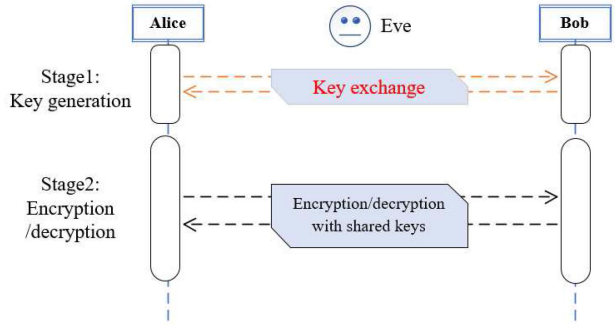

Fig. 2. Typical two-stage encryption/decryption paradigm.

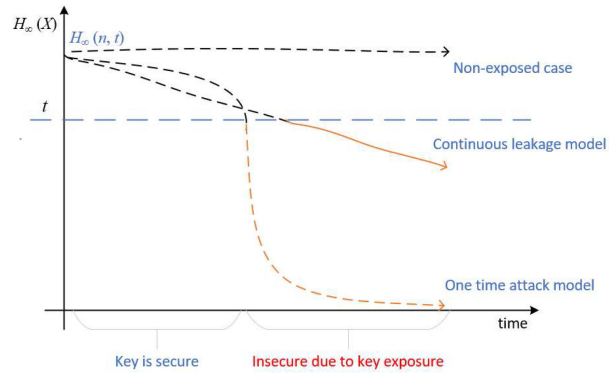

Fig. 3. Model of the key exposure problem.

IV. Highly Exposure-Resilient Framework

A. Problem Description

According to the groundbreaking work of Shannon [10], the basic security problem can be described as the transmission of a message from a sender (referred to Alice) to a receiver (Bob) over an open wired or wireless communication channel such that an adversary (Eve) with access to this channel cannot obtain useful information about the message. Modern cryptographic methodology presumes that both the encryption and decryption algorithms should be assumed to be public [23] so that the entire security depends only on the privacy or unpredictability of a cryptographic key shared by Alice and Bob [31].

A typical encryption/decryption paradigm consists of two stages, as shown in Fig. 2. The first stage is key exchange, which is used to generate shared keys between Alice and Bob. The second stage is symmetric encryption, and typical implementations include RC4, RC5, RC6, blowfish, Data Encryption Standard (DES), 3DES, AES, etc. It is generally believed that symmetric encryption, such as AES, is relatively secure, even in the face of quantum attacks, as long as the key length is long enough. As Bernstein and Lange pointed out [52], simply switching to 256-bit AES keys can resist all known quantum attacks, such as Grover's algorithm, in the foreseeable future. In contrast, the first stage is often prone to key exposure due to various reasons. Keys may be exposed during the key generation or distribution stage. Even if a key is securely generated and distributed, it may be stolen by the adversaries through system backdoors or social engineering [53].

In nature, a cryptographic key can be regarded as a random variable that Eve should not have access to [50]. That is to say, once a key is leaked to Eve, its randomness is basically lost. Therefore, resisting key exposure is essentially equivalent to protecting the unpredictability of the key, i.e., keeping its randomness always maximum. Since the Shannon entropy that describes the average unpredictability is not suitable for the case of formally evaluating cryptographic entropy, many contemporary researchers [9], [31], [49] have adopted min-entropy to measure the difficulty or unpredictability of any adversary guessing a key in the worst case.

As shown in Fig. 3, regardless one-time attack model [29] or continuous leakage model [30], [31], the key exposure is manifested as a decrease in the randomness of keys, which motivates us to protect randomness for resisting key exposure.

B. Solution

In this article, we solve the key exposure problem by incorporating the redundancy of key sources into the design of cryptographic systems. With the continuous reduction of hardware costs, it will be cheaper to obtain keys with redundant randomness. The problem is how we do achieve more secure encrypted communications from the redundant design. We make the following assumptions.

1) The design with redundant randomness. There are redundant and independent keys available for Alice and Bob.
2) All key sources are (n, l)-source and it is unknown, which one is possibly exposed. The key exposure may follow the one-time attack model or the continuous leakage model. For a key X extracted from (n, l)-source, its min-entropy is less than l if and only if it is leaked to Eve; otherwise, its min-entropy must be greater than or equal to l.
3) At least one key source is not exposed. With the increase of redundant components, the difficulty and cost of successful attacks from Eve should continue to increase.
4) Ideal assumption of stage 2. As shown in Fig. 2, we assume that, unless the key is exposed to Eve, the encryption/decryption algorithms are computationally strong, i.e., the adversary cannot obtain any useful information only from the ciphertext. So, we focus on solving the key exposure problem that may occur during the key generation (in stage 1).

