Related Key Secure PKE from Hash Proof Systems *

Dingding Jia[1], Bao Li[1], Xianhui Lu[1], and Qixiang Mei[2]

[1] Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
[2] College of Information, Guangdong Ocean University
{ddjia,lb,xhlu}@is.ac.cn,nupf@163.com

Abstract. In this paper we propose a framework for constructing public key encryption against related key attacks from hash proof systems in the standard model. Compared with the construction of Wee (PKC2012), our framework avoids the use of one-time signatures. We show that the schemes presented by Jia *et al.* (ProvSec2013) could fit into our framework. And we give more instantiations of the proposed framework based on the QR and DCR assumptions for affine key related functions.

Key words: related key attack, 4-wise independent hash, subset membership problem, hash proof system

1 Introduction

Related key attack (RKA)[9, 7] means that the attacker can modify keys stored in the memory and observe the outcome of the cryptographic primitive under the modified keys. It demonstrates a realistic attack that given physical access to a hardware device, an adversary can use fault injection techniques to tamper with and induce modifications to the internal state of the device [9, 7]. RKA security has been studied for a long time in block ciphers [6, 21] and attracts interests in other areas in recent years, like identity based encryptions (IBE), public key encryptions (PKE), signatures, etc. [2, 5].

Specifically, PKE schemes against chosen ciphertext RKA (CC-RKA) is formulated by Bellare *et al.* [2]. In a CC-RKA game for PKE, the adversary can make decryption queries with a function and a ciphertext. On receiving the query, the challenger first applies the function to the secret key and gets a modified key, then it uses the modified key to decrypt the ciphertext and return the message to the adversary.

Bellare and Cash [1] built RKA secure pseudorandom functions (PRF) from key homomorphic PRF and finger-printing under the DDH and DLIN assumptions. Bellare *et al.* [5] built RKA secure IBE from IBE that was key homomorphic and supported collision resistant identity renaming. Bellare *et al.* [2] showed that CC-RKA secure PKE could be achieved from RKA secure PRF and RKA secure IBE separately. Wee [25] proposed a framework for constructing CC-RKA secure PKE from adaptive trapdoor relations that were key homomorphic and finger-printing. These works have some design ideas in common: the key homomorphism property assures RKA queries can be answered as long as queries involving with the normal key can be answered; the finger-printing

* This work is Supported by the National Basic Research Program of China (973 project)(No.2013CB338002), the National Nature Science Foundation of China (No.61070171, No.61272534).

property, similar to collision resistant identity renaming in IBE, assures that a ciphertext is valid for a unique secret key (identity).

However, Wee [25] gave an RKA attack on the DDH based scheme given by Cramer and Shoup [10], and pointed out that the the Cramer-Shoup CCA secure constructions [12, 11] could not achieve finger-printing, since the smoothness requirement in hash proof systems (HPSs) essentially stipulates that the secret key has some residual entropy given only its evaluation on a NO instance of the underlying subset membership problem, thus they achieved the CC-RKA security through "all-but-one" proof technique. Subsequently, Jia *et al.* [18] presented CC-RKA secure PKE schemes based on the DDH and HR assumptions, which seemed consistent with the paradigm of the HPS.

HPS, which is constructed from languages related to hard subset membership problems, is introduced by Cramer and Shoup [11] as an important primitive to build paradigm for CCA secure PKE schemes. After being proposed, several efforts have been made to improve the efficiency of the paradigm for CCA security, such as [20, 22, 16]. Researchers also proved the CCA security of a scheme by showing the scheme can fit into the corresponding paradigm [17]. Security proof for schemes through HPSs and "all-but-one" techniques are very different, thus we are interested in studying the CC-RKA security for schemes based on HPSs.

1.1 Our Contributions.

We give a generic PKE construction from the projective HPS, and prove that the construction is CC-RKA secure in the standard model when the HPS satisfies the key homomorphism and computational finger-printing properties. We show that schemes in [18] fit into this paradigm, and give other efficient instantiations based on the QR and DCR assumptions.

