IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 11, 2018, accepted December 25, 2018, date of publication January 7, 2019, date of current version January 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2891075

Using Transposition Padding to Get CCA2 Security From Any Deterministic Encryption Schemes

LINMING GONG[1], MINGMING WANG[1], XIANGJIAN ZUO[2], SHUNDONG LI[3], AND DAOSHUN WANG[4], (Member, IEEE)

[1] Shaanxi Key Laboratory of Clothing Intelligence, National and Local Joint Engineering Research Center for Advanced Networking and Intelligent Information Service, School of Computer Science, Xi'an Polytechnic University, Xi'an 710048, China
[2] School of Cyber Security, Beijing University of Posts and Telecommunications, Beijing 10087, China
[3] School of Computer Science, Shaanxi Normal University, Xi'an 710048, China
[4] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China

Corresponding authors: Linming Gong (glmxinjing@163.com) and Shundong Li (shundong@snnu.edu.cn)

This work was supported in part by the Ph.D. Science Foundation of Polytechnic University under Grant 107020331, in part by the Natural Science Foundation of China under Grant 61601358, Grant 61272435, Grant 61373020, Grant U1536102, and Grant U1536116, and in part by the China Mobile Research Fund Project under Grant MCM20170407.

ABSTRACT We study how to make any deterministic encryption scheme probabilistic and secure against adaptively chosen ciphertext attacks. A new transpositional padding encryption scheme is proposed, with which we construct a universal scheme, namely, a transpositional padding encryption scheme, which has three novel attributes: 1) it can pad a given plaintext into several different values once the randomness is chosen while the previous padding schemes only pad a given plaintext into a fixed value; 2) it introduces the randomness into a ciphertext without employing hash function or random oracle, and; 3) it enables the encrypted message to contain more useful information that may exceed the upper limit of plaintext space. Then, we give this encryption scheme an instantiation of RSA, which is proven to be indistinguishable under adaptively chosen ciphertext attacks without random oracle that assumes a variant of the standard RSA problem. The variant problem is a novel arithmetic problem, and it is weaker than the standard RSA problem.

INDEX TERMS Adaptive chosen ciphertext attacks, padding encryption, deterministic encryption, standard model.

I. INTRODUCTION

Deterministic public-key encryption schemes [1] always produces the same ciphertexts when it is used to encrypt a given plaintext for a given public key, even if the encryption algorithm is executed separately more than one time. Generally speaking, the deterministic public-key encryption schemes are more efficient than other public encryption schemes. Many deterministic public-key encryption schemes are widely used to provide privacy and to ensure authenticity for the internet users. For instance, RSA [2] is still deployed in many e-commercial systems [3]–[10] nowadays. However, one of the drawbacks of the deterministic encryptions is the possibility of leaking partial information to the adversaries, i.e., for a given key, if an adversary has gotten some ciphertexts and their corresponding plaintexts, he can recover partial even all information of the plaintext m from a new ciphertext, which is also encrypted by the given key.

In order to improve the security performance of the deterministic public-key encryption schemes, researchers proposed to transform the deterministic encryption schemes to the probabilistic ones by introducing randomness into ciphertexts. Using this method, an deterministic encryption scheme can encrypt a given plaintext into one element of many possible ciphertexts, which looks like one element chosen randomly from these ciphertexts. Thus, this method can keep an adversary from recovering some bits of a challenge plaintext through its corresponding ciphertext (which is evaluated using the pairs of plaintext-ciphertext gained by the adversary).

It is important for the users who care about their privacy to know what security level can be obtained by a method that is used to transform any deterministic encryption scheme to a probabilistic one. A preferable transforming method should be able to provide sufficiently strong guarantees on privacy protection such that (1) leaking partial information to the adversaries becomes infeasible; (2) the adversaries cannot correlate any two encryptions of the same message, or correlate a message to its ciphertext, even if accessed to the public encryption key. In other words, a preferable transforming method should be able to make any deterministic encryption scheme to be with the indistinguishable security, which is defined by Shafi and Micali [11]. Indistinguishable security, even in the scenario that chosen plaintext attack, CPA, implies probabilistic encryption. That is, given a plaintext, as different randomness is introduced into encryption, it should be encrypted into variable ciphertexts under a fixed public key.

Although CPA security provides a guarantee on preventing attacks from the completely passive adversaries, no guarantee on the privacy is provided when the attacks from an adversary mount to active attack. To cope with the active attacks, Naor and Yung [12] proposed a security primitive that provides a guarantee on being against the adaptive chosen ciphertext attack (CCA2).

The study on what security level a deterministic public-key encryption provides is initiated by Bellare *et al.* [1]. Bellare *et al.* [13] provided the 'strongest possible' security level for the random oracle model by introducing randomness into encryption algorithm. Modifying a deterministic scheme, Boldyreva *et al.* [14] developed a chosen ciphertext attack (CCA) secure probabilistic scheme without random oracles. In 2012, by introducing a meaningful level of security to privacy protection, Mironov *et al.* [15] presented an approach to model the incrementality of deterministic public-key encryption. In 2013, Fuller *et al.* [16] developed a deterministic public-key encryption scheme, which provides meaningful security if and only if the source of randomness in the encryption process comes with the plaintext itself. Brakerski and Segev [17] formalized a framework that focuses on hard-to-invert auxiliary inputs to study what security level a deterministic public-key encryption scheme provides. A lot of researchers focused on constructing deterministic public-key encryption schemes, among which some schemes employ very novel methods, such as schemes proposed in [16]–[20].

Although the deterministic encryption schemes mentioned above are practically important in searching of encrypted data, they can never amount to the level of semantical security. In addition, finding a general and efficient method to transform any deterministic encryption scheme to a probabilistic one with CCA2 security in the standard model was still an important and open problem. Particularly,it is urgent to address how to transform the RSA cryptosystem to a probabilistic one without random oracle but with CCA2 security.

As a deterministic cryptosystem, for having high efficiency, RSA remains one of the most popular determinist public-key encryption scheme. The padding mechanism is critical and widely adopted to help RSA achieve a higher security level in encrypting messages [21]–[27].

Although these variants of RSA are practically important, they still exhibit some inherent drawbacks:

(1) All the schemes mentioned above adopted the optimal asymmetric padding method which needs padding at least k bits of redundant information in one ciphertext to achieve plaintext awareness. Hence, at most $n-k$ (n is the upper limit of the plaintext space) bits of useful information is included in a ciphertext, which is encrypted with the optimal asymmetric padding method.

(2) All the padding-based RSA-type schemes mentioned above can be against CCA2 in the random oracle model [28], except that [26] can be against CPA in the standard model (under appropriate assumptions on the hash functions used to instantiate OAEP). In addition, as proved by Kiltz and Pietrzak [29], any RSA-OAEP based on the standard RSA problem cannot be secure against CCA2 in the standard model.