For the sake of illustration, we consider a simple example with two key sources $\{S_1, S_2\}$ shared by Alice and Bob.

Example 1: Alice and Bob extract key X_1 from S_1 and X_2 from S_2, respectively. Suppose only one of these two keys is exposed to Eve at some time, but Alice and Bob do not know which one is exposed or when it happens. Which key should Alice and Bob use?

It is obvious that no matter which key Alice and Bob choose, they risk that the key may be exposed, i.e., the encrypted communication with either X1 or X2 has a 50% chance of being insecure. Our idea is to introduce a transformation function, called EMT, which has the following property.

Definition 4 (Entropy-maximizing property): A function $\boldsymbol{f}: (0,1)^n \times (0,1)^n \to (0,1)^n$ is defined as an EMT with entropy-maximizing property if for any random variable $X_1 \in (0,1)^n$ and independent $X_2 \in (0,1)^n$, $X = \boldsymbol{f}(X_1, X_2)$ satisfies the following inequality:

$$H_\infty(X) = H_\infty\left(\boldsymbol{f}(X_1, X_2)\right) \geq \max\left(H_\infty(X_1), H_\infty(X_2)\right) \tag{6}$$

where $\max(.,.)$ is a function that accepts two real arguments and returns the larger one.

According to the first assumption, X_1 and X_2 are independent of each other. According to the assumption that at least one key source is not exposed, we get that either $H_\infty(X_1) \geq l$ or $H_\infty(X_2) \geq l$. Then, by applying the entropy-maximizing property, we get $H_\infty(\boldsymbol{f}(X_1, X_2)) \geq l$. That is to say, the security status of the system can be guaranteed 100% secure as long as Alice and Bob use the output of $\boldsymbol{f}(X_1, X_2)$ as the key for encryption/decryption.

Moreover, an EMT can be extended by some composite functions without losing its properties, which is useful in practice.

Lemma 2: For any random variable $X \in (0,1)^n$ and function $g: (0,1)^n \to (0,1)^n$, $H_\infty(g(X)) = H_\infty(X)$ always holds, if only $g(.)$ is a one-to-one function.

Proof. Notice that one-to-one function means that every element of the range of the function corresponds to exactly one element of the domain, i.e., $\Pr[g(X) = g(x)] = \Pr[X = x]$ always holds. Thus

$$\begin{aligned} H_\infty\left(g(X)\right) &= -\log_2\left(\max_{x \leftarrow X} \Pr[g(X) = g(x)]\right) \\ &= -\log_2\left(\max_{x \leftarrow X} \Pr[X = x]\right) \\ &= H_\infty(X). \end{aligned} \tag{7}$$

■

Lemma 3: A composite function $(g \circ f)(.,.)$ conforms to Definition 4, if only $f: (0,1)^n \times (0,1)^n \to (0,1)^n$ conforms to Definition 4 and $g: (0,1)^n \to (0,1)^n$ is a one-to-one function.

Proof: According to Lemma 2 and Definition 4, we have

$$\begin{aligned} H_\infty\left((g \circ f)(X_1, X_2)\right) &= H_\infty\left(g\left(f(X_1, X_2)\right)\right) \\ &= H_\infty\left(f(X_1, X_2)\right) \\ &\geq \max\left(H_\infty(X_1), H_\infty(X_2)\right). \end{aligned} \tag{8}$$

■

Theorem 1: For any permutation, of all elements in $(0,1)^n$, that is represented as $< z_0, z_1, \ldots, z_{2^n} >$, an EMT denoted by $\boldsymbol{EMT}_g: (0,1)^n \times (0,1)^n \to (0,1)^n$ can be constructed as follows.

$$\boldsymbol{EMT}_g(x, y) = z_i \tag{9}$$

where $i = (x + y + b) \mod 2^n$ and $b \in (0,1)^n$ can take any integer value within its legal range $[0, 2^n - 1]$.