Technical Overview. Generally, in the CC-RKA security proof, the simulator should handle two more problems compared with the CCA security proof: firstly, how to answer decryption queries under the related functions of the secret key without revealing extra information about the secret key? secondly, how to prohibit the adversary from promoting a query out of the challenge ciphertext and the key related function?

In the HPS, decryption queries are easy to answer since the simulator holds the secret key. To make the adversary gain no more information about the secret key from the decryption answers than what it can get from the public key (except for a negligible probability), we require the HPS to satisfy the key homomorphism property analogous to that in previous works [5, 25]. Here key homomorphism means that there exists an efficient algorithm to compute the hash value of the input X under the modified key through the hash value of another input X' under the original secret key, where X' can be publicly computed. It assures that except for negligible probability, decryption answers are completely determined by the public key.

To prohibit the adversary from promoting a query out of the challenge ciphertext and key related functions, we consider the following two points: firstly, we hope that there is a unique secret key involving with a given ciphertext. However, as stated by Wee [25], it is impossible to fulfill the "finger-printing" property for the Cramer-Shoup framework, so we require a weaker notion called the computational finger-printing (CFP) property, which allows the existence of multi secret keys

that correspond to the same hash value for a random input, but no efficient algorithm can find two of them. Secondly, we hope that no adversary can get the same hash value by modifying the input and the secret key simultaneously. Although no existing HPSs can achieve this property, we note that when Kiltz *et al.* [20] realized the CCA secure paradigm from the HPS, they used an interesting primitive called 4-wise independent hash to extract randomness. For a randomly given 4-wise independent hash function $\mathcal{H}$ and two random variables $X, \tilde{X}$ with negligible collision probability, the output $\mathcal{H}(\tilde{X})$ is close to uniformly random even $\mathcal{H}(X)$ is fixed, as long as the min-entropy of X and $\tilde{X}$ are large enough. We prevent the malleability by extending the domain of 4-wise independent hash in [20], so that the output is randomly distributed when the input is changed.

Comparison with Previous Works. Following the original theory given by Bellare and Kohoo [3], modification on the secret key is parameterized by the class of Φ functions. Let S be the secret key space, if S is closed under one operation "+", Φ^{lin} is used to denote the class of linear functions; if S is closed under two operations "+" and "×", Φ^{affine} is used to denote the class of affine functions; $\Phi^{\text{poly}(d)}$ is used to denote the class of polynomial functions bounded by degree d similarly. The PRF given by Bellare and Cash [1] achieves RKA security for $\Phi = \Phi^{\text{lin}}$ under the DDH and DLIN assumptions. The IBE scheme given by Bellare, Paterson and Thomson [5] achieves RKA security for $\Phi = \Phi^{\text{poly}(d)}$ under the non-standard q-EBDDH assumption and $\Phi = \Phi^{\text{affine}}$ under the BDDH assumption.So one can get Φ-CC-RKA secure PKE for $\Phi = \Phi^{\text{lin}}$ under the DDH and DLIN assumptions by combining [2] and [1]; also one can get Φ-CC-RKA secure PKE for $\Phi = \Phi^{\text{poly}(d)}$ under the non-standard q-EBDDH assumption and $\Phi = \Phi^{\text{affine}}$ under the BDDH assumption by combining [2] and [5]. In Wee's instantiation of PKE schemes [25], they achieved Φ-CC-RKA secure for Φ being linear-shift under the factoring, BDDH and LWE assumptions. Our instantiations can achieve Φ-CC-RKA secure for Φ being affine functions under the DDH, HR, QR and DCR assumptions.

Note that compared with previous works, our construction removes the use of one-time signatures and has efficiency close to that of the CCA secure PKE construction in [20].

Related Works. Tamper resilience is also considered along with the leakage resilience security and there are schemes satisfying the corresponding security definitions [19, 13]. However, the scheme in [19] achieved the security via key update and could only encrypt one bit. In [13] Damgård *et al.* defined a security model that bounded the number of times that the adversary could make tampering queries.

