Received January 1, 2020, accepted January 13, 2020, date of publication January 17, 2020, date of current version January 28, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2967457

Public-Key Encryption Secure Against Related Randomness Attacks for Improved End-to-End Security of Cloud/Edge Computing

PENGTAO LIU
College of Cybersecurity, Shandong University of Political Science and Law, Jinan 250014, China
e-mail: ptwave@163.com

This work was supported in part by the Shandong Province Higher Educational Science and Technology Program under Grant J15LN01.

ABSTRACT Public-key encryption is often used to protect data security/privacy and secure communication in scenarios of cloud computing and edge computing. Related randomness attacks model (RRA) for public-key encryption was motivated by randomness failures. This paper proposes some methods of constructing secure public-key encryption scheme against related randomness attacks, i.e. RRA-CPA secure public-key encryption scheme with efficient decryption algorithm and short ciphertexts size obtained from one-way function with weak RKA-security and indistinguishability obfuscation, RRA-CPA secure public-key encryption scheme against arbitrarily function from any publicly deniable encryption and RRA-CCA secure public-key encryption scheme against arbitrarily function from standard IND-CCA public-key encryption scheme with a hardcore function for arbitrarily correlated inputs.

INDEX TERMS Arbitrary restricted function, publicly deniable encryption, public-key encryption, related randomness attack.

I. INTRODUCTION

The rise of Internet, Internet of Things and Cloud Computing, as well as the rapid popularization of mobile devices, intelligent terminals, social networks and e-commerce, has led to the rapid growth of data volume. Cloud computing provides a technical platform and often recommends services to users by cloud service recommendation [1]–[3] for the storage, computation and management of large data, which makes the processing of large data more convenient and efficient. As cloud computing releases the user's burden in maintaining basic storage infrastructures, many individuals and institutions adopt cloud storage to maintain their data so that more and more data are stored on cloud servers. However, cloud servers may tamper with, delete and damage data. Although there are many techniques to improve cloud security [4], [5], the simplest method for the data owners to share the data while keeping the security and privacy is encrypting data using public-key encryption and uploading it to cloud servers.

Traditional cloud computing cannot handle the huge data generated by network edge devices which makes the birth of edge computing solving the problem in combination with cloud computing [6], [7] which scenario is showed in Fig. 1. Edge computing is widely used in the Internet of things, especially in the application scenarios with special requirements such as low delay, high bandwidth, high reliability, massive connections, heterogeneous convergence, local security and privacy-preserving [8]–[15]. The edge computing model requires secure communication among the clouds and the edges. Public-key encryption (PKE) is suitable for the end-to-end security of edge computing participants and is

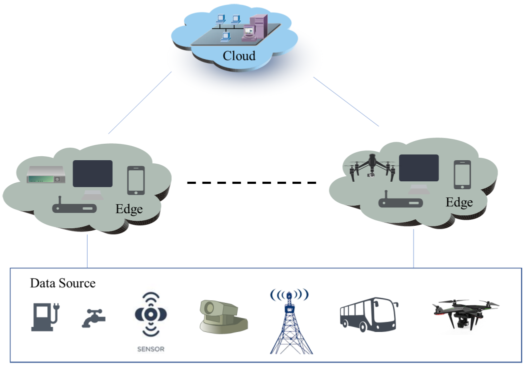

FIGURE 1. Cloud-edge computing scenario.

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaokang Wang.

often used for exchanging a session key between unknown partners according to its advantages in secure broadcast and authentication, while there are many techniques to ensure the edge computing security [16], [17].

The development of information technology has also led to further integration of information, physical systems and human society to form a more complex system, i.e. Cyber-physical-social system (CPSS). The strong coupling of CPSS brings security and privacy issues, e.g. multi-source spatial data can be associated to leak user privacy. Many technologies can be applied to protect the data privacy of cyber-physical-social system, including anonymity, trusted computing, encryption, verifiable computing and data obfuscation, in which public-key encryption can be used for security and access control in cyber-physical-social systems.

Randomness quality is crucial to the security of cryptosystems that consuming lots of randomnesses. However, many researches such as [18]–[21] show the randomness failures including randomness reuse, randomness tampering, etc. For cloud/edge computing scenario, [22] showed that the securely kept DSA keys used in TLS authentication sessions could be extracted by virtual-machine reset attacks due to the randomness repetition. These failures can cause some security problems such as signing keys exposure, plaintext recovery, weak key generation and so on. Motivated by preserving security under randomness failures, related randomness attacks model (RRA) for PKE was abstracted and secure cryptosystems were constructed in this model. Informally, in this model, the adversary has the ability to control the randomness used during encryption and the indistinguishability of ciphertexts should be kept on this condition.

In this paper, we focus on constructing secure PKE schemes in the model of related randomness attacks. First, we propose a method of constructing RRA secure PKE scheme *under chosen plaintext attack* (RRA-CPA) based on indistinguishability obfuscation and one-way function with weak RKA-security. To acquire RRA security against arbitrary function, we give two constructions. The first one is publicly deniable encryption which can be proved to have RRA security *under chosen plaintext attack* (RRA-CPA), and the other one is constructed by combining a secure standard PKE scheme *under chosen ciphertext attack* (IND-CCA) with a hardcore function for arbitrarily correlated inputs which can achieve RRA security *under chosen ciphertext attack.*

A. RELATED WORKS

Recently, many works address the problem of randomness failures. Austrin *et al.* [23] showed a negative result that standard encryption schemes can be broken under randomness failure. Feltz and Cremers [24] analyzed the authenticated key exchange protocols and showed that bad randomness results in the insecurity of the protocols. Paterson *et al.* [25] introduced a security model for PKE schemes called "*related randomness attacks model*", in which the adversary has the ability to force the usages of related randomness in encryption which are abstracted to the outputs of specified functions applied to some initial randomness. They also proposed many kinds of schemes in this model. They showed that a RRA-secure PKE in the random oracle model can be obtained by taking the hash value of the input random together with the message and public key as the rand coins used in encryption. To construct a RRA-secure PKE scheme in the standard model, they applied pseudorandom function secure against related-key attacks (RKA-PRF) to a standard PKE scheme. The restricted function families depend on that of RKA-PRF which currently are restricted to the function families consisting of polynomials of bounded degree according to the instantiations of available RKA-PRFs. To obtain further constructions for other kinds of restricted function families, Paterson et al. considered weakened security models; they first restricted honest generations of the public keys (HK-RRA) and provided a generic method of constructing RRA-secure schemes in this condition by taking the value hashed by a Correlated-Input Secure (CIS) hash function proposed in [26] instead of a standard hash function as the randomness used in encryption process of a PKE scheme; then they considered the situation with no restriction on public keys where the adversary is restricted to use a vector of prefixed functions to implement its attack (FV-RRA) and gave a concrete FV-RRA secure scheme under chosen-plaintext attack under the DDH assumption where the used functions are hard-to-invert ones. To achieve FV-RRA security under chosen-ciphertext attack, Paterson *et al.* [27], presented a general transformation for PKE using a value extracted by an auxiliary input reconstructive extractor as randomness. Yuen *et al.* [28] proposed some related randomness attack models which cover related key/randomness attacks for PKE and digital signature, and provided generic constructions for security against these attacks. Schuldt and Shinagawa [29] analyzed the related-randomness security about RSA-OAEP and gave a positive result. A basic comparison between our schemes and two typical RRA secure schemes is shown in Table I.

TABLE 1. Comparison of schemes.