Proof: Notice that $y = (i - x - b) \mod 2^n$, so for any given z_i, y will go through every sample in $(0,1)^n$ when x takes each sample in $(0,1)^n$. Thus, based on the assumption of independence between X and Y, we get

$$\begin{aligned} \Pr[Z = z_i] &= \sum_{j=1}^{2^n} (\Pr[X = x_j] \times \Pr[Y = y'_j]) \\ &\leq \sum_{j=1}^{2^n} ((\max_{x \leftarrow X} \Pr[X = x]) \times \Pr[Y = y'_j]) \\ &= \left(\max_{x \leftarrow X} \Pr[X = x]\right) \times \sum_{j=1}^{2^n} \Pr[Y = y'_j] \\ &= \max_{x \leftarrow X} \Pr[X = x] \end{aligned} \tag{10}$$

where $y'_j = (i - x_j - b) \mod 2^n$ and $\sum_{j=1}^{2^n} Pr[Y = y'_j] = 1$.

Notice that $\log_2(s)$ is an increasing function for $s \in [0, 1]$. From (10), we get

$$\begin{aligned} H_\infty(Z) &= -\log_2\left(\max_{z \leftarrow Z} \Pr[Z = z_i]\right) \\ &\geq -\log_2\left(\max_{x \leftarrow X} \Pr[X = x]\right) \\ &= H_\infty(X). \end{aligned} \tag{11}$$

Since the form of $\boldsymbol{EMT}_g(x, y)$ remain the same when x and y are swapped, we can also get $H_\infty(Z) \geq H_\infty(Y)$. Accordingly, we finally get

$$H_\infty\left(\boldsymbol{EMT}_g(X, Y)\right) \geq \max\left(H_\infty(X), H_\infty(Y)\right) \tag{12}$$

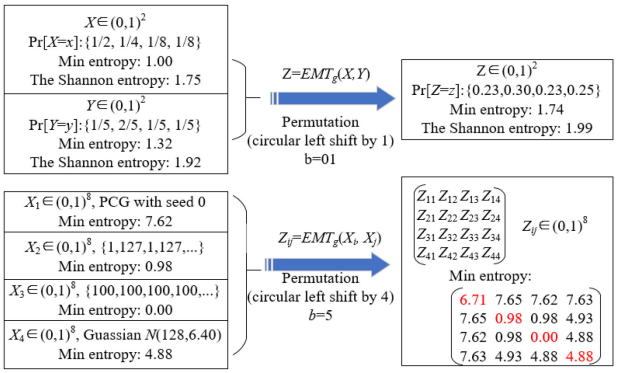

Fig. 4. Examples for verifying the effectiveness of EMTs.

which is conforms to Definition 4. ■

Notice that, for every permutation of all elements in $(0,1)^n$, we can derive a new EMT instance like $\boldsymbol{EMT}_g()$. Since there are 2^n elements in the sample space of $(0,1)^n$, the number of permutations of all elements is $(2^n!)$. So, the number of such EMT instances is at least $(2^n!)$.

Based on Lemmas 2 and 3 and Theorem 1, various functions with the entropy-maximizing property can be derived for a pair of independent keys. For a detailed example for constructing EMT instances, please refers to Fig. 4 that is explained in Section V-A. Furthermore, the methodology can be extended to multivariate situations, as long as $\boldsymbol{f}$ is iteratively applied to a set of independent keys.

V. Numerical Results

Although our method partially sacrifices the available key rate of the cryptographic system by fusing multiple keys, the impact on the communication systems is to improve the ability to resist unknown or unpredicted key exposure.

Next, we first verify the effectiveness of EMTs through numerical calculations by constructing two EMT instances, and then, analyze the advantages of the proposed method on the security level based on a typical scenario.

A. Verification of EMTs

Fig. 4 shows how two instances of EMTs can be constructed by following Theorem 1. Here, only two decimal digits of precision are kept for real numbers in the figure.

1) Instance for 2-Bit Keys: According to Theorem 1, the first EMT instance, $Z = EMT_g(X,Y)$, is constructed by choosing a circular left shift as a permutation and setting b to 01 in the key space of $(0,1)^2$. For a binary number in $(0,1)^2$, circular left shift by 1 actually means mapping $\{00,01,10,11\}$ to $\{00,10,01,11\}$, respectively. For example, if $x = 10$ and $y = 11$, then we get that $i = (x + y + b) \mod 2^2 = 10$ and $\mathrm{EMT}_g(x,y)$ returns 01. $X \in (0,1)^2$ is a random number with probability distribution $\{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{8}\}$. Its min-entropy and the Shannon entropy are 1.00 and 1.75, respectively. $Y \in (0,1)^2$ is with probability distribution $\{\frac{1}{5}, \frac{2}{5}, \frac{1}{5}, \frac{1}{5}\}$. Its min-entropy and the Shannon entropy are 1.32 and 1.92, respectively. After applying $\mathrm{EMT}_g(X,Y)$ to X and Y, we get Z, whose min-entropy and the Shannon entropy are 1.74 and 1.99, respectively. It can be seen that the min-entropy of Z is greater than that of both X and Y, i.e., $1.74 > \max(1.0, 1.32)$, which verifies the effectiveness of $\mathrm{EMT}_g(X,Y)$ in the key space of $(0,1)^2$.