Organization. The rest of our paper is organized as follows: in section 2 we give definitions and preliminaries; in section 3 we give our generic construction and security proof; in section 4 we show instantiations based on the DDH, QR and DCR assumptions; section 5 is the conclusion.

2 Definitions and Preliminaries

2.1 Notations

We use PPT as the abbreviation of probabilistic polynomial time. Let $l(X)$ denote the length of X. Let $s \leftarrow_R S$ denote choosing a random element s from S if S is a set, and assigning to s the output of S on uniformly chosen randomness if S is a PPT algorithm. Let X and Y be probability spaces on a finite set S, the statistical distance $SD(X,Y)$ between X and Y is defined as $SD(X,Y) := \frac{1}{2}\Sigma_{\alpha\in S}|\Pr_X[\alpha] - \Pr_Y[\alpha]|$, The min-entropy of a random variable X is defined as $H_\infty(X) = -\log_2(max_{x\in D}\Pr[X = x])$, wherein D is the domain of X. A function $f(n)$ is said negligible if for any polynomial $p(\cdot) > 0$, there exists an N such that for all $n > N, f(n) < \frac{1}{p(n)}$. A function $g(n)$ is said overwhelming if $1 - g(n)$ is negligible.

2.2 Security Definitions

Public Key Encryption. A public key encryption scheme consists of three polynomial time algorithms: $(Keygen, Enc, Dec)$. The key generation algorithm takes as input the public parameters and outputs a pair of keys $(pk, sk), Keygen(pp) \rightarrow_R (pk, sk)$; the encryption algorithm takes as input a message m, a public key pk and outputs a ciphertext C, $Enc(pk, m) \rightarrow_R C$; the decryption algorithm Dec takes as input the ciphertext C and a secret key sk and outputs a message m or $\perp, Dec(sk, C) = m$ or $\perp$. For correctness it is required that $Dec(sk, Enc(pk, m)) = m$.

Φ-CC-RKA Security. Here we give the security definition of Φ-CC-RKA. Let PKE= ($Keygen, Enc$, Dec) be a public key encryption scheme, the advantage of an adversary $\mathcal{A}$ in breaking the Φ-CC-RKA security of PKE is defined as:

$$Adv^{\Phi\text{-CC-RKA}}_{\mathcal{A},\text{PKE}} = \left|\Pr\left[b = b' : \begin{array}{l}(pk, sk) \leftarrow_R Keygen(pp); (m_0, m_1) \leftarrow \mathcal{A}^{\mathcal{O}(sk,\cdot,\cdot)}(pk);\\ b \leftarrow_R \{0,1\}; C^* \leftarrow_R Enc(pk, m_b); b' \leftarrow \mathcal{A}^{\mathcal{O}(sk,\cdot,\cdot)}(C^*, pk)\end{array}\right] - \frac{1}{2}\right|.$$

When the adversary issues queries (ϕ, C), where $\phi \in \Phi$, the oracle $\mathcal{O}(sk, \cdot, \cdot)$ responds with $Dec(\phi(sk), C)$. And after seeing the challenge ciphertext, the adversary is not allowed to make queries with $(\phi(sk), C) = (sk, C^*)$.

Definition 1 (Φ-CC-RKA Security). *A PKE scheme is Φ-CC-RKA secure if for any PPT adversary $\mathcal{A}$, $Adv^{\Phi\text{-}CC\text{-}RKA}_{\mathcal{A},PKE}$ is negligible in λ.*

Here our security definition follows the definition given by Bellare *et al.* [2].

Symmetric Encryption. A symmetric encryption scheme consists of two polynomial time algorithms: $(\mathcal{E}, \mathcal{D})$. Let $\mathcal{K}_{SE}$ be the secret key space. The encryption algorithm $\mathcal{E}$ takes as input a message m and a secret key K and outputs a ciphertext χ, $\mathcal{E}(K, m) = \chi$; the decryption algorithm $\mathcal{D}$ takes as input the ciphertext χ and a secret key K and outputs a message m or $\perp, \mathcal{D}(K, \chi) = m$ or $\perp$. Here both algorithms are deterministic. For correctness it is required that $\mathcal{D}(K, \mathcal{E}(K, m)) = m$.