Our Contributions: We construct a universal mechanism that can bring enough plaintext awareness for any deterministic encryption scheme. During this construction, we focus on the following aspects:

- Developing a newly padding method that can pad a given plaintext into several different values once the randomness is chosen while the previous method that can only pad a given plaintext into one padding result.
- Obtaining indistinguishable (or semantic) security under CCA2 without random oracle, i.e., the randomness introduced into a ciphertext no longer employ hash function or random oracle.
- Enabling the encrypted message to contain more useful information that may exceed the upper limit of plaintext space or ciphertext space.

We then give this encryption scheme an instantiation of RSA, which is based on a newly arithmetic problem related to the RSA problem but it is weaker than the standard RSA problem.

II. PRELIMINARIES

A. FUNDAMENTAL THEOREM OF ARITHMETIC

For given integer a, $a \geq 2$, there exists a unique factorization such that

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s},$$

where the p_i are distinct primes, $p_i < p_{i+1}$, and at least one of the α_i is a nonzero positive integer.

B. GÖDEL NUMBER

Davis *et al.* [30] defined *Gödel* number of a sequence $(\alpha_1, \alpha_2, \cdots, \alpha_s)$ as a number such that

$$\mathbb{x} = [\alpha_1, \alpha_2, \cdots, \alpha_s] = \prod_{i=1}^{s} p_i^{\alpha_i}, \quad \text{where } \alpha_s \neq 0.$$

For instance, the *Gödel* number of the sequence (34,2,0,19,114,5,0,27) is

$$[34, 2, 0, 19, 114, 5, 0, 27] = 2^{44} \cdot 3^2 \cdot 5^0 \cdot 7^{19} \cdot 11^{114} \cdot 13^5 \cdot 17^0 \cdot 19^{27}.$$

This is a one-to-one mapping between a sequence $(\alpha_1, \alpha_2, \cdots, \alpha_s)$ and an integer $z = \prod_{i=1}^{s} p_i^{\alpha_i}$.

Davis *et al.* [30] put forward that this result is an immediate consequence of the uniqueness of the factorization of integers into primes, which is also referred as the unique factorization theorem or the fundamental theorem of arithmetic. (For a proof, see any elementary number theory textbook.)

C. PADDING-BASED ENCRYPTION SCHEMES

According to Kiltz and Pietrzak [29], a padding-based encryption (PBE) scheme is defined as follows. Assume that g is a public injective transformation, m is a message from the plaintext space, r is a randomness, f is a trapdoor permutation, and $\perp$ is a special rejection symbol. A PBE scheme first applies g to m and r, i.e., $g(m, r)$, and then f to $g(m, r)$, i.e., $Enc(m, r) = f(g(m, r))$. The decryption algorithm inverts $f(g(m, r))$ and an inverse transformation g' of g to reconstruct m (or output '$\perp$'), i.e., $Dec(c) = g'(f^{-1}(c))$. Note that $\coprod = (g, g')$ satisfies the consistency requirement i.e., $g'(g(m, r)) = m$.

D. COLLISION-RESISTANT HASH FUNCTIONS

Assume that $\mathcal{H}$ is a hash function set, $H(\bullet)$ (where '$\bullet$' stands for any input) is a function extracting uniformly from $\mathcal{H}$, and x, y are two different variables. $\mathcal{H}$ is a collision-resistant hash function only if computing $H(x)$ is easy, but finding two different variables x and y that satisfy $H(x) = H(y)$ is difficult. According to [31], hash function set has a weaker notion. Hash function set is a universal family composed one-way hash functions. For an adversary, to extract a $H(\bullet)$ uniformly from $\mathcal{H}$ and find a different input y such that $H(x) = H(y)$ is infeasible, where x is selected by the adversary itself. Such a hash function family is also defined as target collision resistant hash function set. See [32] for recent results and further discussion.

E. SECURE GAMES

Assume that a public encryption scheme is defined by Π, a probabilistic polynomial-time adversary is defined by $\mathcal{A}$, and the security parameter of the public encryption scheme is defined by k. According to [33], the indistinguishable games under IND-CPA and IND-CCA2 should be defined as follows.

The IND-CPA game $PubK^{cpa}_{\mathcal{A},\Pi}(k)$:

1) Given a security parameter 1^k, the challenger runs the Setup algorithm to generate all system parameters, and delivers K_{pub} to the adversary but keeps K_{pri} in private.
2) Having K_{pub}, the adversary $\mathcal{A}$ can access to an encryption oracle $Enc_{K_{pub}}(\cdot)$ (issue arbitrary queries to an 'encryption oracle'). Once $\mathcal{A}$ decides to terminate its access to $Enc_{K_{pub}}(\cdot)$ then it outputs two messages m_0, m_1 such that $|m_0| = |m_1| < |\mathcal{M}|$, where $|m_0| = |m_1|$ means m_0, m_1 have the same length.
3) The challenger uniformly selects a bit $b \leftarrow \{0, 1\}$ and then evaluates a challenge ciphertext $C = Enc_{K_{pub}}(m_b)$ and delivers C to $\mathcal{A}$.
4) $\mathcal{A}$ can continue to access to $Enc_{K_{pub}}(\cdot)$ (issue queries to an 'encryption oracle'). Once $\mathcal{A}$ gives up its access then it outputs a guess bit $b' \in \{0, 1\}$ on b.
5) If $b' = b$, the result of the game is 1, otherwise it is 0. In case, $PubK^{cpa}_{\mathcal{A},\Pi}(k) = 1$, we say that $\mathcal{A}$ succeeds.

If a negligible function $\delta(k)$ exists and satisfies that

$$Adv^{cpa}_{\mathcal{A},\Pi}(k) = \left| Pr[PubK^{cpa}_{\mathcal{A},\Pi}(k) = 1] - \frac{1}{2} \right| \leq \delta(k).$$

the Π is defined as an encryption scheme with semantical secure under adaptive chosen plaintext attacks.

The IND-CCA2 game $PubK^{cca2}_{\mathcal{A},\Pi}(k)$:

1) Given a security parameter 1^k, the challenger runs the Setup algorithm to generate all system parameters, and delivers K_{pub} to the adversary but keeps K_{pri} in private.
2) Except for having K_{pub}, $\mathcal{A}$ has an access to a decryption oracle $Dec_{K_{pri}}(\cdot)$ (make arbitrary queries to a 'decryption oracle'). Once $\mathcal{A}$ decides to terminate its access to $Enc_{K_{pub}}(\cdot)$ then it outputs two messages m_0, m_1 such that $|m_0| = |m_1| < |\mathcal{M}|$, where $|m_0| = |m_1|$ means m_0, m_1 have the same length.
3) The challenger uniformly selects a bit $b \leftarrow \{0, 1\}$ and then evaluates a challenger ciphertext $C = Enc(K_{pub}, m_b)$ and delivers C to $\mathcal{A}$.
4) $\mathcal{A}$ can continue to access to its 'decryption oracle' $Dec_{K_{pri}}(\cdot)$(This access may be adaptive, that is, each query q_i issued to $Dec_{K_{pri}}(\cdot)$ may depend on the replies to $q_1, \cdots, q_{i-1}$.) but is not allowed to request the decryption of the challenge itself. Once $\mathcal{A}$ gives up its access then it outputs a guess bit $b' \in \{0, 1\}$ on b.
5) The output of the game is defined to be 1 if $b' = b$, and 0 otherwise.