Scheme	CCA/ CPA	Arbitrary restricted function	Efficient Decryption
[25]	CCA	×	×
[28]	CCA	×	×
Our scheme I	CPA	√	√
Our scheme II	CPA	√	×
Our scheme III	CCA	√	×

B. OUR CONTRIBUTIONS

In consideration of the importance of resisting related randomness attacks in PKE scheme, we focus on how to build secure PKE schemes against related randomness attacks in this paper. Our contributions are summarized in the following:

(1) Propose a method of constructing RRA-CPA secure PKE scheme from indistinguishability obfuscation and weak RKA-secure one-way function. We first give a weak

definition of RKA-secure one-way function (wRKAOWF) and show how to construct weak RKA-secure one-way function. Then, we build related-seed secure pseudorandom generator using weak RKA-secure one-way function and a hardcore function for arbitrarily correlated inputs proposed in [30]. At last, we replace the standard pseudorandom generator used in the PKE scheme in [31] with a related-seed secure pseudorandom generator and prove the RRA-CPA security of the new scheme. The construction is simple, and has advantage in the efficiency in the decryption algorithm and ciphertexts size.

(2) Construct RRA-secure PKE schemes against arbitrary function.

- Prove that any publicly deniable encryption with *Indistinguishability under Chosen Plaintext Attack(IND-CPA)* and *Indistinguishability of Explanation* [31] is RRA-CPA secure PKE against arbitrary function.
- Propose a method of constructing a RRA-CCA secure PKE scheme by applying a hardcore function for arbitrarily correlated inputs proposed in [30] to a standard IND-CCA secure PKE scheme. To encrypt messages, the construction first apply the hardcore function to a randomness r to obtain the output r'. Then it implements the encryption algorithm of PKE scheme taking r' as the actual random coin for encryption. At last, we prove the RRA-CCA security of the construction.

C. ORGANIZATION

Section 2 reviews some preliminaries. Section 3 gives a method of constructing RRA-CPA secure PKE scheme from weak RKA-secure OWF. We define weak RKA-security of one-way function and a concrete instance of it. We construct a RRA-CPA secure PKE scheme from indistinguishability obfuscation and weak RKA-secure one-way function. In Section 4, we describe in detail how to construct PKE schemes with RRA-security against arbitrary function. We prove that any publicly deniable encryption is a RRA-CPA secure PKE against arbitrary function. To obtain RRA-CCA secure secure PKE against arbitrary function, we combine the standard IND-CCA PKE scheme with hardcore function for arbitrarily correlated inputs. Finally, conclusions are drawn in Section 5.

II. PRELIMINARIES

A. PUBLIC-KEY ENCRYPTION

Let PKE = (Keygen, Encrypt, Decrypt) be a PKE scheme (PKE) [32]. Keygen is used to generate a public/secret key pair (pk, sk) randomly. The probabilistic algorithm Encrypt uses pk and a randomly chosen coin r from randomness space **Rnd** to encrypt a message $m \in \mathcal{M}$ to its corresponding cipher text c. Using a private key sk, the deterministic algorithm Decrypt can return the corresponding plain text m or an error symbol $\perp$ by decrypting a cipher text c.

There are two classical security definitions for PKE, i.e., *Indistinguishability under Chosen Plaintext Attack*(*IND-CPA* in abbreviation) and *Indistinguishability under Chosen Ciphertext Attack*, (*IND-CCA* in abbreviation). Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a PPT adversary of a PKE scheme Π, and the advantage of $\mathcal{A}$ to break the security of Π is defined as follows:

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{IND-ATK}(\lambda) = \Pr\left[b = b' : \begin{array}{l} (sk, pk) \leftarrow KeyGen(1^\lambda); \\ (state, m_0, m_1) \\ \quad \leftarrow \mathcal{A}_1^{EO(pk,m),DO(sk,c)}(\cdot); \\ b \leftarrow_R \{0,1\}; \\ c^* \leftarrow LR(m_0, m_1); \\ b' \leftarrow \mathcal{A}_2^{EO(pk,m),DO(sk,c)}(pk, c^*, state) \end{array} \right] - \frac{1}{2}$$

1) IND-ATK SECURITY (ATK=CPA,CCA)

A PKE scheme is called IND-ATK secure if for any adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in λ.

The *related randomness security under Chosen Plaintext/Ciphertext Attack*(*RRA-CPA/RRA-CCA* for short) is two formal security definition introduced by [25] for PKE. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be a PPT adversary of a PKE scheme Π with a class of Φ of functions, and the advantage of $\mathcal{A}$ to break the related randomness security of Π is defined as follows:

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{\Phi-RRA-ATK}(\lambda) = \Pr\left[b = b' : \begin{array}{l} (sk, pk) \leftarrow KeyGen(1^\lambda); \\ CoinTable \leftarrow \emptyset; \\ (state, m_0, m_1) \\ \quad \leftarrow \mathcal{A}_1^{EO(pk,m,\phi),DO(sk,c)}(\cdot); \\ b \leftarrow_R \{0,1\}; \\ c^* \leftarrow LR(m_0, m_1, i, \phi); \\ b' \leftarrow \mathcal{A}_2^{EO(pk,m,\phi),DO(sk,c)}(pk, c^*, state) \end{array} \right] - \frac{1}{2}$$

EO(pk, m, ϕ) and LR(m_0, m_1, i, ϕ) are oracles proceed as follows in Table II:

TABLE 2. Encrypt and LR oracles in RRA-ATK security game.

EO(pk, m, ϕ):	LR(m_0, m_1, i, ϕ):
If CoinTable$[i]$=$\perp$	If CoinTable$[i]$=$\perp$
CoinTable$[i]$$\leftarrow_R$**Rnd**	CoinTable$[i]$$\leftarrow_R$**Rnd**
r_i $\leftarrow$CoinTable$[i]$	r_i $\leftarrow$CoinTable$[i]$
c $\leftarrow$PKE.Encrypt$(pk, m, \phi(r_i))$	c^* $\leftarrow$PKE.Encrypt$(pk, m_b, \phi(r_i))$
Return c	Return c^*

2) RRA-ATK SECURITY (ATK=CPA,CCA)

A PKE scheme is called RRA-ATK secure if for any adversary $\mathcal{A}$, the advantage of $\mathcal{A}$ is negligible in λ.

Note that *EO* is encrypt oracle and *DO* is decrypt oracle. The adversary's access to decrypt oracle *DO* is removed if ATK = CPA.

B. ONE-WAY FUNCTION

We use the description about one-way function in [33]. A function family $\mathbf{F}$ is *one-way* or called one-way function **OWF**, if the following advantage $\mathrm{Adv}^{ow}_{\mathbf{F},\mathcal{A}}(\lambda)$ for any probabilistic adversary $\mathcal{A}$ to break the one-wayness of $\mathbf{F}$ is a negligible function in λ.

$$\mathrm{Adv}^{ow}_{\mathbf{F},\mathcal{A}}(\lambda) = \Pr\left[\, x' : \begin{array}{l} k \leftarrow Key_F(1^\lambda) \\ y \leftarrow Eval_F(k,x) \\ x' \leftarrow \mathcal{A}(1^\lambda,k,y) \\ Eval_F(k,x') = y \end{array} \right]$$

C. INDISTINGUISHABILITY OBFUSCATION

Let $\{\mathcal{C}_\lambda\}$ be a circuit class. It is called an indistinguishability obfuscator for $\{\mathcal{C}_\lambda\}$ if an uniform PPT algorithm $i\mathcal{O}$ satisfies the following conditions:

- For all $\lambda \in \mathbb{N}$, all $\mathcal{C} \in \{\mathcal{C}_\lambda\}$ and all input x
  $\Pr[\mathcal{C}'(x) = \mathcal{C}(x) : \mathcal{C}' \leftarrow i\mathcal{O}(\lambda,\mathcal{C})] = 1.$
- For any PPT algorithm $\mathcal{A} = (\mathcal{A}_1,\mathcal{A}_2)$, if $\Pr[\forall x, \mathcal{C}_0 = \mathcal{C}_1 : (\mathcal{C}_0,\mathcal{C}_1,\sigma) \leftarrow \mathcal{A}_1(1^\lambda)] > 1-\epsilon(\lambda)$, then
  $|\Pr[\mathcal{A}_2(\sigma, i\mathcal{O}(\lambda,\mathcal{C}_0)) = 1 : (\mathcal{C}_0,\mathcal{C}_1,\sigma) \leftarrow \mathcal{A}_1(1^\lambda)] - \Pr[\mathcal{A}_2(\sigma, i\mathcal{O}(\lambda,\mathcal{C}_1)) = 1 : (\mathcal{C}_0,\mathcal{C}_1,\sigma) \leftarrow \mathcal{A}_1(1^\lambda)]| \le \epsilon(\lambda)$
  where $\epsilon(\lambda)$ is a negligible function.

The existences of this kind of $i\mathcal{O}$ for all polynomial size circuits were given in [34].

D. PUNCTURABLE PSEUDORANDOM FUNCTION

A puncturable family of PRFs $\mathbf{F}$ described in [31] can be defined by three algorithms Key_F,$Puncture_F$, and $Eval_F$, and two computable functions $n(\cdot)$ and $m(\cdot)$, which satisfy the following conditions:

-Functionality preserved under puncturing. The following equality is established for every PPT adversary $\mathcal{A}$ and for all $x \in \{0,1\}^{n(\lambda)}$, $x \notin S$ where $S \subseteq \{0,1\}^{n(\lambda)}$ is output by adversary $\mathcal{A}$:

$$\Pr\left[\begin{array}{ll} Eval_F(K,x) = : & K \leftarrow Key_F(1^\lambda) \\ Eval_F(K_S,x) & K_S \leftarrow Puncture_F(K,S) \end{array}\right] = 1$$

-Pseudorandom at punctured points. For a negligible function $negl(\cdot)$ and every PPT adversary $(\mathcal{A}_1,\mathcal{A}_2)$ such that $\mathcal{A}_1$ outputs a set $S \subseteq \{0,1\}^{n(\lambda)}$ and state σ, then:

$$\begin{aligned} |\Pr[\mathcal{A}_2(\sigma, K_S, S, Eval_F(K,S)) = 1] \\ - \Pr[\mathcal{A}_2(\sigma, K_S, S, U_{m(\lambda)\cdot|S|}) = 1]| = negl(\lambda) \end{aligned}$$

where $S = (x_1,\cdots,x_k)$, $K \leftarrow Key_F(1^\lambda)$, $K_S \leftarrow Puncture_F(K,S)$ and $Eval_F(K,S)$ denotes the concatenation of $Eval_F(K,x_1),\cdots,Eval_F(K,x_k)$, U_l denotes the uniform distribution over l bits.

E. HARDCORE FUNCTION FOR CORRELATED INPUTS

In [30], the authors constructed hardcore functions to extract random bits on the condition where the inputs are arbitrarily correlated. Let $\mathbf{HC}$ be a family of functions and $\mathbf{F}$ be a one-way function family. $\mathbf{HC}$ is hardcore function for $\mathbf{F}$ if the following advantage $\mathrm{Adv}^{\mathcal{H}}_{\mathbf{F},\mathbf{HC},\mathcal{I}}$ of an adversary $\mathcal{H}$ is negligible in λ.

$$\begin{aligned} &\mathrm{Adv}^{\mathcal{H}}_{\mathbf{F},\mathbf{HC},\mathcal{I}}(\lambda) \\ &= \Pr\left[\, b = b' : \begin{array}{l} b \leftarrow \{0,1\} \\ k \leftarrow Key_F(1^\lambda) \\ hp \leftarrow \mathbf{HC}.\mathbf{Pg}(1^\lambda) \\ \vec{y} \leftarrow Eval_F(k,\vec{x}) \\ \text{if } b = 1 \text{ then } \vec{r} \leftarrow \mathbf{HC}(hp,\vec{x}) \\ \text{else } \vec{r} \leftarrow \mathbf{Rnd}(\vec{x}, \mathbf{HC}.ol(1^\lambda)) \\ b' \leftarrow \mathcal{H}(1^\lambda,k,hp,\vec{y},\vec{r}) \end{array} \right] - \frac{1}{2} \end{aligned}$$

Here, we denote $\vec{y} \leftarrow Eval_F(k,\vec{x})$ as a vector of $y_i \leftarrow Eval_F(k,x_i)$ for each $x_i \in \vec{x}$. In [30], the authors gave a construction of hardcore function $\mathbf{HC}$ for *injective* one way functions $\mathbf{F}$ which can extract hardcore bits for arbitrarily correlated inputs.

III. RRA-SECURE PKE SCHEME FROM RKA-SECURE OWF

In [33], the authors proposed the definition of RKA-secure one-way function (RKAOWF) and applied it to construct RKA-secure signature schemes. However, their definition of RKAOWF is somewhat strong and cannot be used to construct RRA-secure PKE schemes. In this section, we will give a weak definition of RKAOWF and construct RRA-secure PKE schemes via it.

Firstly, we describe the definition of RKA-secure one-way function in [33] in the following. Let $\mathbf{F}$ be a function family. A class of polynomial-time computable functions Φ for $\mathbf{F}$ that specifies for each $\lambda \in \mathbb{N}$, each $k \in Key_F(1^\lambda)$ and each $\phi \in \Phi$ is called the related-key deriving (RKD) function.

Definition 1 (RKAOWF): $\mathbf{F}$ is called Φ-RKA secure if for any PPT adversary $\mathcal{A}$ for $\mathbf{F}$, the following advantage $\mathrm{Adv}^{\Phi-RKA}_{\mathbf{F},\mathcal{A}}(\lambda)$ is a negligible function in λ.

$$\mathrm{Adv}^{\Phi-RKA}_{\mathbf{F},\mathcal{A}}(\lambda) = \Pr\left[\, x' : \begin{array}{l} k \leftarrow Key_F(1^\lambda) \\ y \leftarrow Eval_F(k,x) \\ x' \leftarrow \mathcal{A}^{Eval}(1^\lambda,k,y) \\ Eval_F(k,x') = y \end{array} \right]$$

Eval(ϕ) is an oracle proceeds as follows:

$$\begin{array}{l} \mathrm{Eval}(\phi): \\ x' \leftarrow \phi(1^\lambda,k,x) \\ y' \leftarrow Eval_F(k,x') \\ return y' \end{array}$$

In the following, we give a weak definition of RKA-secure one-way function (wRKAOWF) which will be used to construct RRA-secure PKE schemes. Informally, wRKAOWF definition is as same as RKAOWF definition except that we weaken the adversary's advantage and let it return x' which satisfies that $Eval_F(k,x') = Eval_F(k,\Phi(1^\lambda,k,\phi,x))$.