Ciphertext Indistinguishability. Let $SE = (\mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme, the advantage of an adversary $\mathcal{A}$ in breaking the ciphertext indistinguishability (IND-OT) of SE is defined as:

$$Adv^{\text{IND-OT}}_{\mathcal{A},\text{SE}} = \left| \Pr \left[b = b' : \begin{array}{l} K^* \leftarrow_R \mathcal{K}_{SE}; (m_0, m_1) \leftarrow \mathcal{A}; b \leftarrow_R \{0,1\}; \\ \chi^* \leftarrow \mathcal{E}(K^*, m_b); b' \leftarrow \mathcal{A}(\chi^*) \end{array} \right] - \frac{1}{2} \right|.$$

We say that SE is one-time secure in the sense of indistinguishability (IND-OT) if for every PPT $\mathcal{A}$, $Adv^{\text{IND-OT}}_{\mathcal{A},\text{SE}}$ is negligible.

Ciphertext Integrity. Informally, ciphertext integrity requires that it is difficult to create a valid ciphertext corresponding to a uniformly chosen secret key for any PPT adversary $\mathcal{A}$, even $\mathcal{A}$ is given an encryption of a chosen message with the same key before. Let $SE = (\mathcal{E}, \mathcal{D})$ be a symmetric encryption scheme, the advantage of an adversary $\mathcal{A}$ in breaking the ciphertext integrity (INT-OT) of SE is defined as:

$$Adv^{\text{INT-OT}}_{\mathcal{A},\text{SE}} = \Pr \left[\chi \neq \chi^* \wedge \mathcal{D}(K^*, \chi) \neq \perp : \begin{array}{l} K^* \leftarrow_R \mathcal{K}_{SE}; m \leftarrow \mathcal{A}; \\ \chi^* \leftarrow \mathcal{E}(K^*, m); \chi \leftarrow \mathcal{A}(\chi^*) \end{array} \right].$$

We say that SE is one-time secure in the sense of integrity (INT-OT) if for every PPT $\mathcal{A}$, $Adv^{\text{INT-OT}}_{\mathcal{A},\text{SE}}$ is negligible.

Authenticated Encryption. A symmetric encryption scheme SE is secure in the sense of one-time authenticated encryption (AE-OT) iff it is IND-OT and INT-OT secure. An AE-OT secure symmetric encryption can be easily constructed using a one-time symmetric encryption and an existentially unforgeable MAC [12, 4].

2.3 Hash Proof Systems

Recall the concept of hash proof system (HPS) introduced by Cramer and Shoup [11]. Let $\mathcal{X}, \mathcal{Y}, \mathcal{SK}$, $\mathcal{PK}$ be sets and $\mathcal{L} \subset \mathcal{X}$ be a language, in which an instance $L \in \mathcal{L}$ can be efficiently sampled with a witness $r \in \mathcal{R}$. Let Λ be a family of hash functions indexed by $sk \in \mathcal{SK}$ mapping from $\mathcal{X}$ to $\mathcal{Y}$. Let μ be a PPT function mapping from $\mathcal{SK}$ to $\mathcal{PK}$. A hash proof system $\mathbf{H} = (\Lambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{R}, \mathcal{Y}, \mathcal{PK}, \mu)$ is projective if for all $sk \in \mathcal{SK}$, the action of Λ_{sk} on $\mathcal{L}$ is determined by $\mu(sk)$. That is, there are two PPT algorithms $(Priv, Pub)$ to compute $\Lambda_{sk}(L)$ for $L \in \mathcal{L}$ with witness r :

$$\Lambda_{sk}(L) = Priv(sk, L) = Pub(\mu(sk), L, r).$$

For $X \in \mathcal{X} \backslash \mathcal{L}$, it is required that there is still enough min-entropy for $\Lambda_{sk}(X)$ given $\mu(sk)$ and X.