If a negligible function $\delta(k)$ exists and satisfies that

$$Adv^{cca2}_{\mathcal{A},\Pi}(k) = \left| Pr[PubK^{cca2}_{\mathcal{A},\Pi}(k) = 1] - \frac{1}{2} \right| \leq \delta(k),$$

the Π is defined as an encryption scheme with semantical secure under adaptive chosen ciphertext attacks.

III. UNIVERSAL TRANSPOSITIONAL PADDING ENCRYPTION SCHEMES

A. GÖDEL ENCODING

There are several methods that can be used to encode a number into *Gödel* encoding, such as short division, circuits, Pollard rho factorization and even cloud outsourcing. Here we give an algorithm (see **Algorithm 1**) based on short division and Pollard rho factorization method.

B. TRANSPOSITIONAL PADDING

Suppose that there is an original sequence $S_{OR} = (\alpha_1, \alpha_2, \cdots, \alpha_i, \cdots, \alpha_s)$, where each α_i is an integer between 0 and $n - 1$. The transpositional padding (TP) is defined as a process to develop a new sequence:

$$(\alpha^t_1, \alpha^t_2, \cdots, \alpha^t_i, \cdots, \alpha^t_{s+h}), \quad h \in Z_n$$

by two steps as follows.

Algorithm 1 Encode($\mathbb{x}$,N)-Encoding a Number Into a *Gödel* Sequence

```
Input: a number $\mathbb{x} < N$.
Output: $(\alpha_1, \alpha_2, \cdots, \alpha_s)$ : $[\alpha_1, \alpha_2, \cdots, \alpha_s] = \mathbb{x}$ and $\alpha_s \neq 0$.
$\mathbb{x}' \leftarrow 1$;
T ← true;
for each $i \le \mathbb{x}$ and $p_i$ do
    if $\mathbb{x} \neq \mathbb{x}'$ then
        if $\min_{t_i \le \mathbb{x}}( p_i^{t_i+1} \mid \mathbb{x}) = T$ then
            $\mathbb{x}' \leftarrow \mathbb{x}' \times p_i^{t_i+1}$;
            $\alpha_i \leftarrow t_i + 1$;
        end if
    end if
    $s \leftarrow i$;
end for
return $(\alpha_1, \alpha_2, \cdots, \alpha_s)$
```

1) Chooses several ℓ-bit random numbers $r_{1\ell}, r_{2\ell}, \cdots, r_{h\ell} \in Z_n$ at random and lays them at the rear of S_{OR} using the following way: $S_{OR+r_\ell} \leftarrow (\alpha_1, \alpha_2, \cdots, \alpha_s, \boxed{\alpha_{s+1} \leftarrow r_{1\ell}}, \boxed{\alpha_{s+2} \leftarrow r_{2\ell}}, \cdots, \boxed{\alpha_{s+h} \leftarrow r_{h\ell}})$;
2) Implements stochastic transposition on $s+h$ elements of S_{OR+r_ℓ}, and thereby generates a stochastic transposition sequence denoted as $S_{TP} = (\alpha_1^t, \alpha_2^t, \cdots, \alpha_{s+h}^t)$.

For example, assume that $S_{OR} = (45, 222, 33, 494, 521, 3, 7)$ is a sequence, and 88, 99, 110 are three numbers selected at random. We can implement an TP on S_{OR} as follows.

1) Lays 88, 99, 110 at the rear of $S_{OR} = (45, 222, 33, 494, 521, 3, 7)$: $S_{OR+r_\ell} = (45, 222, 33, 494, 521, 3, 7, \boxed{\alpha_8 \leftarrow 88}, \boxed{\alpha_9 \leftarrow 99}, \boxed{\alpha_{10} \leftarrow 110})$;
2) Implements transposition stochastically on $7+3 = 10$ elements of S_{OR+r_ℓ}, such as $222 \leftrightarrow 110, 494 \leftrightarrow 88, 3 \leftrightarrow 99$, and thereby generates a stochastic sequence: $S_{TP} \leftarrow (\alpha_1^t, \alpha_2^t, \cdots, \alpha_{10}^t) = (45, 110, 33, 88, 521, 99, 7, 494, 3, 222)$.

C. TP USED FOR ENCRYPTION SCHEMES

For convenience and without loss of generality, we only show how to use TP for encryption when padding one number to a sequence. In this case, an encryption scheme using transpositional padding method develops through the following steps:

1) Encodes the message M as *Gödel* numbers:

$$M = [\alpha_1, \alpha_2, \cdots, \alpha_s],$$

and generates a *Gödel* sequence of plaintext M:

$$S_{OR} \leftarrow (\alpha_1, \alpha_2, \cdots, \alpha_s);$$

2) Selects a random number $r_\ell \in Z_n$ and creates a sequence:

$$S_{OR+r_\ell} \leftarrow (\alpha_1, \alpha_2, \cdots, \alpha_s, \boxed{\alpha_{s+1} \leftarrow r_\ell})$$

by laying r_ℓ at the end of S_{OR};
3) Creates a sequence $S_{L_{\alpha_i}} = (1, 2, \cdots, i \cdots, s+1)$ with the subscript of α_i in sequence S_{OR+r_ℓ};
4) Implements uniform TP operation on the S_{OR+r_ℓ} and $S_{L_{\alpha_i}}$, and forms their respective stochastic transpositions:

$$\pi(1) \leftarrow (\beta_1, \beta_2, \cdots, \beta_{s+1}),$$
$$\pi(2) \leftarrow (\beta_1', \beta_2', \cdots, \beta_{s+1}');$$