2) Instance for 8-Bit Keys: The second EMT instance, $Z_{ij} = \mathrm{EMT}_g(X_i, X_j)$, is constructed by choosing a circular left shift by 4 and setting b to 5. In order to test its effectiveness, we constructed four numerical sequences, namely X_1, X_2, X_3, and X_4, each consisting of 100 000 numbers in $(0,1)^8$. X_1 is generated with the PCG64 toolkit that comes with Numpy 1.19.4 in Python 3.8.6. X_2 is an alternating sequence with a period of 2, i.e., $\{1, 127, 1, 127, \cdots\}$. X_3 is a constant sequence of 100 s. X_4 is a Gaussian integer sequence with mean 128 and variance 6.4. According to (5), their min-entropies are calculated as 7.62, 0.98, 0.00, and 4.88, respectively. After applying $Z_{ij} = \mathrm{EMT}_g(X_i, X_j)$, where i and j are from 1 to 4, it can be seen that the min-entropy of Z_{ij} is always larger than that of X_i and X_j for every i and j, unless i is equal to j. In fact, this conclusion is always valid, as long as Lemmas 2 and 3 and Theorem 1 are followed.

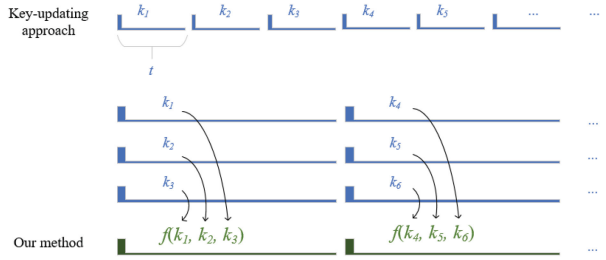

Fig. 5. Comparison of the KUA and our method.

B. Secrecy Outage Probability

In order to facilitate analysis, we set up a scenario, in which Alice and Bob extract a sequence of independent keys, $\{X_1, X_2, \cdots, X_m\}$. This is feasible because almost all key generation mechanisms [20], [21] mandate that the generated keys be statistically independent of each other.

The lifetime of a key is defined as the time before it is exposed. By adopting the continuous leakage model [31] and assuming that all keys following the same distribution, the lifetime T_i of the key X_i can be expressed as a random variable in exponential distribution $F_i(t) = P(T_i > t) = e^{-\lambda t}, i = 1, \cdots, m$, where λ is the average number of occurrences of exposure events per time unit and t is the time interval between events.

Fig. 5 shows the difference between the KUA [5], [18] and our method. When the KUA is applied, keys are updated one by one and the working time of each key is t. When our approach is applied, multiple secret keys are used to form an EMT secret key. Although the working time of each key becomes longer, the resistance to secret key exposure is improved. To illustrate this point, we borrow the concept of SOP [54] as an indicator to measure the security state of the encrypted communications. In

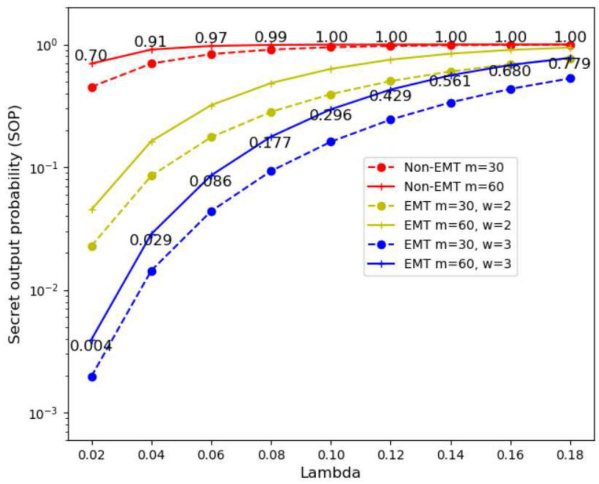

Fig. 6. Comparison between SOP_{KUA} and SOP_{EMT} with setting $m = 60$.