Definition 2 (wRKAOWF): We say that $\mathbf{F}$ is Φ-wRKA secure if for any PPT adversary $\mathcal{A}$ for $\mathbf{F}$, the following advantage $\mathrm{Adv}_{\mathbf{F},\mathcal{A}}^{\Phi-wRKA}(\lambda)$ is a negligible function in λ.

$$\mathrm{Adv}_{\mathbf{F},\mathcal{A}}^{\Phi-wRKA}(\lambda) = \Pr\left[x' : \begin{array}{l} k \leftarrow Key_F(1^\lambda) \\ y \leftarrow Eval_F(k,x) \\ x' \leftarrow \mathcal{A}^{Eval}(1^\lambda, fp, y) \\ \mathbf{Eval_F}(1^\lambda, k, x') = \\ \qquad Eval_F(k, \phi(1^\lambda, k, x)) \end{array} \right]$$

A. CONSTRUCTION OF wRKAOWF

In [33], it is proved that a function family $\mathbf{F}$ is $\Phi-$RKA secure if $\mathbf{F}$ is $\Phi-$key-malleable and one-way, where Φ is a class of RKD functions and $\Phi-$key-malleable property is defined as follows:

$\Phi-$key-malleable property([33]). Let $\mathbf{F}$ be a function family and Φ be a class of RKD functions for $\mathbf{F}$. $\mathbf{F}$ is called $\Phi-$key-malleable if there is a polynomial-time algorithm T, such that $T(1^\lambda, k, \phi, Eval_F(k,x)) = Eval_F(k, \phi(1^\lambda, k, x))$ for all $\lambda \in \mathbb{N}$, all $k \in [Key_F(1^\lambda)]$, all $\phi \in \{0,1\}^*$ and all x.

In the following, we will prove that if $\mathbf{F}$ is Φ-RKA secure and Φ is *root samplable* then $\mathbf{F}$ is Φ-wRKA secure. Here, we define *root samplable* class of functions below:

Definition 3 (Root Samplable): A function ϕ is root samplable if there exists a polynomial-time algorithm **CompR** which can uniformly output an element from $\phi^{-1}(0)$. A class of RKD functions Φ is root samplable if for each $\phi \in \Phi$ and each constant c, $\phi' = \phi - c$ is root samplable.

Note that the classes of linear functions, affine functions and polynomial functions over Z_p are root samplable as for a d-degree polynomial function f over Z_p, Ben-Or's algorithm [35] can compute the root of $f(x)$ in Z_p using $O((\log p)d^{2+e})$ operations in Z_p [7].

Theorem 1: Let $\mathbf{F}$ be a function family and Φ be a class of RKD functions for $\mathbf{F}$. If $\mathbf{F}$ is Φ-RKA secure and Φ is *root samplable* then $\mathbf{F}$ is Φ-wRKA secure.

Proof: Let $\mathcal{A}$ be a $\Phi-$wRKA adversary of $\mathbf{F}$. We can construct a $\Phi-$RKA adversary $\mathcal{B}$ of $\mathbf{F}$. On input $(1^\lambda, k, y)$, adversary $\mathcal{B}$ runs $\mathcal{A}$ and responds to $\mathcal{A}$'s Eval query by sending the same query to its challenger and returning the corresponding result. When $\mathcal{A}$ stops and outputs a value x' satisfying that $Eval_F(k, x') = Eval_F(k, \phi(1^\lambda, k, x))$ for a RKD function ϕ, adversary $\mathcal{B}$ can return x'' satisfying that $Eval_F(k, x'') = y$ by sampling the root x'' of $\phi(1^\lambda, k, x) - x'$. Note: If the advantage of $\mathcal{A}$ is ϵ then $\mathcal{B}$'s advantage is $\epsilon/poly(1^\lambda)$. If we assume $\mathbf{F}$ is injective, i.e. $\mathbf{F}$ is a family of one-way permutations, then $\mathcal{B}$'s advantage is ϵ.

Instance: In [33], the authors give three instances of RKAOWF for different classes of RKD functions. The first one-way function (permutation) described in Table 3 is based on discrete exponentiation in a cyclic group of prime order p and is Φ-RKA secure for a class Φ of affine RKD functions. Therefore, it is also Φ-wRKA secure one-way function (permutation). Next, we can prove that this one-way function (permutation) is also Φ-wRKA secure for a class Φ of polynomial RKD functions with upper bound $d = d(\lambda)$ of the degrees of the polynomials in $\Phi \leq q$ as long as the $q-$SDL assumption described in the following holds.

TABLE 3. The instance.

k	x	$Eval_F(k,x)$	$\phi(1^\lambda, k, x)$
$(< G >, g, p)$	$\in Z_p^*$	g^x	$a_i \in Z_p, \sum_{i=0}^{d} a_i x^i \bmod p$

q-Strong Discrete Logarithm (q-SDL) Problem [33]. Let $\mathbb{G}$ be a cyclic group. Let $\mathcal{A}$ be an algorithm outputting previously unknown random value $x \in Z_p^*$ with advantage $\mathrm{Adv}_{\mathcal{A},q}^{SDL}$ given $(g, g^x, g^{x^2}, \cdots, g^{x^q}) \in \mathbb{G}^{q+1}$, where $g \in \mathbb{G}$ is a generator of group $\mathbb{G}$ and

$$\mathrm{Adv}_{\mathcal{A},q}^{SDL} = \Pr[\mathcal{A}(g, g^x, g^{x^2}, \cdots, g^{x^q}) = x]$$

Definition 4: The q-SDL assumption holds in $\mathbb{G}$ if for all PPT algorithm $\mathcal{A}$, the advantage $\mathrm{Adv}_{\mathcal{A},q}^{SDL}$ of $\mathcal{A}$ in solving the q-SDL problem in $\mathbb{G}$ is negligible.

Proof: Now, we continue the proof of Φ-wRKA security. Let $\mathcal{A}$ be a PPT adversary breaking Φ-RKA security with an advantage ϵ with respect to the class of non-zero polynomials over Z_p. An algorithm $\mathcal{B}$ that solves a given random instance of q-SDL problem with the same advantage ϵ by interacting with $\mathcal{A}$ can be built as follows.

Given a random instance $(g, g^x, g^{x^2}, \cdots, g^{x^q}) \in \mathbb{G}^{q+1}$ of the q-SDL problem in $\mathbb{G}$, where $x \in Z_p^*$ is a unknown random value, $\mathcal{B}$ can output x as follows. $\mathcal{B}$ invokes $\mathcal{A}$ and gives $y = g^x$ to $\mathcal{A}$. Then $\mathcal{B}$ responds to $\mathcal{A}$'s Eval(ϕ) query with $y' = Eval_F(k, \phi(1^\lambda, k, x)) = g^{\sum_{i=0}^{d} a_i x^i} = \prod_{i=0}^{d} (g^{x^i})^{a_i}$. Eventually, $\mathcal{B}$ returns the same output x' of $\mathcal{A}$.

Definition 5: Related-Seed Pseudorandom Generator. We say that a pseudorandom generator (PRG) is $\Phi-$related-seed secure if for all PPT distinguisher $\mathcal{D}$

$$|\Pr[\mathcal{D}(r) = 1] - \Pr[\mathcal{D}(PRG(\phi(seed)) = 1]| \leq \mathrm{negl}(\lambda)$$

where Φ is a class of RKD functions and $\phi \in \Phi$.

Construction of Related-Seed Pseudorandom Generator. Let $\mathbf{F}$ be a one-way permutation family and Φ be a class of RKD functions for $\mathbf{F}$, let **HC** be a hard-core predicate of $\mathbf{F}$. PRG=($Eval_F(k, seed)$,**HC**($seed$)) is proved to be a pseudorandom generator. Now, we can prove the following theorem.