5) Concatenates all the elements of $\pi(1)$ such that

$$c' = \beta_1 \| \beta_2 \| \cdots \| \beta_{s+1};$$

6) Concatenates all the elements of $\pi(2)$ such that

$$R_{TP} = \beta_1' \| \beta_2' \| \cdots \| \beta_{s+1}'$$

7) Chooses some encryption scheme to encrypt R_{TP}, and denotes the ciphertext of R_{TP} as c^*;
8) Evaluates $\alpha = H(r_\ell, c', c^*)$, and outputs the ciphertext $c = (c', c^*, \alpha)$;
9) Decrypts c^* using the decryption algorithm corresponding to the encryption scheme chosen in step 8, and obtains the TP massage R_{TP};
10) De-concatenates c' and R_{TP}, thereout, recovers the original sequence S_{OR};
11) Recovers the original message M by

$$M = [\alpha_1, \alpha_2, \cdots, \alpha_s] = \prod_{i=1}^{s} p_i^{\alpha_i}.$$

D. INSTANTIATING TP ENCRYPTION SCHEME OF RSA

By applying *Gödel* numbers encoding and TP to RSA [2], we develop a RSA-type scheme which is defined as RSA-based TP encryption scheme that involves six random algorithms: Key Generate, *Gödel* Encode, TP, Encrypt, Decrypt, Message Recover, which is denoted by

$$\mathcal{E} = (KGen, GEnc, TP, Enc, Dec, MRec).$$

We describe this scheme in Fig 1:

IV. DECISIONAL TP-RSA PROBLEM

The general idea of decisional TP-RSA problem is to decide which one is selected uniformly from $Z_{N=pq}$ at random and which one is computed from TP, between r and $(R_{TP})^e \bmod n$. Formally, assume that R_{TP} is the result developed from plaintext M by seven successive steps described as steps **1)**∼ **7)** in section III-C, $\mathcal{D}$ is a polynomial distinguisher, and D_{Ran}, D_{Rtp} are two distributions:

$$D_{Ran} = \{(n, \mathcal{R}) = (N, r) | n \leftarrow N, \mathcal{R} \overset{r}{\leftarrow} Z_N\},$$

$$D_{Rtp} = \{(n, \mathcal{R}) = (N, (R_{TP})^e \pmod N) | n \leftarrow N, \mathcal{R} \leftarrow (R_{TP})^e \pmod N)\};$$

$$\mathcal{E} = (KGen, GödelEnc, TP, Enc, Dec, MRec)$$

KGen: Upon input 1^n, generates the key (e, N), (d, N) as RSA.
GEnc: Encodes the message M into *Gödel* numbers:

$$M = [\alpha_1, \cdots, \alpha_s],$$

then obtains the *Gödel* sequence of plaintext M: $(\alpha_1, \alpha_2, \cdots, \alpha_s)$.
TP: $S_{OR} \leftarrow (\alpha_1, \alpha_2, \cdots, \alpha_s)$, $S_{OR+r_\ell} \leftarrow (\alpha_1, \alpha_2, \cdots, \alpha_s, \boxed{\alpha_{s+1} \leftarrow r_\ell})$, $S_{L_{\alpha_i}} \leftarrow (1, 2, \cdots, s+1)$(where $1 \leq i \leq s+1$ represents the position of α_i in the sequence of S_{OR+r_ℓ}), $\pi(1) \leftarrow (\beta_1, \beta_2, \cdots, \beta_{s+1})$, $\pi(2) \leftarrow (\beta'_1, \beta'_2, \cdots, \beta'_{s+1})$.
Enc: Inputs (e, N), computes $c' = \beta_1 \| \beta_2 \| \cdots \| \beta_{s+1}$, $R_{MTP} = \beta'_1 \| \beta'_2 \| \cdots \| \beta'_{s+1}$, and computes $c^* \equiv (R_{MTP})^e \bmod N$; then outputs the ciphertext $c = (c', c^*, \alpha)$.
Dec: Inputs (e, N, d) and ciphertext c, returns $Dec(c^*) = ((c^*)^d) \bmod N = R_{MTP}$; de-concatenates c' and R_{TP}, then recovers the origin sequence S_{OR} and the random number r'_ℓ; then evaluates $\alpha' = H(r'_\ell, c', c^*)$.
MRec: Verifies $\alpha' \overset{?}{=} \alpha$, if $\alpha' = \alpha$, then computes $m = [\alpha_1, \alpha_2, \cdots, \alpha_s] = \prod_{i=1}^{s} p_i^{\alpha_i}$.

FIGURE 1. Scheme $\mathcal{E}$ = (*KGen*, *GödelEnc*, *TPad*, *Enc*, *Dec*, *MRec*).

The decisional TP-RSA problem can be expressed as follows. The advantage $Adv_{\mathcal{D}}(k)$ of the distinguisher $\mathcal{D}$ distinguishing distributions D_{Ran} from D_{Rtp} can be expressed as

$$Adv_{\mathcal{D}}(k) = \left| Pr\left[\mathcal{D}(n, \mathcal{R}) = D_{Ran}\right] - Pr\left[\mathcal{D}(n, \mathcal{R}) = D_{Rtp}\right] \right|,$$

where $\mathcal{D}(n, \mathcal{R}) \in \{D_{Ran}, D_{Rtp}\}$, and k is the security parameter of the TP-RSA scheme.

We say the decisional TP-RSA problem is intractable for any probabilistic algorithm $\mathcal{D}$ in polynomial-time if a negligible function $(\delta(k))$ exists and satisfies that

$$Adv_{\mathcal{D}}(k) \leq \delta(k).$$

Theorem 1: The decisional TP-RSA problem is as intractable as RSA prolem.

Proof: Recall that R_{TP} is developed in section III-D as the following steps:

(1) Encodes the message M into *Gödel* numbers such that

$$M = [\alpha_1, \cdots, \alpha_s],$$

and obtains the *Gödel* sequence $(\alpha_1, \alpha_2, \cdots, \alpha_s)$ of plaintext M;

(2) Selects a random number $r_\ell \in Z_n$ and creates a sequence$(\alpha_1, \alpha_2, \cdots, \alpha_s, \alpha_{s+1})$ by laying r_ℓ at the rear of S_{OR}:

$$S_{OR+r_\ell} \leftarrow (\alpha_1, \alpha_2, \cdots, \alpha_s, \boxed{\alpha_{s+1} \leftarrow r_\ell});$$

(3) Constructs a sequence $S_{L_{\alpha_i}} = (1, 2, \cdots, i \cdots, s+1)$ with the subscript of α_i in sequence S_{OR+r_ℓ};

(4) Implements TP operation in the S_{OR+r_ℓ} and $S_{L_{\alpha_i}}$ uniformly, and thereby forms their respective stochastic transpositions:

$$\pi(1) \leftarrow (\beta_1, \beta_2, \cdots, \beta_{s+1}),$$
$$\pi(2) \leftarrow (\beta'_1, \beta'_2, \cdots, \beta'_{s+1});$$

(5) Concatenates all the elements of $\pi(1)$ such that

$$c' = \beta_1 \| \beta_2 \| \cdots \| \beta_{s+1};$$

(6) Concatenates all the elements of $\pi(2)$ such that

$$R_{TP} = \beta'_1 \| \beta'_2 \| \cdots \| \beta'_{s+1}.$$

This implies that R_{TP} is generated by stochastic transposition from a random number $r_\ell \in Z_N$, and $(R_{TP})^e \pmod{N}$ that distributes uniformly in Z_N. So D_{Ran} and D_{Rtp} are two identical distributions, in the view of distinguisher $\mathcal{D}$, unless $\mathcal{D}$ can solve the RSA problem. In fact, there is no algorithm that can solve RSA problem in polynomial time on non-quantum computers. Consequently, the decisional TP-RSA problem is as intractable as RSA prolem.