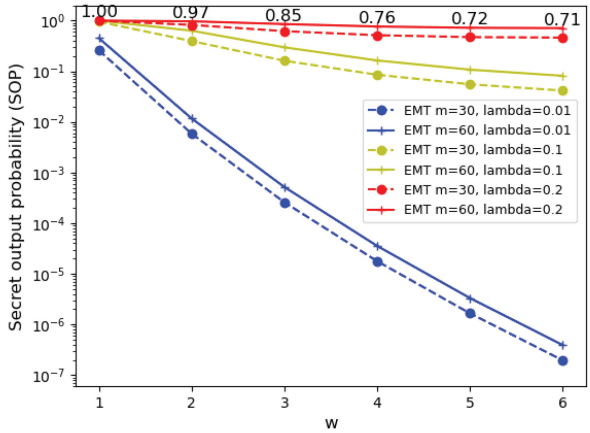

Fig. 7. Effect of varying w on SOP.

previous researches [54], SOP usually measures the probability that the achievable secrecy rate fails to reach a given rate. Since we presume that the system security only depends on the privacy of keys, key exposure is regarded as the only reason for the decrease in the secrecy rate. So, we define SOP as the probability that an adversary can correctly determine the plaintext from ciphertext due to any possible exposure of keys. Correspondingly, SOP is calculated as follows.

$$\text{SOP}_{\text{KUA}} = 1 - (e^{-\lambda t})^m \tag{13}$$

where $e^{-\lambda t}$ is the probability that the key exposure occurs at least once.

In contrast, our method enables $\boldsymbol{f}$ to be applied for every w keys so that each output of $\boldsymbol{f}$ has to keep working for at least the period of wt. In Fig. 5, w was set to 3. So, the SOP is calculated as follows:

$$\begin{aligned}\text{SOP}_{\text{EMT}} &= 1 - \left[1 - (1 - e^{-\lambda w t})^w\right]^{\frac{m}{w}} \\ &= 1 - \left[1 - (1 - e^{-3\lambda t})^3\right]^{\frac{m}{3}}.\end{aligned} \tag{14}$$

Based on the aforementioned metrics, the following results are obtained by calculations.

In Fig. 6, SOP_{KUA} and SOP_{EMT} are compared by setting $m = 60$ and $t = 1$ and varying lambda (λ) and w. "Non-EMT" and "EMT" are corresponding to SOP_{KUA} and SOP_{EMT}, respectively. The vertical axis processes a logarithmic scale. As λ increases, both SOP_{KUA} and SOP_{EMT} keep increasing. SOP_{KUA} is about 0.7, 0.91, and 0.97, while SOP_{EMT} is about 0.004, 0.029, and 0.086, for $\lambda = 0.02$, $\lambda = 0.04$, and $\lambda = 0.06$, respectively. It can be seen that our method significantly reduces the SOP by about 100 times, and as w increases, the improvement effect becomes more obvious.

Fig. 7 shows the effect of varying w on SOP. As w increases, the SOP decreases, but the improvement effect is more obvious when lambda is smaller. This is reasonable because our method relies on high-quality key sources to shield the exposure risk of low-quality key sources. It will be difficult to achieve good security, even with bountiful redundancy, if all key sources are of low quality. Therefore, it is still valuable to develop high-quality key sources, such as lattice-based key generation and quantum key distribution.

VI. Conclusion

This article presents a highly exposure-resilient framework for securing the encrypted communication systems so that each single key can be free from the threat of key exposure through fusion with other keys. The framework exploits the entropy-maximizing property of a family of functions, called EMTs, so that the redundant randomness of keys can be fused to construct a new key with stronger security than the original keys in the strictest sense of min-entropy. Finally, the effectiveness of EMTs is strictly verified by digital calculations, and the numerical results show that the proposed framework can significantly improve the security level in terms of SOP.

In addition, various EMT instances may exhibit different characteristics, which has not been fully explored in this article. For example, some EMT instances satisfy the commutative and associative laws, but not all of them. In many situations, keys from different sources may have inconsistent lengths, in which alignment operations may be required before fusion. Integrating EMTs into key management is also worth considering. These issues need further efforts invested.

References

[1] G. Li, Z. Zhang, J. Zhang, and A. Hu, "Encrypting wireless communications on the fly using one-time pad and key generation," *IEEE Internet Things J.*, vol. 8 no. 1, pp. 357–369, Jan. 2021.