Theorem 2: If **HC** is hardcore function for arbitrarily correlated inputs and $\mathbf{F}$ is Φ-wRKA secure, then the above PRG is $\Phi-$related-seed secure.

Proof: Let $\varepsilon(\lambda)$ be a non-negligible function. Assume that there exists a probabilistic polynomial-time distinguisher $\mathcal{D}$ such that

$$\varepsilon(\lambda) = \left| \Pr_{s \in \{0,1\}^\lambda} [\mathcal{D}(\mathbf{Eval_F}(k, \phi(s)), \mathbf{HC}(\phi(s))) = 1] \right.$$
$$\left. - \Pr_{r \in \{0,1\}^{n+1}} [\mathcal{D}(r) = 1] \right|$$

Note that

$$\Pr_{r \in \{0,1\}^{\lambda+1}} [\mathcal{D}(r) = 1]$$
$$= \Pr_{r \in \{0,1\}^\lambda, r' \in \{0,1\}} [\mathcal{D}(r, r') = 1]$$

$$
\begin{aligned}
&= \Pr_{s\in\{0,1\}^\lambda, r'\in\{0,1\}}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), r') = 1]\\
&= \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \mathbf{HC}(\phi(s))) = 1]\\
&\quad + \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \overline{\mathbf{HC}(\phi(s))}) = 1]
\end{aligned}
$$

Therefore,

$$
\begin{aligned}
\varepsilon(\lambda) = \frac{1}{2}\cdot \Big| &\Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \mathbf{HC}(\phi(s))) = 1]\\
&- \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \overline{\mathbf{HC}(\phi(s))}) = 1]\Big|.
\end{aligned}
$$

Then an algorithm $\mathcal{A}$ can be constructed based on $\mathcal{D}$ to guess $\mathbf{HC}(\phi(s))$ given $y = \mathbf{Eval_F}(k, \phi(s))$. Upon inputting $y = \mathbf{Eval_F}(k, \phi(s))$ for a random s, algorithm $\mathcal{A}$ works as follows:

1) Choose $r' \in \{0, 1\}$ uniformly.
2) Invoke $\mathcal{D}(y, r')$. If $\mathcal{D}$ returns 1, then output r'. Otherwise, output $\overline{r'}$.

We analyze the success probability of $\mathcal{A}$.

$$
\begin{aligned}
&\Pr_{s\in\{0,1\}^\lambda}[\mathcal{A}(\mathbf{Eval_F}(k,\phi(s))) = \mathbf{HC}(\phi(s))]\\
&= \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^\lambda}[\mathcal{A}(\mathbf{Eval_F}(k,\phi(s)))\\
&\qquad\qquad = \mathbf{HC}(\phi(s)) \mid r' = \mathbf{HC}(\phi(s))]\\
&\quad + \frac{1}{2}\cdot \Pr_{s\in\{0,1\}^\lambda}[\mathcal{A}(\mathbf{Eval_F}(k,\phi(s)))\\
&\qquad\qquad = \mathbf{HC}(\phi(s)) \mid r' \neq \mathbf{HC}(\phi(s))]\\
&= \frac{1}{2}\cdot \Big| \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \mathbf{HC}(\phi(s))) = 1]\\
&\quad + \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \overline{\mathbf{HC}(\phi(s))}) = 0]\Big|\\
&= \frac{1}{2}\cdot \Big| \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \mathbf{HC}(\phi(s))) = 1]\\
&\quad + (1 - \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \overline{\mathbf{HC}(\phi(s))}) = 1]\Big|)\\
&= \frac{1}{2} + \frac{1}{2}\cdot \Big| \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \mathbf{HC}(\phi(s))) = 1]\\
&\quad - \Pr_{s\in\{0,1\}^\lambda}[\mathcal{D}(\mathbf{Eval_F}(k,\phi(s)), \overline{\mathbf{HC}(\phi(s))}) = 1]\Big|\\
&= \frac{1}{2} + \varepsilon(\lambda).
\end{aligned}
$$

So $\mathcal{A}$ guesses $\mathbf{HC}(\phi(s))$ with probability $\frac{1}{2} + \varepsilon(\lambda)$. We get a contradiction to the assumption that $\mathbf{HC}$ is a hardcore function for arbitrarily correlated inputs since $\varepsilon(\lambda)$ is a non-negligible. We complete the proof.

B. RRA-CPA SECURE PKE SCHEMES VIA wRKAOWF

Our construction is the same as the PKE construction from indistinguishability obfuscation in [31]. We prove that if the PRG used in the construction is $\Phi-$related-seed secure, then the PKE scheme is RRA-CPA secure against a Φ-restricted adversary. Let PRG be a $\Phi-$related-seed secure pseudorandom generator that which takes a seed $r \in \{0, 1\}^\lambda$ and outputs a pseudorandom value $prv \in \{0, 1\}^{2\lambda}$. Let F be a puncturable PRF whose domain is $\{0, 1\}^{2\lambda}$ and range $\subseteq \{0, 1\}^l$. The construction is described as follows:

TABLE 4. PKE encrypt and PKE encrypt*.

PKE Encrypt:
Hardwired:Key of the punctured PRF, i.e., K.
Input parameters: Plaintext $m \in \{0,1\}^l$, random value $r \in \{0,1\}^\lambda$.
1. Compute $prv = PRG(r)$
2. Output $c = (c_1 = prv, c_2 = F(K, prv) \bigoplus m)$

PKE Encrypt*:
Hardwired:Key of the punctured PRF, i.e., $K(\{prv^*\})$.
Input parameters: Plaintext $m \in \{0,1\}^l$, random value $r \in \{0,1\}^\lambda$.
1. Compute $prv = PRG(r)$
2. Output $c = (c_1 = prv, c_2 = F(K, prv) \bigoplus m)$

- Setup(1^λ): Chooses a puncturable PRF key K for F as the secret key SK and obfuscates the program PKE Encrypt in Table IV. The public key, PK, is the obfuscated program. PKE Encrypt* in Table 4 is only used in the proof of security.
- Encrypt$(PK, m \in \mathcal{M})$: Runs the public key PK which is an obfuscated program taking as input a random coin $r \in \{0, 1\}^\lambda$ and the plaintext m.
- Decrypt$(SK, c = (c_1, c_2))$: Outputs $m' = F(K, c_1) \bigoplus c_2$.

Proof: In [31], the construction is proved IND-CPA secure by a sequence of hybrid games Hyb$_0$,Hyb$_1$,Hyb$_2$,Hyb$_3$. As we only change the pseudorandomness generator PRG in the construction of [31] to a $\Phi-$related-seed secure pseudorandomness generator, Φ-RRA-CPA security of the construction can be proved using the same technique while just modifying the first game Hyb$_0$ as follow:

- Hyb$_0$: This is the original RRA-CPA security game.
  1) $r^* \in \{0, 1\}^\lambda$ is chosen randomly and $prv^* = PRG(\phi(r^*))$.
  2) The key for the puncturable PRF is set to K.
  3) The obfuscated program PKE Encrypt is taken as the public key PK.
  4) The adversary receives PK and sends to the challenger $m_0, m_1 \in \{0, 1\}^l$.
  5) The challenger outputs the challenge ciphertext $c^* = (c_1^* = prv^*, c_2^* = F(K, prv^*) \bigoplus m_b)$ by randomly choosing $b \in \{0, 1\}$.

The description of Hyb$_1$,Hyb$_2$,Hyb$_3$ is straightly same as that in [31].