V. SECURITY PROOF

In this section, we show that the developed scheme $\mathcal{E}$ is secure against CCA2 in light of a logic as follows. We first reduce the higher security(IND-CCA2) of scheme $\mathcal{E}$ to its lower security(IND-CPA). Then we reduce its lower security to the decisional TP-RSA problem. In other words, we show that if $\mathcal{E}$ cannot be against CCA2 then it cannot be against CPA either, if $\mathcal{E}$ cannot be against CPA then we can employ $\mathcal{E}$ as a subroutine to construct an algorithm that can be used to solve the TP-RSA problem, which implies that RSA problem is feasible to solve, which contradicts the facts.

A. SECURITY ON CPA

We prove that our scheme $\mathcal{E}$ has indistinguishability in the presence both of an eavesdropper and active attacker, which implies that it is IND-CPA secure by the security definition in [11].

Theorem 2: If the decisional TP-RSA problem is intractable, $\mathcal{E}$ is an encryption scheme with indistinguishable security under the adaptive CPA.

Proof: Recall that the challenger of the decisional TP-RSA runs in the following ways: runs $\mathcal{G}(1^n)$ to generate (e, N); uniformly chooses a random number $r_\ell \in Z_n$ and a $f \in \{0, 1\}$; if $f = 0$ sets $\mathcal{R} = (R_{MTP})$, otherwise sets $\mathcal{R} = R$; and finally, delivers $(e, N, (N, \mathcal{R}))$ to adversary $\mathcal{A}$.

Assume that $\mathcal{E}$ = (KGen, GEnc, TP, Enc, Dec, MRec) is our TP encryption scheme, $\mathcal{A}$ denotes a polynomial-time adversary attacking $\mathcal{E}$, and δ denotes its succeeding advantage in the IND-CPA security game. We can use algorithm $\mathcal{A}$ as a subroutine to construct an algorithm that is used to solve the decisional TP-RSA problem via the following way.

Algorithm 2 Algorithm $\mathcal{B}$

```
1. Receives parameters $(e, N, (N, \mathcal{R}))$ from the decisional TP challenger;
2. Sets $pk = (e, N)$;
3. Sends $1^n$ and $pk$ to $\mathcal{A}$;
4. Receives $M_b$ from $\mathcal{A}$, where $(b \in \{0, 1\}) \wedge (M_0 = M_1)$;
5. Uniformly selects a $b \in \{0, 1\}$;
6. Transform $M_b$ into $R_{M_bTP}$ according to steps 1)∼7) in section III-C;
7. Sets $c^* = (e, N, \mathcal{R} \cdot (R_{M_bTP})^{e-1} \bmod N)$ and delivers it to $\mathcal{A}$;
8. Denotes $\mathcal{A}$'s guess output about $b$ by $b'$;
9. Outputs $f'$ (If $b = b'$, then $f'$ is set to be 0, otherwise, $f'$ is set to be 1).
```

Composed of the polynomial-time algorithms $\mathcal{A}$ and $\mathcal{G}(1^n)$, $\mathcal{B}$ is also a polynomial-time algorithm. By the Bayes Theorem, the probability that $\mathcal{B}$ wins the decisional TP-RSA security game can be computed as follows.

$$\begin{aligned} &Pr[f = f'] \\ &= Pr[f=0]Pr[f=f'|f=0] + Pr[f=1]Pr[f=f'|f=1] \\ &= \frac{1}{2}Pr[f' = 0|f = 0] + \frac{1}{2}Pr[f' = 1|f = 1] \\ &= \frac{1}{2}Pr[b = b'|f = 0] + \frac{1}{2}Pr[b \neq b'|f = 1]. \end{aligned} \tag{1}$$

When it comes with $f = 0$, the decisional TP-RSA challenger will set $\mathcal{R}$ to be R_{M_bTP}. In this case, the view presented to $\mathcal{A}$ by $\mathcal{B}$ is identical to the view of $\mathcal{A}$ in the actual IND-CPA security game. Hence, condition on $f = 0$, the probability of $b = b'$ is equal to what $\mathcal{A}$ wins the IND-CPA security game i.e.,

$$Pr[b = b'|f = 0] = \frac{1}{2} + \delta. \tag{2}$$

When it comes with $f = 1$, the decisional TP-RSA challenger will set $\mathcal{R}$ to be R. Because R is uniformly picked from Z_n, it follows that $(R_{M_bTP})^{e-1} \cdot \mathcal{R} \pmod N$ distributes uniformly on Z/NZ. Moreover, the random variables $M_0, M_1, R_{M_0TP}, R_{M_1TP}$ and b are jointly independent. Therefore, pk and c^* do not disclose any information about b, and the guess b' about b must be independent of b. Since the probabilities of b being 0 and 1 are $\frac{1}{2}$ respectively, it follows that

$$Pr[b = b'|f = 1] = \frac{1}{2}. \tag{3}$$

Combining all the three equations (1),(2) and (3), we have

$$Pr[f = f'] = \frac{1}{2}(\frac{1}{2} + \delta) + \frac{1}{2} \times \frac{1}{2} = \frac{1}{2} + \frac{1}{2}\delta. \tag{4}$$

Thus, the advantage that $\mathcal{B}$ succeeds in the decisional TP-RSA security can be calculated as

$$\left|Pr[f = f'] - \frac{1}{2}\right| = \left|(\frac{1}{2} + \frac{1}{2}\delta) - \frac{1}{2}\right| = \frac{\delta}{2}. \tag{5}$$

As we have showed that decisional TP-RSA problem is intractable, $\mathcal{B}$ can succeed only with a negligible advantage in the decisional TP-RSA security game, which means that $\frac{\delta}{2}$ must be a negligible value. It follows immediately that δ must be also a negligible value. Therefore, algorithm $\mathcal{A}$ can win the IND-CPA game only with a negligible advantage.

B. SECURITY ON CCA2

Theorem 3: If scheme $\mathcal{E}$ is secure under CPA, and $H(\cdot)$ is a collision-resistant hash fuction, $\mathcal{E}$ is an indistinguishable encryption scheme with CCA2 security.