Definition 2 (κ-entropic [20]). *The projective HPS is κ-entropic if for all $X \in \mathcal{X} \backslash \mathcal{L}$, $H_\infty(\Lambda_{sk}(X) | X, \mu(sk)) \geq \kappa$.*

We assume that there are efficient algorithms to sample $sk \in \mathcal{SK}$ and $X \in \mathcal{X}$ uniformly at random.

Definition 3 (Subset Membership (SM) Problem). *SM problem in the HPS* $\boldsymbol{H}$ *is to distinguish a randomly chosen* $Z_0 \in \mathcal{L}$ *from a randomly chosen* $Z_1 \in \mathcal{X} \backslash \mathcal{L}$*. Concretely, the advantage of an adversary* $\mathcal{A}$ *in breaking SM is defined as:*

$$Adv_{\mathcal{A}}^{SM} = \left|\Pr[\mathcal{A}(\mathcal{X}, \mathcal{L}, Z_1)] - \Pr[\mathcal{A}(\mathcal{X}, \mathcal{L}, Z_0)]\right|.$$

We say that the SM problem is hard if for every PPT $\mathcal{A}$*,* $Adv_{\mathcal{A}}^{SM}$ *is negligible.*

HPS with Trapdoor. Following [22, 20], we also require that the SM problem can be efficiently solved with a master trapdoor, which will be used not in the actual scheme but in the security proof. In fact, all known hash proof systems have such a trapdoor.

2.4 4-wise Independent Hash Functions

Here we review the primitive called 4-wise independent hash family [20] that can be used as a randomness extractor. A simple construction of 4-wise independent hash family is shown in [20].

Definition 4 (4-wise Independent Hash Family [20]). *Let* $\mathcal{HS}$ *be a family of hash functions* $\mathcal{H} : \mathcal{X} \to \mathcal{Y}$*. We say that* $\mathcal{HS}$ *is 4-wise independent if for any distinct* $x_1, x_2, x_3, x_4 \in \mathcal{X}$*, the output* $\mathcal{H}(x_1), ..., \mathcal{H}(x_4)$ *are uniformly and independently random, where* $\mathcal{H} \leftarrow_R \mathcal{HS}$*.*

The next two lemmata state that for a 4-wise independent hash function $\mathcal{H}$ and two random variables $X, \tilde{X}$ with $\Pr[X = \tilde{X}] = \delta$ negligible that even related, the random variable $(\mathcal{H}, \mathcal{H}(X))$ and $(\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X}))$ are close to uniformly random as long as the min-entropy of X and $\tilde{X}$ are large enough.

Lemma 1 (Leftover Hash Lemma [15]). *Let* $X \in \mathcal{X}$ *be a random variable where* $H_\infty(X) \geq \kappa$*. Let* $\mathcal{HS}$ *be a family of pairwise independent hash functions with domain* $\mathcal{X}$ *and range* $\{0,1\}^l$*. Then for* $\mathcal{H} \leftarrow_R \mathcal{HS}$ *and* $U_l \leftarrow_R \{0,1\}^l$*,*

$$SD((\mathcal{H}, \mathcal{H}(X)), (\mathcal{H}, U_l)) \leq 2^{(l-\kappa)/2}.$$

Lemma 2 (A Generalization of the Leftover Hash Lemma [20]). *Let* $(X, \tilde{X}) \in \mathcal{X} \times \mathcal{X}$ *be two random variables having joint distribution where* $H_\infty(X) \geq \kappa, H_\infty(\tilde{X}) \geq \kappa$ *and* $\Pr[X = \tilde{X}] = \delta$*. Let* $\mathcal{HS}$ *be a family of 4-wise independent hash functions with domain* $\mathcal{X}$ *and range* $\{0,1\}^l$*. Then for* $\mathcal{H} \leftarrow_R \mathcal{HS}$ *and* $U_{2l} \leftarrow_R \{0,1\}^{2l}$*,*

$$SD((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, U_{2l})) \leq \sqrt{1+\delta} \cdot 2^{l-\kappa/2} + \delta.$$

The following lemma from [18] that will be used in our security proof states that for a 4-wise independent hash function $\mathcal{H}$ and two random variables $X, \tilde{X}$ with $\Pr[X = \tilde{X}] = \delta$ negligible that even related, the output $\mathcal{H}(\tilde{X})$ is close to uniformly random even $\mathcal{H}(X)$ is fixed as long as the min-entropy of X and $\tilde{X}$ are large enough.