[2] N. At, J.-L. Beuchat, E. Okamoto, I. San, and T. Yamazaki, "Compact hardware implementations of ChaCha, BLAKE, threefish, and skein on FPGA," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 2, pp. 485–498, Feb. 2014.

[3] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted Internet of Things: From security and efficiency perspectives," *IEEE Netw.*, vol. 33, no. 2, pp. 50–57, Mar./Apr. 2019.

[4] L. Guan, J. Lin, Z. Ma, B. Luo, L. Xia, and J. Jing, "Copker: A cryptographic engine against cold-boot attacks," *IEEE Trans. Dependable Secur. Comput.*, vol. 15, no. 5, pp. 742–754, Sep./Oct. 2018.

[5] B. Liu, W. Zhang, and T. Jiang, "A scalable key distribution scheme for conditional access system in digital pay-TV system," *IEEE Trans. Consum. Electron.*, vol. 50, no. 2, pp. 632–637, May 2004.

[6] D. Das *et al.*, "ASNI: Attenuated signature noise injection for low-overhead power side-channel attack immunity," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 10, pp. 3300–3311, Oct. 2018.

[7] J. Cao, P. Yu, X. Xiang, M. Ma, and H. Li, "Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system," *IEEE Internet Things J.*, vol. 6, no. 6, pp. 9794–9805, Dec. 2019.

[8] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[9] Y. Dodis, X. Li, T. D. Wooley, and D. Zuckerman, "Privacy amplification and non-malleable extractors via character sums," in *Proc. IEEE 52nd Annu. Symp. Found. Comput. Sci.*, Oct. 2011, pp. 668–677.

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

[11] R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," *Nature Commun.*, vol. 9, no. 1, pp. 1–11, Jan. 2018, doi: 10.1038/s41467-017-02307-4.

[12] S. Raza and R. Magnússon, "TinyIKE: Lightweight IKEv2 for Internet of Things," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 856–866, Feb. 2019.

[13] N. Merhav and E. Arikan, "The Shannon cipher system with a guessing wiretapper," *IEEE Trans. Inf. Theory*, vol. 45, no. 6, pp. 1860–1866, Sep. 1999.

[14] X.-B. Wang, J.-T. Wang, J.-Q. Qin, C. Jiang, and Z.-W. Yu, "Guessing probability in quantum key distribution," *npj Quantum Inf.*, vol. 6, no. 1, pp. 1–5, 2020, doi: 10.1038/s41534-020-0267-3.

[15] M. A. Mellal, S. Al-Dahidi, and E. J. Williams, "System reliability optimization with heterogeneous components using hosted cuckoo optimization algorithm," *Rel. Eng. Syst. Saf.*, vol. 203, 2020, Art. no. 107110. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832020306116

[16] G. Li, W. Wang, K. Gai, Y. Tang, B. Yang, and X. Si, "A framework for mimic defense system in cyberspace," *J. Signal Process. Syst.*, vol. 93, no. 2, pp. 169–185, 2021, doi: 10.1007/s11265-019-01473-6.

[17] J. Wu, *Cyberspace Mimic Defense*. Switzerland Springer, 2020.

[18] Y. Dodis, K. Haralambiev, A. Lopez-Alt, and D. Wichs, "Cryptography against continuous memory attacks," in *Proc. IEEE 51st Annu. Symp. Found. Comput. Sci.*, Oct. 2010, pp. 511–520.

[19] J.-D. Wu, Y.-M. Tseng, S.-S. Huang, and T.-T. Tsai, "Leakage-resilient certificate-based signature resistant to side-channel attacks," *IEEE Access*, vol. 7, pp. 19041–19053, 2019.

[20] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, 2008, pp. 128–139, doi: 10.1145/1409944.1409960.

[21] S. Liu, Y. Hong, and E. Viterbo, "Unshared secret key cryptography," *IEEE Trans. Wireless Commun.*, vol. 13, no. 12, pp. 6670–6683, Dec. 2014.

[22] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

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

[24] G. K. Kurt, Y. Khosroshahi, E. Ozdemir, N. Tavakkoli, and O. A. Topal, "A hybrid key generation and a verification scheme," *IEEE Trans. Ind. Inform.*, vol. 16, no. 1, pp. 703–714, Jan. 2020.

[25] L. Jiao, N. Wang, P. Wang, A. Alipour-Fanid, J. Tang, and K. Zeng, "Physical layer key generation in 5G wireless networks," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 48–54, Oct. 2019.