Proof: We prove this theorem according to the logic below. Since $H(\cdot)$ is collision-resistant, α can be viewed as the unique fingerprint of (r_ℓ, c', c^*), and all the queries issued to the decryption oracle are viewed to be invalid, unless these queries were previously ciphertexts obtained by the adversary from its encryption oracle. In this case, because the response does not need the decryption oracle at all, $\mathcal{E}$'s CCA2 security is reduced to its IND-CPA security. More specifically, we first show that the queries issued to the decryption oracle by the adversary are valid only with a negligible probability, unless those queries were previously generated by the encryption oracle. Given this claim, we then show that if $\mathcal{E}$ is not secure against CCA2, but neither is it secure against CPA. It follows from the fact that any adversary amounting to CPA in a scheme with IND-CPA security can actually simulate a decryption oracle for a CCA2 adversary, but it makes the CCA2 adversary feel no gaps. This is because all the simulation works via the following way: (1) returning 'rejection' if the issued ciphertexts were never queried before; (2) returning the appropriate message corresponding to the queries if the ciphertexts were queried before(or evaluated by the encryption oracle). The validity of the simulation follows from **Claim 1** and **Claim 2**. We now conduct the formal proof.

Let $\mathcal{A}$ be any probabilistic polynomial-time adversary carrying out CCA2 on $\mathcal{E}$. Define *ValidQuery* as the event that in the game $PubK^{cca2}_{\mathcal{A},\mathcal{E}}(k)$. In order to succeed, $\mathcal{A}$ has to generate a query (c', c^*) to the decryption oracle, where (c', c^*) are not the previous ones generated by the encryption oracle. However, when it comes to the following cases

$$C1 \begin{cases} \text{Selects a random number } r_\ell{}', \\ \text{Selects two random numbers } r_1, r_2 \text{ to substitute} \\ c', c^* \text{ respectively,} \\ \text{Evaluates } \alpha' = H(r_\ell{}', r_1, r_2), \\ \text{The ciphertext is } c = (r_1, r_2, \alpha'). \end{cases}$$

$$C2\begin{cases}\text{Selects a random number } r_\ell{}', \\ \text{Selects one random number } r \text{ to substitute } c' \text{ or } c^*, \\ \text{Evaluates } \alpha' = H(r_\ell{}', c', r) \text{ or } \alpha' = H(r_\ell{}', r, c^*), \\ \text{The ciphertext is } c = (c', r, \alpha') \text{ or } c = (r, c^*, \alpha').\end{cases}$$

$$C3\begin{cases}\text{Selects a random number } r_\ell{}', \\ \text{Evaluates } \alpha' = H(r_\ell{}', c', c^*), \\ \text{The ciphertext is } c = (c', c^*, \alpha').\end{cases}$$

such that:

$$\begin{aligned}&Pr[PubK^{cca2}_{\mathcal{A},\mathcal{E}}(n)] = 1] \\ &\quad\le Pr[ValidQuery] + Pr[PubK^{cca2}_{\mathcal{A},\mathcal{E}}(n) = 1 \wedge \overline{ValidQuery}].\end{aligned}$$

Now this theorem follows immediately from **Claim 1** and **Claim 2** below.

Claim 1: If $H(\cdot)$ is collision-resistant, $Pr[ValidQuery]$ is at most a negligible value.

Intuitively, this comes from the fact that if the event *ValidQuery* occurs (with the premise that $H(\cdot)$ is collision-resistant), $\mathcal{A}$ then successfully forges a valid unique fingerprint for (r_ℓ, c', c^*). This implies that $\mathcal{A}$ finds out a $(r'_\ell, c'', c^{*\prime})$ such that $H(r_\ell, c', c^*) = H(r'_\ell, c'', c^{*\prime})$. We argue that if such a case appears with a non-negligible probability, it follows that $H(\cdot)$ is not universal one-way at all, which contradicts the fact that $H(\cdot)$ is a hash function selected uniformly from the universal one-way family of hash functions.

Therefore, the i^{th} invalid ciphertext issued by $\mathcal{A}$ will be rejected with a probability at least $1 - 1/(q(n) - i + 1)$, where $i \in Z_{q(n)}$ and the polynomial $q(n)$ is an upper-bound of oracle queries issued by $\mathcal{A}$. This implies that only except for a negligible probability, the decryption oracle cannot accept any invalid ciphertexts, i.e.,

$$Pr[H(r_\ell, c', c^*) = H(r'_\ell, c'', c^{*\prime})] \ge \frac{Pr[ValidQuery]}{q(n)}.$$

It makes sense that *ValidQuery* occurs except a negligible probability, i.e.,

$$Pr[ValidQuery] \le \delta(n).$$

Claim 2: There exists a negligible value $\delta'(n)$ satisfying that

$$Pr\left[PubK^{cca2}_{\mathcal{A},\mathcal{E}}(n) = 1 \wedge \overline{ValidQuery}\right] \le \frac{1}{2} + \delta'(n).$$

We assume that $\mathcal{A}$ is a probabilistic polynomial-time adversary for $PubK^{cca2}_{\mathcal{A},\mathcal{E}}$, and $\mathcal{A}_\mathcal{E}$ is an adversary carrying out CPA on $\mathcal{E}$. In the following, we employ $\mathcal{A}$ to construct the adversary $\mathcal{A}_\mathcal{E}$ for the CPA experiment with $\mathcal{E}$.

Adversary $\mathcal{A}_\mathcal{E}$ selects $(e, N) \leftarrow \{0,1\}^n$ and calls $\mathcal{A}$. Whenever $\mathcal{A}$ issues an encryption query for m, $\mathcal{A}_\mathcal{E}$ works as follows:

1) Selects $(e, N) \leftarrow \{0,1\}^n$.
2) Invokes the CCA2 adversary $\mathcal{A}$; Adversary $\mathcal{A}_\mathcal{E}$ then simulates the encryption oracle for $\mathcal{A}$ in the way that using key pair (e, N). When $\mathcal{A}$ issues the query to the encryption oracle for m, $\mathcal{A}_\mathcal{E}$ answers as follows.
    a) turns to issue this query to the encryption oracle, and gets a reply (c', c^*);
    b) choose a random number r_ℓ;
    c) computes $\alpha \leftarrow H(r_\ell, c', c^*)$, and delivers (c', c^*, α) to $\mathcal{A}$;

    When $\mathcal{A}$ issues (c', c^*, α) to the decryption oracle, $\mathcal{A}_\mathcal{E}$ answers as follows.

    If (c', c^*, α) was ever generated from an encryption query, then returns m. Else, outputs "rejection".
3) As the adversay $\mathcal{A}$ outputs a message pair (m_0, m_1), the adversary $\mathcal{A}_\mathcal{E}$ also outputs (m_0, m_1), and $\mathcal{A}_\mathcal{E}$ then receives the challenge ciphertext c^*. $\mathcal{A}_\mathcal{E}$ computes $\alpha \leftarrow H(r_\ell, c', c^*)$, and delivers (c', c^*, α) that acts as the the challenge ciphertext to $\mathcal{A}$. As above, $\mathcal{A}_\mathcal{E}$ proceeds with handing (c', c^*, α)(acts as the challenge ciphertext) to $\mathcal{A}$, where $\alpha = H(r_\ell, c', c^*)$.