Lemma 3. *[18] Let $\delta \leq \frac{1}{2}, l \leq 6$, $(X, \tilde{X}) \in \mathcal{X} \times \mathcal{X}$ be two random variables having joint distribution where $\Pr[X = \tilde{X}] = \delta$ and $H_\infty(X) \geq \kappa, H_\infty(\tilde{X}) \geq \kappa$. Let $\mathcal{HS}$ be a family of 4-wise independent hash functions with domain $\mathcal{X}$ and range $\{0,1\}^l$. Then for $\mathcal{H} \leftarrow_R \mathcal{HS}$ and $U_l \leftarrow_R \{0,1\}^l$,*

$$SD((\mathcal{H}, \mathcal{H}(X), \mathcal{H}(\tilde{X})), (\mathcal{H}, \mathcal{H}(X), U_l)) \leq 2^{l - \frac{\kappa - 1}{2}} + \delta.$$

3 RKA Secure PKE from Hash Proof Systems

3.1 Computational Finger-Printing and Φ-key Homomorphism

In this section we begin by introducing two additional properties for the HPS to build RKA secure PKE. Generally speaking, computational finger-printing means that for any PPT adversary, for a randomly given X, it cannot compute two different secret keys that can get the same hash value of X. Φ-key homomorphism means that there exists an efficient algorithm T to compute the value $\Lambda_{\phi(sk)}(X)$ on input $\Lambda_{sk}(X')$ and X, where X' can be computed publicly, here we use the word "homomorphism" to indicate that the evaluation on $\phi(sk)$ can be transformed to the evaluation on sk.

Computational Finger-Printing (CFP). For a uniformly chosen $X \in \mathcal{X} \backslash \mathcal{L}$, the CFP problem is to compute $sk_1 \neq sk_2$, s.t. $\Lambda_{sk_1}(X) = \Lambda_{sk_2}(X)$. The advantage of $\mathcal{A}$ in solving the CFP problem is formally defined as

$$Adv_{\mathcal{A}}^{\text{CFP}} = \Pr[\Lambda_{sk_1}(X) = \Lambda_{sk_2}(X), sk_1 \neq sk_2 | X \leftarrow_R \mathcal{X} \backslash \mathcal{L}; (sk_1, sk_2) \leftarrow \mathcal{A}(X)].$$

Definition 5 (CFP). *We say that the CFP holds for an HPS if for all PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{CFP}$ is negligible in λ.*

We stipulate that "+" and "×" are two operations defined on the secret key space $\mathcal{SK}$ and $\mathcal{SK}$ is closed under "+" and "×" to define the affine functions on $\mathcal{SK}$.

Definition 6 (Φ-key Homomorphism). *We say an HPS is Φ-key homomorphic if there are PPT algorithms T_1, T_2 such that with overwhelming probability over pp, for all $\phi \in \Phi$, and all $sk, X \in \mathcal{X}$:*

$$\Lambda_{\phi(sk)}(X) = T_2(pp, \phi, \Lambda_{sk}(X'), X), \text{ where } X' = T_1(pp, pk, \phi, X).$$

3.2 The General Construction

In this part we give a general PKE construction from hash proof systems. The structure of our construction inherits that in [20]. By extending the domain of the 4-wise independent hash function to $\mathcal{X} \times \mathcal{Y}$, we can prove the Φ-CC-RKA security of the construction.