[26] S. Pirandola *et al.*, "High-rate measurement-device-independent quantum cryptography," *Nature Photon.*, vol. 9, no. 6, pp. 397–402, Jun. 2015, doi: 10.1038/nphoton.2015.83.

[27] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, and M. O'Neill, "On practical discrete Gaussian samplers for lattice-based cryptography," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 322–334, Mar. 2018.

[28] R. Chaudhary, G. S. Aujla, N. Kumar, and S. Zeadally, "Lattice-based public key cryptosystem for Internet of Things environment: Challenges and solutions," *IEEE Internet Things J.*, vol. 6, no. 3 pp. 4897–4909, Jun. 2019.

[29] M. Naor and G. Segev, "Public-key cryptosystems resilient to key leakage," in *Proc. 29th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, Aug. 16–20, 2009, pp. 18–35, doi: 10.1007/978-3-642-03356-8_2.

[30] J. Alwen, Y. Dodis, and D. Wichs, "Leakage-resilient public-key cryptography in the bounded-retrieval model," in *Proc. 29th Annu. Int. Cryptol. Conf.*, Santa Barbara, CA, USA, Aug. 16–20, 2009, pp. 36–54, doi: 10.1007/978-3-642-03356-8_3.

[31] J. Wu, Y. Tseng, and S. Huang, "An identity-based authenticated key exchange protocol resilient to continuous key leakage," *IEEE Syst. J.*, vol. 13, no. 4, pp. 3968–3979, Dec. 2019.

[32] Y. Zhou, B. Yang, and Y. Mu, "Continuous leakage-resilient identity-based encryption without random oracles," *Comput. J.*, vol. 61, no. 4, pp. 586–600, Apr. 2018.

[33] Y. Zhou, B. Yang, Z. Xia, Y. Mu, and T. Wang, "Anonymous and updatable identity-based hash proof system," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2818–2829, Sep. 2019.

[34] J. Ma *et al.*, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, 2018, doi: 10.1038/s41586-018-0609-x.

[35] D. Brumley and D. Boneh, "Remote timing attacks are practical," *Comput. Netw.*, vol. 48, no. 5, pp. 701–716, 2005.

[36] J. Kim and S. Hong, "Side-channel attack using meet-in-the-middle technique," *Comput. J.*, vol. 53, no. 7, pp. 934–938, Sep. 2010.

[37] D. Lardner, "Babbage's calculating engine," *Edinburgh Rev.*, vol. 1, pp. 263–327, 1834.

[38] Y. Yeh, "Triple-triple redundant 777 primary flight computer," in *Proc. IEEE Aerosp. Appl. Conf.*, 1996, vol. 1, pp. 293–307.

[39] J. Navarro, P. Fernández-Martínez, J. Fernández-Sánchez, and A. Arriaza, "Relationships between importance measures and redundancy in systems with dependent components," *Probability Eng. Informational Sci.*, vol. 34, no. 4, pp. 583–604, 2020.

[40] J. Navarro and P. Fernández-Martínez, "Redundancy in systems with heterogeneous dependent components," *Eur. J. Oper. Res.*, vol. 290, no. 2, pp. 766–778, 2021.

[41] L. Wang, J. Zhu, S. Tian, T. Pei, H. Liu, and Y. Li, "Fast finding optimal redundancy to satisfy reliability requirement for safety-critical parallel applications on heterogeneous distributed automotive systems," in *Proc. IEEE Int. Conf Parallel Distrib. Process. Appl., Big Data Cloud Comput., Sustain. Comput. Commun., Social Comput. Netw.*, Dec. 2019, pp. 372–379.

[42] L. Yang and Y. Wang, "Simulation experiment of scheduling algorithm in dynamic heterogeneous redundancy," in *Proc. Int. Conf. Inf. Sci., Parallel Distrib. Syst.*, 2020, pp. 189–195.

[43] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, pp. 612–613, Nov. 1979, doi: 10.1145/359168.359176.

[44] I. Issa and A. B. Wagner, "Measuring secrecy by the probability of a successful guess," *IEEE Trans. Inf. Theory*, vol. 63, no. 6, pp. 3783–3803, Jun. 2017.

[45] J. Massey, "Guessing and entropy," in *Proc. IEEE Int. Symp. Inf. Theory*, 1994, p. 204.

[46] D. Malone and W. Sullivan, "Guesswork is not a substitute for entropy," in *Proc. Inf. Technol. Telecommun. Conf.*, Oct. 2005, pp. 1–5.