Notice that for any new query issued by $\mathcal{A}$, the adversary $\mathcal{A}_\mathcal{E}$ only needs to responses with '$\perp$', i.e., $\mathcal{A}_\mathcal{E}$ does not need to turn to a decryption oracle. This implies that any new query issued by $\mathcal{A}$ is treated as invalid by $\mathcal{A}_\mathcal{E}$. In addition, the adversary $\mathcal{A}_\mathcal{E}$ runs in a probabilistic polynomial-time because it just calls $\mathcal{A}$, and $\alpha = H(r_\ell, c', c^*)$ can be evaluated in a probabilistic polynomial-time. Therefore, it is straightforward to see that when the event *ValidQuery* does not appear, the probability that the adversary $\mathcal{A}_\mathcal{E}$ succeeds in the security game $PubK^{cpa}_{\mathcal{A}_\mathcal{E},\mathcal{E}}$ equals to the probability that $\mathcal{A}$ succeeds in the security game $PubK^{cca2}_{\mathcal{A},\mathcal{E}}$. That is,

$$\begin{aligned}Adv^{cpa}_{\mathcal{A}_\mathcal{E},\mathcal{E}}(n) &= Adv^{cca2}_{\mathcal{A},\mathcal{E}}(n) \\ &= Pr[PubK^{cpa}_{\mathcal{A}_\mathcal{E},\mathcal{E}}(n) = 1 \wedge \overline{ValidQuery}] \\ &= Pr[PubK^{cca2}_{\mathcal{A},\mathcal{E}}(n) = 1 \wedge \overline{ValidQuery}],\end{aligned}$$

which implies that

$$\begin{aligned}Pr[PubK^{cpa}_{\mathcal{A}_\mathcal{E},\mathcal{E}}(n){=}1] &\ge Pr[PubK^{cpa}_{\mathcal{A},\mathcal{E}}(n){=}1 \wedge \overline{ValidQuery}] \\ &= Pr[PubK^{cca2}_{\mathcal{A},\mathcal{E}}(n){=}1 \wedge \overline{ValidQuery}].\end{aligned}$$

Since $\mathcal{E}$ has been proven to be a scheme with indistinguishable security under CPA in **A** of **Section V**, there must exist a negligible value $\delta'(n)$ such that

$$Pr[PubK^{cpa}_{\mathcal{A}_\mathcal{E},\mathcal{E}}(n) = 1] \le \frac{1}{2} + \delta'(n).$$

Consequently,

$$\begin{aligned}Adv^{cca2}_{\mathcal{A},\mathcal{E}}(n) &= \left|Pr[PubK^{cca2}_{\mathcal{A},\mathcal{E}}(n) = 1] - \frac{1}{2}\right| \\ &\le |Pr[ValidQuery] \\ &\quad + Pr[PubK^{cca2}_{\mathcal{A},\mathcal{E}}(n) = 1 \wedge \overline{ValidQuery}] - \frac{1}{2}| \\ &\le \left|\delta(n) + (\frac{1}{2} + \delta'(n)) - \frac{1}{2}\right| \\ &= \delta(n) + \delta'(n).\end{aligned}$$

Obviously, $\delta(n) + \delta'(n)$ is a negligible value, value, since we have shown both $\delta'(n)$ and $\delta(n)$ are negligible values in **A** of **Section V**. Hence, it follows that the adversary $\mathcal{A}$

TABLE 1. Comparisons between OAEP and TP.

Type	PA-HNO	CCA2-No-RO	CUI-E-UPL	GPSR-P-DV
OAEP	×	×	×	×
OAEP+	×	×	×	×
OAEP++	×	×	×	×
TP	√	√	√	√

×: having no certain property;
√: having certain property.

succeeds only with a negligible advantage in the security game $PubK^{cca2}_{\mathcal{A},\mathcal{E}}$. To conclude, $\mathcal{E}$ is an encryption scheme with semantical security against CCA2.

C. ADVANTAGES ANALYSIS

Compared to some other padding methods(OAEP, OAEP+, OAEP++) that transform a deterministic encryption scheme to a probabilistic one, our padding way (TP) has three advantages as follows (A simple and clear comparison, as shown in Tab 1).

1 In terms of security, our TP scheme only uses simple transposition to make a deterministic encryption scheme achieve plaintext awareness while OAEP, OAEP+ and OAEP++ need complex hash-net operations(simply denoted by PA-HNO); and to make a deterministic encryption scheme achieve CCA2 security, our TP scheme only relies on the selected randomness, as opposed to OAEP, OAEP+ and OAEP++ that heavily rely on random oracle(simply denoted by CCA2-No-RO).

2 For the same length of plaintext, including the introduced random number(s), TP enables an encryption operation to carry more useful information that may exceed the upper limit of plaintext space or ciphertext space while OAEP, OAEP+ and OAEP++ enable an encryption operation to carry useful information that is k bits smaller than the upper limit of plaintext space or ciphertext space (k is the length of the random number that these schemes are used to fill)(simply denoted by CUI-E-UPL).

3 Regarding the padding effect, compared to OAEP, OAEP+ and OAEP++ that can only pad a given plaintext into one padding result with the selected randomness, our TP scheme can pad the plaintext into several different values(simply denoted by GPSR-P-DV).

VI. CONCLUSIONS

We propose a universal encryption scheme with a novel property that can transform any deterministic encryption scheme to a probabilistic one. An instantiation of RSA to this universal encryption scheme is constructed. This example of RSA is proved semantically indistinguishable under CCA2. In addition, a new arithmetic problem related to RSA, defined as decisional TP-RSA, is put forward.

REFERENCES

[1] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in *Proc. Annu. Int. Cryptol. Conf.* New York, NY, USA: Springer, 2007, pp. 535–552.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[3] M. U. Sharif, R. Shahid, K. Gaj, and M. Rogawski, "Hardware-software codesign of RSA for optimal performance vs. Flexibility trade-off," in *Proc. FPL*, Aug./Sep. 2016, pp. 1–4.

[4] A. Boorghany, S. B. Sarmadi, P. Yousefi, P. Gorji, and R. Jalili, "Random data and key generation evaluation of some commercial tokens and smart cards," in *IEEE ISSCC Dig. Tech. Papers.*, Sep. 2014, pp. 49–54.

[5] F.-Y. Leu, Y.-L. Huang, and S.-M. Wang, "A secure M-commerce system based on credit card transaction," *Electron. Commerce Res. Appl.*, vol. 14, no. 5, pp. 351–360, 2015.

[6] A. B. Justicia, "Privacy-preserving mechanisms for e-commerce," in *Proc. 2nd URV Doctoral Workshop Comput. Sci. Math.* Tarragona, Spain: Publicacions Universitat Rovira I Virgili, 2015, p. 21.