Let $\mathbf{H} = (\Lambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{R}, \mathcal{Y}, \mathcal{PK}, \mu)$ be a projective hash proof system with κ-entropic. Let SE be an AE-OT secure symmetric encryption scheme with secret key space $\{0,1\}^l$. Let $\mathcal{HS}$ be a family of 4-wise independent hash functions with domain $\mathcal{X} \times \mathcal{Y}$ and image $\{0,1\}^l$ and $\mathcal{H}$ is chosen uniformly random from $\mathcal{HS}$. Public parameters are set as $pp = (\mathbf{H}, \mathcal{H})$.

$Keygen(pp)$: The key generation algorithm chooses random secret key $sk \leftarrow_R \mathcal{SK}$ and computes the public key as $pk = \mu(sk)$.

$Enc(pk, m)$: The encryption algorithm samples random $L \in \mathcal{L}$ with witness r, the ciphertext $C = (C_0, C_1)$ is computed as:

$$C_0 = L, Y = Pub(pk, L, r), K = \mathcal{H}(C_0, Y), C_1 = \mathcal{E}(K, m).$$

$Dec(sk, C)$: The decryption algorithm computes the message as:

$$Y = Priv(sk, C_0), K = \mathcal{H}(C_0, Y), m = \mathcal{D}(K, C_1).$$

Correctness can be easily verified from the correctness of the symmetric encryption scheme and the projective property of the HPS. In terms of concrete security, it requires the entropy κ to be sufficiently large to assure the security of SE.

Remark. Compared with the paradigm in [20], we extend the domain of the 4-wise independent hash function to $\mathcal{X} \times \mathcal{Y}$, so that related key attacks such that $(C_0 \neq C_0^*, \Lambda_{\phi(sk)}(C_0) = \Lambda_{sk}(C_0^*))$ can be prevented.

3.3 Security Proof

Theorem 1. *If $\boldsymbol{H}$ is a projective HPS with the corresponding SM problem hard and satisfies the CFP and Φ-key homomorphism properties, SE is an AE-OT secure symmetric encryption scheme with secret key space $\{0,1\}^l$, $\mathcal{HS}$ is a family of 4-wise independent hash functions with domain $\mathcal{X} \times \mathcal{Y}$ and image $\{0,1\}^l$, then our PKE scheme is Φ-CC-RKA secure. In particular, for every CC-RKA adversary $\mathcal{A}$ against security of the above scheme, there exist adversaries $\mathcal{B}, \mathcal{C}, \mathcal{D}, \mathcal{F}$ with*

$$Adv^{\Phi\text{-}CC\text{-}RKA}_{\mathcal{A},PKE} \leq Adv^{SM}_{\mathcal{B}} + (q+1)2^{l-(\kappa-1)/2} + q(Adv^{CFP}_{\mathcal{C}} + Adv^{INT\text{-}OT}_{\mathcal{D},SE}) + Adv^{IND\text{-}OT}_{\mathcal{F},SE}$$

where $\kappa = H_\infty(Y)$.

First let us recall a lemma that will be used in our proof.

Lemma 4. *[12] Let S_1, S_2, S_0 be events defined on some probability space satisfying that event $S_1 \wedge \neg S_0$ occurs iff $S_2 \wedge \neg S_0$ occurs, then*

$$|\Pr[S_1] - \Pr[S_2]| \leq \Pr[S_0].$$

Proof (of Theorem 1). Suppose that the public key is pk and the secret key is sk. The challenge ciphertext is denoted by $C^* = (C_0^*, C_1^*)$. We also denote by r^*, Y^*, K^* the values corresponding with r, Y, K related to C^*. We say a ciphertext C is invalid if $C_0 \notin \mathcal{L}$. The master trapdoor mt is used to solve the SM problem.

To prove the security of our scheme, we define a sequence of games that any PPT adversary can not tell the difference between two adjacent games. Let q denote the number of decryption queries that the adversary makes during the whole game.

$Game_0$**:** the real security game.

$Game_1$**:** the same as $Game_0$ except that the challenge ciphertext is generated using the secret key. That is

$$Y^* = Priv(sk, C_0^*).$$

$Game_2$**:** the same as $Game_1$ except that the challenge ciphertext is invalid. That is, C_0^* is chosen uniformly from $\mathcal{X}\backslash\mathcal{L}$.