- Hyb$_1$: this game only changes the generation step of prv^* in Hyb$_0$ by choosing it randomly in $\{0, 1\}^{2\lambda}$.
- Hyb$_2$: this game only changes the public key generation step in Hyb$_1$. The public key in Hyb$_2$ is generated by obfuscating the program PKE Encrypt* in Table IV.
- Hyb$_3$: compared with Hyb$_2$, this game only changes the challenge ciphertext. A random z^* is chosen and the challenge ciphertext is formed as $(c_1^* = prv^*, c_2^* = z^*)$.

As PRG is $\Phi-$related-seed secure, we can prove Hyb$_0$ and Hyb$_1$ is indistinguishable. Also, the indistinguishability between Hyb_1 and Hyb_2, and the indistinguishability between Hyb_2 and Hyb_3 were proved in [11]. As the adversary has zero advantage in Hyb_3, we prove the Φ-RRA-CPA security of the construction.

TABLE 5. Performance.

g	p	x	speed
6703903964971298549787012499102923063739682910296196688861780721860882015036773488400937149083451713845015929093243025426876941405973284973216824503042048	7079874630119430796647323924133231840408588693993280009524913780184393787303995550949511996380726140939419197764786066126307402334847046986031896530667173	6982670607535038360833387703535522507947024988091051400140924913206856807470413382055160191591968239180861084026505352080342750354783520080778291923285934	0.698 ms (512 bit)
89884656743115795386465259539451236680898848947115328636715040578866337902750481566354238661203768010560056939935696678829394884407208311246423715319737062188883946712432742638151109800623047059726541476042502884419075341171231440736956555270413618581675255342293149119973622969239858152417678164812112068608	134732397759107784689547260867646234257252180822914674575875491714870709977355190117010489662127418648579900338567452222656052952584830279506967803666112459696839766572438777953486722322262059813718790783868093392596888465804646398431124100283967775767819468754497256028085548213521126993418605046877126964667	121594364640372747565780456154997162661273709810450362528453863680960541328117148136127537244600327400384328368328609113881721678691383336164017611987232508853677716851678869807341259065510667841621708567686177092954328255002428765548895876091899789886529779168836838070988584881670620069952881962782816915523	3.789 ms (1024 bit)
16158503035655503650357438344334975980222051334857742016065172713762327569433945446598600705761456731844358980460949009747059779575245460547544076193224141560315438683650498045875098875194826053398028819192033784138396109321309878080919047169238085235290822926018152521443787945770532904303776199561965192760957166694834171210342487393282284747428088017663161029038902829665513096354230157075129296432088558362971801859230928678799175576150822952201848806616643615613562842355410104862578550863465661734839271290328348967522998634176499319107762583194718667771801067716614802322659239302476074096777926805529798115328	29936105704876906552575622808675964757141216883777136759978311851108670985236963533348126016307483887596365139075056600043945255756053123703252961521994442337893845311743070302256297301920426724946769821242298138616832378686893705202892914666501782685806731174944802565075945285771486333907975294272267962579209808253096500028288988132283410012477979923354483923476889006389238447893042740254652523887787853330049389862841577815236961068531734823387170584395363280850834786585486338426303432484316194003879642020289166238489755756760081607731753198791246792794028461264987827838462081428843152732265289283371721985653	26689959531476972010578858862771629243060212857156992030321513407437022789051158952094954396841674360054270083801202755385656690075649072368458932652868811466884173619339090900627315931884652637038947625430082191813552982093683348639341341408122426751723817523982796465585538781163944670610944510761819745285552146715638627307369645714314323478105051356520169022625384025467051942164676312318937355964416961692248628016482161280767436528462332755298015237492194387891985879454019622547345432177122418318016759493069898336368487897279519521999275218838946691301488596581476250185041809575339658860098987646735704173838	24.14 ms (2048 bit)

C. PERFORMANCE

We will give some concrete performance results for the above scheme. As the encryption algorithm has to execute an obfuscated program, we must admit its inefficiency in real life. Therefore, we only show the efficiency of the decryption algorithm of our scheme. We use Python to generate three groups with their generator g and order p in the length of 512/1024/2048 bits and formalize one-way functions $\mathbf{F}$ respectively. To evaluate the somewhat worst-case performance, we generate keys for these $\mathbf{F}$s in the same bit length as its respective order p. The following Table 5 gives the results, where the decryption speed is tested on a personal computer with Intel(R) Core(TM) i7-8550 CPU @ 1.80GHz, 8GB RAM and Windows 10 operating system.

IV. RRA-SECURE PKE SCHEME AGAINST ARBITRARY FUNCTION

A. CONSTRUCTION FROM PUBLICLY DENIABLE ENCRYPTION

The first construction comes from the publicly deniable encryption. We will prove that any publicly deniable encryption scheme is RRA-secure PKE scheme against arbitrary function. Publicly deniable encryption is formally proposed by [31] as follows:

Definition 6: (Publicly Deniable Encryption). Let PDE Π = (Setup, Encrypt, Decrypt, Explain) be a publicly deniable encryption scheme.

- Setup(1^λ): it is a randomized algorithm which outputs a public/secret key pair (pk,sk) taking as input a security parameter λ.
- Encrypt($pk, m; u$): it is a probabilistic algorithm which uses a public key pk and random coins u to encrypt a plaintext m to its corresponding ciphertext c.
- Decrypt(sk, c): it is a deterministic algorithm which can obtain the corresponding plaintext m or error symbol $\perp$ by decrypting a ciphertext c using a secret key sk.
- Explain($pk, c, m; r$): it can output a randomness e which is with the same size as the random coin u used in Encrypt above given a public key pk, a ciphertext c, and a plaintext m.

In [31], two security requirements for publicly deniable encryption called *Indistinguishability under Chosen Plaintext Attack* (IND-CPA) and *Indistinguishability of Explanation* are presented as follows:

Indistinguishability under Chosen Plaintext Attack. For any probabilistic polynomial-time adversary of a publicly deniable encryption PDE Π, $\mathcal{A}$, the following advantage $\mathrm{Adv}_{\Pi,\mathcal{A}}^{IND-CPA}(\lambda)$ is a negligible function in n.

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{IND-CPA}(\lambda)$$

$$= \Pr\left[b = b' \ : \begin{array}{l} (sk, pk) \leftarrow Setup(1^\lambda); \\ (m_0, m_1) \leftarrow \mathcal{A}; \\ b \leftarrow_R \{0, 1\}; \\ c^* \leftarrow Encrypt(pk, m_b; u); \\ b' \leftarrow \mathcal{A}(c^*) \end{array} \right] - \frac{1}{2}$$

TABLE 6. Enc and LR oracles in game$_1$.