[7] Y. Shi, J. Lin, G. Xiong, X. Wang, and H. Fan, "Key-insulated undetachable digital signature scheme and solution for secure mobile agents in electronic commerce," *Mobile Inf. Syst.*, vol. 2016, Apr. 2016, Art. no. 4375072.

[8] D. Kumar and N. Goyal, "Security issues in M-commerce for online transaction," in *Proc. 5th Int. Conf. Rel., Infocom Technol. Optim. (Trends Future Directions)(ICRITO)*, Sep. 2016, pp. 409–414.

[9] A. A. Al-Saggaf and L. Ghouti, "Efficient abuse-free fair contract-signing protocol based on an ordinary crisp commitment scheme," *IET Inf. Secur.*, vol. 9, no. 1, pp. 50–58, 2015.

[10] N. Koblitz and A. J. Menezes, "Cryptocash, cryptocurrencies, and cryptocontracts," *Des., Codes Cryptogr.*, vol. 78, no. 1, pp. 87–102, 2016.

[11] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, Apr. 1984.

[12] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *Proc. 22nd Annu. ACM Symp. Theory Comput.*, 1990, pp. 427–437.

[13] M. Bellare, M. Fischlin, A. O'Neill, and T. Ristenpart, "Deterministic encryption: Definitional equivalences and constructions without random oracles," in *Proc. Annu. Int. Cryptol. Conf.* New York, NY, USA: Springer, 2008, pp. 360–378.

[14] A. Boldyreva, S. Fehr, and A. O'Neill, "On notions of security for deterministic encryption, and efficient constructions without random oracles," in *Proc. Annu. Int. Cryptol. Conf.* New York, NY, USA: Springer, 2008, pp. 335–359.

[15] I. Mironov, O. Pandey, O. Reingold, and G. Segev, "Incremental deterministic public-key encryption," *J. Cryptol.*, vol. 31, no. 1, pp. 134–161, 2018.

[16] B. Fuller, A. O'Neill, and L. Reyzin, "A unified approach to deterministic encryption: New constructions and a connection to computational entropy," *J. Cryptol.*, vol. 28, no. 3, pp. 671–717, 2015.

[17] Z. Brakerski and G. Segev, "Better security for deterministic public-key encryption: The auxiliary-input setting," *J. Cryptol.*, vol. 27, no. 2, pp. 210–247, 2014.

[18] M. Bellare and V. T. Hoang, "Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* New York, NY, USA: Springer, 2015, pp. 627–656.

[19] V. Koppula, O. Pandey, Y. Rouselakis, and B. Waters, "Deterministic public-key encryption under continual leakage," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.* New York, NY, USA: Springer, 2016, pp. 304–323.

[20] M. Bellare, R. Dowsley, and S. Keelveedhi, "How secure is deterministic encryption?" in *Proc. IACR Int. Workshop Public Key Cryptogr.* New York, NY, USA: Springer, 2015, pp. 52–73.

[21] M. Bellare and P. Rogaway, "Optimal asymmetric encryption," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* New York, NY, USA: Springer, 1994, pp. 92–111.

[22] V. Shoup, "OAEP reconsidered," in *Proc. Annu. Int. Cryptol. Conf.* New York, NY, USA: Springer, 2001, pp. 239–259.

[23] D. Boneh, "Simplified OAEP for the RSA and rabin functions," in *Proc. Annu. Int. Cryptol. Conf.* New York, NY, USA: Springer, 2001, pp. 275–291.

[24] T. Okamoto and D. Pointcheval, "REACT: Rapid enhanced-security asymmetric cryptosystem transform," in *Proc. Cryptograph. Track RSA Conf.* New York, NY, USA: Springer, 2001, pp. 159–174.

[25] D. H. Phan and D. Pointcheval, "OAEP 3-round: A generic and secure asymmetric encryption padding," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.* New York, NY, USA: Springer, 2004, pp. 63–77.

[26] E. Kiltz, A. O'Neill, and A. Smith, "Instantiability of RSA-OAEP under chosen-plaintext attack," *J. Cryptol.*, vol. 30, no. 3, pp. 889–919, 2017.

[27] S. A. Kakvi and E. Kiltz, "Optimal security proofs for full domain hash, revisited," *J. Cryptol.*, vol. 31, no. 1, pp. 276–306, 2018.

[28] M. Bellare and P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols," in *Proc. 1st ACM Conf. Comput. Commun. Secur.*, 1993, pp. 62–73.

[29] E. Kiltz and K. Pietrzak, "On the security of padding-based encryption schemes-or-why we cannot prove OAEP secure in the standard model," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* New York, NY, USA: Springer, 2009, pp. 389–406.

[30] M. Davis, R. Sigal, and E. J. Weyuker, *Computability, Complexity, and Languages: Fundamentals of Theoretical Computer Science*. Amsterdam, The Netherlands: Elsevier, 1994.

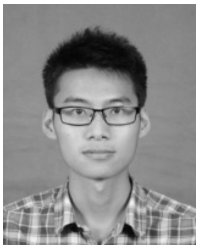
[31] M. Naor and M. Yung, "Universal one-way hash functions and their cryptographic applications," in *Proc. 21st Annu. ACM Symp. Theory Comput.*, 1989, pp. 33–43.

[32] I. Haitner, T. Holenstein, O. Reingold, S. Vadhan, and H. Wee, "Universal one-way hash functions via inaccessible entropy," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Springer, 2010, pp. 616–637.

[33] Y. Lindell and J. Katz, *Introduction to Modern Cryptography*. London, U.K.: Chapman & Hall, 2014.

LINMING GONG received the Ph.D. degree from the School of Computer Science, Shaanxi Normal University. He is currently a Teaching Fellow with the School of Computer Science, Xi'an Polytechnic University, Xi'an, China. His current research interests include applied cryptography, secure multiparty computation, computer and network security, mobile and wireless communication security, and privacy-preserving data mining.

MINGMING WANG received the Ph.D. degree from the School of Computer Science, Beijing University of Posts and Telecommunications, China, in 2013. He is currently an Associate Professor with the School of Computer Science, Xi'an Polytechnic University. His research interests include information security, quantum communication, and quantum computation.



XIANGJIAN ZUO is currently pursuing the Ph.D. degree with the School of Cyber-Security, Beijing University of Posts and Telecommunications, China. His main research interests include information security and privacy preserving.

SHUNDONG LI received the Ph.D. degree from the School of Computer Science, Xi'an Jiaotong University. He is currently a Professor of computer science with Shaanxi Normal University, Xi'an, China. He is also an Associate Professor with the School of Computer Science, Beijing Normal University, Beijing, China. His current research interests include secure multiparty computation, computer and network security, and privacy-preserving data mining.

DAOSHUN WANG received the Ph.D. degree from the College of Mathematics, Sichuan University. He is currently an Associate Professor of computer science with Tsinghua University, Beijing, China. His current research interests include applied cryptography, secret sharing, and computer and network security.