[47] NIST, "NIST special publication 800-90b. recommendation for the entropy sources used for random bit generation," Accessed: Jan. 19, 2022. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf

[48] M. Turan, E. Barker, J. Kelsey, K. McKay, M. Baish, and M. Boyle, "NIST special publication 800-90b: Recommendation for the entropy sources used for random bit generation," U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2018.

[49] F. Dupuis and O. Fawzi, "Entropy accumulation with improved second-order term," *IEEE Trans. Inf. Theory*, vol. 65, no. 11, pp. 7596–7612, Nov. 2019.

[50] Y. Dodis and A. Smith, "Entropic security and the encryption of high entropy messages," in *Theory of Cryptography*, J. Kilian, Ed. Berlin, Germany: Springer, 2005, pp. 556–577.

[51] D. Aggarwal, Y. Dodis, Z. Jafargholi, E. Miles, and L. Reyzin, "Amplifying privacy in privacy amplification," in *Advances in Cryptology—CRYPTO 2014*, J. A. Garay and R. Gennaro, Eds. Berlin, Germany: Springer, 2014, pp. 183–198.

[52] D. J. Bernstein and T. Lange, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017, doi: 10.1038/nature23461.

[53] S. Gupta, A. Isha Bhattacharya, and H. Gupta, "Analysis of social engineering attack on cryptographic algorithm," in *Proc. 9th Int. Conf. Rel., Infocom Technol. Optim.*, 2021, pp. 1–5.

[54] T.-H. Chou, S. C. Draper, and A. M. Sayeed, "Secret key generation from sparse wireless channels: Ergodic capacity and secrecy outage," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1751–1764, Sep. 2013.

Longjiang Li (Member, IEEE) received the B.S. degree in computer science and engineering from Xidian University, Xi'an, China, in 2001, the M.S. degree in computer science and engineering from Xi'an Telecommunication Institute, Xi'an, in 1998, and the Ph.D. degree in computer science and technology from Shanghai Jiao Tong University, Shanghai, China, in 2007.

He was a Visiting Scholar with North Carolina State University, Raleigh, NC, USA, from 2015 to 2016. He is currently an Associate Professor with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China. His research interests include the domain of communication and information engineering, especially with regard to ad hoc networks (including VANETs/UAVs/WSNs), cryptography, and intelligent interaction.

Jie Wang received the B.S. degree in electronic information engineering from Sichuan University, Chengdu, China, in 2020. He is currently working toward the master's degree in information and communication engineering with the Department of Network Engineering, School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu.

His research interests include the domain of communication and information engineering, especially relating to artificial-intelligence-based network security, edge computing, and electric vehicles.

Rui Zhang received the B.S. degree in information and communication engineering from the School of Information Science and Technology, Northwest University, Xi'an, China, in 2019. She is currently working toward the master's degree in information and communication engineering with the Department of Network Engineering, School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China.

Her research interests include network security, edge computing, and human–computer interaction.

Yuanchen Gao received the B.S. degree in electronic information engineering from Hangzhou Dianzi University, Hangzhou, China, in 2020. He is currently working toward the master's degree in information and communication engineering with the Department of Network Engineering, School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China.

His research interests include network security, network engineering, and edge computing.

Yonggang Li received the B.S. degree in electrical engineering from Northeast Electric Power University, Jilin, China, in 1997, the M.S. degree in electrical engineering from Si Chuan University, Chengdu, China, 2002, and the Ph.D. degree in electrical engineering from Shanghai Jiao Tong University, Shanghai, China, in 2007.

He was an Assistant and Associate Professor with the University of Electronic Science and Technology of China, Chengdu, from 2007 to 2014, and a Visiting Scholar with Electrical Engineering Department, University of Wisconsin-Madison, Madison, WI, USA, from 2011 to 2012. He is currently an Associate Professor with the Chongqing University of Posts and Telecommunications, Chongqing, China, which he joined in 2014. His research interests include large-scale networks, communication security, smart grid, and military system engineering.

Yuming Mao received the B.S. degree in communication engineering and the M.S. degree in information engineering and processing from the University of Electronic Science and Technology of China, Chengdu, China, in 1982 and 1984, respectively.

He is currently a Professor and Doctoral Advisor with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, China. His research interests include broadband communication network, network organization and protocol analysis, TCP/IP technology, network management and protocol, routing protocol, and network engineering.

He was the recipient of several awards including the first grade, second grade, and third grade awards of the Ministry of Electronic Industry for science and technology progress, the second grade national award for science and technology progress.