EO(pk, m, ϕ):	LR(m_0, m_1, i, ϕ):
If CoinTable[i]=$\perp$	If CoinTable[i]=$\perp$
CoinTable[i]$\leftarrow_R$**Rnd**	CoinTable[i]$\leftarrow_R$**Rnd**
$r_i \leftarrow$CoinTable[i]	$r_i \leftarrow$CoinTable[i]
$c \leftarrow$PKE.Encrypt($pk, m, \phi(r_i)$)	$c^* \leftarrow$PKE.Encrypt($pk^*, m_b, \phi(r_i)$)
$r' =$PKE.Explain($pk, c, m; u$)	$r^{'} =$PKE.Explain($pk^*, c, m; u$)
$c' =$PKE.Encrypt($pk, m, r^{'}$)	$c'^* =$PKE.Encrypt($pk^*, m, r^{'}$)
Return c'	Return c'^*

Indistinguishability of Explanation. For any probabilistic polynomial-time adversary of a publicly deniable encryption PDE Π, $\mathcal{A}$, the following advantage $\mathrm{Adv}_{\Pi,\mathcal{A}}^{IND-EXP}(\lambda)$ is a negligible function in n.

$$\mathrm{Adv}_{\Pi,\mathcal{A}}^{IND-EXP}(\lambda) = \Pr\left[b = b' : \begin{array}{l} (sk, pk) \leftarrow Setup(1^{\lambda}); \\ m \leftarrow \mathcal{A}; \\ c^* \leftarrow Encrypt(pk, m; u_0); \\ u_1 = Explain(pk, c, m; r); \\ b \leftarrow_R \{0, 1\}; \\ b' \leftarrow \mathcal{A}(c^*, u_b) \end{array} \right] - \frac{1}{2}$$

Theorem 3: If the publicly deniable encryption scheme satisfies *Indistinguishability under Chosen Plainext Attack* and *Indistinguishability of Explanation*, then this scheme is RRA-CPA secure against arbitrary function.

Proof: We can prove the above theorem via a sequence of games.

Game$_0$: This is the real RRA-CPA security game played by an adversary $\mathcal{A}$ against the publicly deniable encryption scheme.

Game$_1$: This game is the same as Game$_0$ except that we explain the ciphertext c and c^* to get a new randomness and return a new ciphertext obtained by encrypting the message using this new randomness. More precisely, in this game, the Enc and LR oracle are changed as follows in Table VI:

The *Indistinguishability of Explanation* of the publicly deniable encryption scheme guarantees that Game$_0$ and Game$_1$ are computationally indistinguishable.

Game$_2$: This game is the same as Game$_1$ except that r' in Enc and LR oracle is randomly selected from **Rnd**. Also, the *Indistinguishability of Explanation* of the publicly deniable encryption scheme guarantees that Game$_1$ and Game$_2$ are computationally indistinguishable.

In Game$_2$, the *Indistinguishability under Chosen Plainext Attack* of the publicly deniable encryption scheme guarantees that the adversary's advantage to break the security of the scheme is negligible. Therefore, we can prove the theorem as the advantage of the adversary in real RRA-CPA security game is negligible by the indistinguishability of all the games.

TABLE 7. Scheme HC-PKE based on a standard PKE scheme, PKE and a hardcore function for correlated inputs, HC.

Alg. HC-PKE.KeyGen(1^{λ}):	Alg. HC-PKE.Encrypt(pk, m):
(pk, sk) $\leftarrow$PKE.KeyGen(1^{λ})	$r \leftarrow$ **Rnd**
Alg. HC-PKE.Decrypt(sk, c):	$r' \leftarrow$HC(r)
$m \leftarrow$PKE.Decrypt(sk,c)	$c \leftarrow$PKE.Encrypt($pk, m; r'$)
return m	return c

TABLE 8. Enc and LR oracles in game$_0$.

EO(pk, m, ϕ):	LR(m_0, m_1, i, ϕ):
If CoinTable[i]=$\perp$	If CoinTable[i]=$\perp$
CoinTable[i]$\leftarrow_R$**Rnd**	CoinTable[i]$\leftarrow_R$**Rnd**
$r_i \leftarrow$CoinTable[i]	$r_i \leftarrow$CoinTable[i]
$r' = \mathbf{HC}(\phi(r_i))$	$r' = \mathbf{HC}(\phi(r_i))$
$c' \leftarrow$PKE.Encrypt($pk, m; r'$)	$c'^* \leftarrow$PKE.Encrypt($pk^*, m_b; r'$)
Return c'	Return c'^*

TABLE 9. EO and LR oracles in game$_1$.

Enc(pk, m, ϕ):	LR(m_0, m_1, i, ϕ):
If CoinTable[i]=$\perp$	If CoinTable[i]=$\perp$
CoinTable[i]$\leftarrow_R$**Rnd**	CoinTable[i]$\leftarrow_R$**Rnd**
$r_i \leftarrow$CoinTable[i]	$r_i \leftarrow$CoinTable[i]
$r' \leftarrow_R$**Rnd**	$r^{'} \leftarrow_R$**Rnd**
$c' =$PKE.Encrypt($pk, m; r'$)	$c'^* =$PKE.Encrypt($pk^*, m; r'$)
Return c'	Return c'^*

B. CONSTRUCTION FROM POLY-MANY HARDCORE BITS FOR ARBITRARILY CORRELATED INPUTS

The above construction is only secure under Chosen-Plainext-Attack. In the following, we will describe the construction of a RRA-CCA secure public-key encryption scheme. The construction combines a hardcore function for arbitrarily correlated inputs [30] with an IND-CCA secure PKE scheme. Specifically, the randomness r is used as an input to the hardcore function, the output from the hardcore function is then used as the actual randomness for encryption. Table 7 formalizes the construction, and we prove its security in the following theorem.

Theorem 4: If **HC** is hardcore function for arbitrarily correlated inputs, then the scheme in Table 7 is RRA-ATK secure against a Φ-restricted adversary where Φ is a class of arbitrary functions.

Proof: We can prove the above theorem via two games.

Game$_0$: This is the real RRA-ATK security game played by an adversary $\mathcal{A}$ against the scheme in Table VI. The Enc and LR oracles are shown in Table VIII.

Game$_1$: This game is the same as Game$_0$ except that r' in Enc and LR oracle is randomly selected from **Rnd** as in Table IX:

The hardcore function **HC** for arbitrarily correlated inputs guarantees that Game$_0$ and Game$_1$ are computationally indistinguishable.

In Game$_1$, the *IND-ATK* security of the public-key encryption scheme guarantees that the adversary's advantage to break the security of the scheme is negligible.

Therefore, we can prove the theorem as the advantage of the adversary in real RRA-ATK security game is negligible by the indistinguishability of all the games.

C. PERFORMANCE ANALYSIS

The two constructions are based on PDE and PKE schemes respectively. The first construction is as efficient as the based PDE scheme. The efficiency of the second construction relies on the based PKE scheme and the hardcore function, and the execution time is the total time of both of them.

V. CONCLUSION

In this paper, we give some methods of constructing a secure PKE scheme against related randomness attacks. We propose a RRA-CPA secure PKE scheme with an efficient decryption algorithm and short ciphertexts size. To obtain RRA-secure PKE scheme against arbitrary function, we first prove that any publicly deniable encryption scheme is a RRA-CPA secure public-key encryption scheme against arbitrary function. Then we combine standard IND-CCA PKE scheme with hardcore function for arbitrarily correlated inputs to get a RRA-CCA secure public-key encryption scheme against arbitrary function. In terms of efficiency, the encryption algorithm of our first proposed scheme is inefficient, while the decryption algorithm of it is very efficient. Our first scheme secure against arbitrary function is actually a publicly deniable encryption scheme so that it is inefficient at present, as the known publicly deniable encryption schemes are constructed based on indistinguishability obfuscation which is not practical at this stage. We have to admit that use of indistinguishability obfuscation in the first two schemes of our work makes the methods only with theoretical significance. Their practical significance depends on the development of indistinguishability obfuscation in efficiency. Compared with it, the efficiency of our second scheme secure against any arbitrary function depends on the PKE scheme and hardcore function it is based on which is acceptable. In the future, we will measure the performance of our proposed methods via the cloud-edge platform and study how to construct other cryptographic primitives with RRA-Security such as IBE, ABE, and so on.

REFERENCES

[1] L. Qi, X. Zhang, W. Dou, and Q. Ni, "A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 11, pp. 2616–2624, Nov. 2017.

[2] Y. Xu, L. Qi, W. Dou, and J. Yu, "Privacy-preserving and scalable service recommendation based on SimHash in a distributed cloud environment," *Complexity*, vol. 2017, pp. 1–9, 2017.

[3] C. Yan, X. Cui, L. Qi, X. Xu, and X. Zhang, "Privacy-aware data publishing and integration for collaborative service recommendation," *IEEE Access*, vol. 6, pp. 43021–43028, 2018.

[4] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, "Ensuring security and privacy preservation for cloud data services," *ACM Comput. Surv.*, vol. 49, no. 1, pp. 1–39, Jun. 2016.

[5] Y. Wang, M. Zhao, Y. Hu, Y. Gao, and X. Cui, "Secure computation protocols under asymmetric scenarios in enterprise information system," *Enterprise Inf. Syst.*, pp. 1–21, Mar. 2019, doi: 10.1080/17517575.2019.1597387.

[6] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[7] X. Wang, L. T. Yang, X. Xie, J. Jin, and M. J. Deen, "A cloud-edge computing framework for cyber-physical-social services," *IEEE Commun. Mag.*, vol. 55, no. 11, pp. 80–85, Nov. 2017.

[8] P. Hu, S. Dhelim, H. Ning, and T. Qiu, "Survey on fog computing: Architecture, key technologies, applications and open issues," *J. Netw. Comput. Appl.*, vol. 98, pp. 27–42, Nov. 2017.

[9] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile edge computing: A survey," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 450–465, Feb. 2018.

[10] L. T. Yang, X. Wang, X. Chen, L. Wang, R. Ranjan, X. Chen, and M. J. Deen, "A multi-order distributed HOSVD with its incremental computing for big services in cyber-physical-social systems," *IEEE Trans. Big Data*, to be published, doi: 10.1109/tbdata.2018.2824303.

[11] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment," *Future Gener. Comput. Syst.*, vol. 88, pp. 636–643, Nov. 2018.

[12] W. Gong, L. Qi, and Y. Xu, "Privacy-aware multidimensional mobile service quality prediction and recommendation in distributed fog environment," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–8, 2018.

[13] L. Qi, R. Wang, C. Hu, S. Li, Q. He, and X. Xu, "Time-aware distributed service recommendation with privacy-preservation," *Inf. Sci.*, vol. 480, pp. 354–364, Apr. 2019.

[14] X. Wang, L. T. Yang, L. Kuang, X. Liu, Q. Zhang, and M. J. Deen, "A tensor-based big-data-driven routing recommendation approach for heterogeneous networks," *IEEE Netw.*, vol. 33, no. 1, pp. 64–69, Jan. 2019.

[15] L. Qi, X. Zhang, S. Li, S. Wan, Y. Wen, and W. Gong, "Spatial-temporal data-driven service recommendation with privacy-preservation," *Inf. Sci.*, vol. 515, pp. 91–102, Apr. 2020.

[16] Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge computing security: State of the art and challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019.

[17] X. Wang, L. T. Yang, H. Li, M. Lin, J. Han, and B. O. Apduhan, "NQA: A nested anti-collision algorithm for RFID systems," *ACM Trans. Embed. Comput. Syst.*, vol. 18, no. 4, pp. 1–21, Jul. 2019.

[18] Y. Dodis, D. Pointcheval, S. Ruhault, D. Vergniaud, and D. Wichs, "Security analysis of pseudo-random number generators with input: /Dev/random is not robust," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Berlin, Germany, 2013, pp. 647–658.

[19] L. Dorrendorf, Z. Gutterman, and B. Pinkas, "Cryptanalysis of the windows random number generator," in *Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS)*, Alexandria, VA, USA, 2007, pp. 476–485.

[20] K. Michaelis, C. Meyer, and J. Schwenk, "Randomly failed! The state of randomness in current java implementations," in *Proc. CT-RSA*, San Francisco, CA, USA, 2013, pp. 129–144.

[21] Y. Wang, A. Bracciali, T. Li, F. Li, X. Cui, and M. Zhao, "Randomness invalidates criminal smart contracts," *Inf. Sci.*, vol. 477, pp. 291–301, Mar. 2019.

[22] T. Ristenpart and S. Yilek, "When good randomness Goes bad: Virtual machine reset vulnerabilities and hedging deployed cryptograph," in *Proc. NDSS*, San Diego, CA, USA, 2010, pp. 1–18.

[23] P. Austrin, K.-M. Chung, M. Mahmoody, R. Pass, and K. Seth, "On the impossibility of cryptography with tamperable randomness," *Algorithmica*, vol. 79, no. 4, pp. 1052–1101, Dec. 2017.

[24] M. Feltz and C. Cremers, "Strengthening the security of authenticated key exchange against bad randomness," *Des., Codes Cryptogr.*, vol. 86, no. 3, pp. 481–516, Mar. 2018.

[25] K. G. Paterson, J. C. N. Schuldt, and D. L. Sibborn, "Related randomness attacks for public key encryption," in *Proc. PKC*, Buenos Aires, Argentina, 2014, pp. 465–482.

[26] V. Goyal, A. O'Neill, and V. Rao, "Correlated-input secure hash functions," in *Proc. TCC*, Providence, RI, USA, 2011, pp. 182–200.

[27] K. G. Paterson, J. C. N. Schuldt, D. L. Sibborn, and H. Wee, "Security against related randomness attacks via reconstructive extractors," in *Proc. IMACC*, Oxford, U.K., 2015, pp. 23–40.

[28] T. H. Yuen, C. Zhang, S. S. Chow, and S. M. Yiu, "Related randomness attacks for public key cryptosystems," in *Proc. 10th ACM Symp. Inf., Comput. Commun. Secur. (ASIA CCS)*, 2015, pp. 215–223.

[29] J. C. Schuldt and K. Shinagawa, "On the robustness of RSA-OAEP encryption and RSA-PSS signatures against (malicious) randomness failures," in *Proc. ACM Asia Conf. Comput. Commun. Secur. (ASIA CCS)*, Abu Dhabi, UAE, 2017, pp. 241–252.

[30] M. Bellare, I. Stepanovs, and S. Tessaro, "Poly-many hardcore bits for any one-way function and a framework for differing-inputs obfuscation," in *Proc. ASIACRYPT*, Kaohsiung, Taiwan, 2014, pp. 102–121.

[31] A. Sahai and B. Waters, "How to use indistinguishability obfuscation: Deniable encryption, and more," in *Proc. 46th Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2014, pp. 475–484.

[32] M. Naor and M. Yung, "Public-key cryptosystems provably secure against chosen ciphertext attacks," in *Proc. 32nd Annu. ACM Symp. Theory Comput. (STOC)*, Baltimore, MD, USA, 1990, pp. 427–437.

[33] M. Bellare, S. Meiklejohn, and S. Thomson, "Key-versatile signatures and applications: RKA, KDM and joint enc/sig," in *Proc. EUROCRYPT*, Copenhagen, Denmark, 2014, pp. 496–513.

[34] S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters, "Candidate indistinguishability obfuscation and functional encryption for all circuits," in *Proc. FOCS*, Berkeley, CA, USA, 2013, pp. 40–49.

[35] M. Ben-Or, "Probabilistic algorithms in finite fields," in *Proc. FOCS*, Nashville, TN, USA, 1981, pp. 394–398.

PENGTAO LIU received the master's degree in computer software and theory from Shandong University. She is currently with the College of Cybersecurity, Shandong University of Political Science and Law. Her main research interests include public key encryption and digital signature.