$Game_3$**:** the same as $Game_2$ except that the decryption oracle rejects all queries (ϕ, C) that satisfy $T_1(pp, pk, \phi, C_0) \notin \mathcal{L}$. This can be achieved with the help of the master trapdoor mt.

$Game_4$**:** the same as $Game_3$, except that SE encrypts m_b using a random key K^+ instead of K^*.

Let $Adv_{\mathcal{A}}^i$ denote $\mathcal{A}$'s advantage in $Game_i$ for $i = 0, 1, ..., 4$.

It is clear to see $Adv_{\mathcal{A}}^0 = Adv_{\mathcal{A}}^1$ from the projective property of HPS.

Lemma 5. *Suppose that there exists a PPT adversary $\mathcal{A}$ such that $Adv_{\mathcal{A}}^1 - Adv_{\mathcal{A}}^2 = \epsilon$, then there exists a PPT adversary $\mathcal{B}$ with advantage ϵ in solving the SM problem.*

Proof. $\mathcal{B}$ receives

$$D = (\mathcal{X}, \mathcal{L}, Z)$$

and its task is to decide whether $Z \in \mathcal{L}$. $\mathcal{B}$ picks a random $sk \in \mathcal{SK}$, computes $pk = \mu(sk)$ and sends pk to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits (ϕ, C), $\mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ randomly chooses $b \leftarrow_R \{0, 1\}$, it sets $C_0^* = Z, Y^* = Priv(sk, Z)$, $K^* = \mathcal{H}(C_0^*, Y^*), C_1^* = \mathcal{E}(K^*, m_b)$ and responds with $C^* = (C_0^*, C_1^*)$.

When $\mathcal{A}$ outputs b', $\mathcal{B}$ outputs 1 if $b' = b$ and 0 otherwise.

Note that when $Z \in \mathcal{L}$, then the above game perfectly simulates $Game_1$; when $Z \in \mathcal{X}\backslash\mathcal{L}$, the above game perfectly simulates $Game_2$. □

Lemma 6. *Suppose that there exists a PPT adversary $\mathcal{A}$ in $Game_2$ and $Game_3$ such that it can submit a query (C, ϕ) satisfying $C_0 = C_0^*$, $\phi(sk) \neq sk, Y = Y^*$ with probability δ, then there exists a PPT adversary $\mathcal{B}$ with advantage δ in breaking the CFP property.*

Proof. $\mathcal{B}$ receives X and its task is to compute $sk_1 \neq sk_2$ such that $\Lambda_{sk_1}(X) = \Lambda_{sk_2}(X)$. $\mathcal{B}$ chooses random $sk \in \mathcal{SK}$ and computes $pk = \mu(sk)$. Then $\mathcal{B}$ sends pk to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits $(\phi, C), \mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ randomly chooses $b \leftarrow_R \{0, 1\}$, it sets $C_0^* = X, Y^* = Priv(sk, X)$, $K^* = \mathcal{H}(C_0^*, Y^*), C_1^* = \mathcal{E}(K^*, m_b)$ and responds with $C^* = (C_0^*, C_1^*)$.

Whenever $\mathcal{A}$ submits (ϕ, C) satisfying $C_0 = C_0^*, \phi(sk) \neq sk, Y = Y^*$, which means $\Lambda_{sk}(X) = \Lambda_{\phi(sk)}(X)$. Thus $\mathcal{B}$ can solve the CFP problem with output $(sk, \phi(sk))$. □

Lemma 7. *Assume that the symmetric encryption scheme is AE-OT secure, $\mathcal{HS}$ is a family of 4-wise independent hash functions, the CFP assumption holds, then*

$$|Adv^2_{\mathcal{A}} - Adv^3_{\mathcal{A}}| \leq q(2^{l-(\kappa-1)/2} + Adv^{CFP}_{\mathcal{C}} + Adv^{INT\text{-}OT}_{\mathcal{D},SE}).$$

Proof. Let E be the event that a query (C, ϕ) is rejected in $Game_3$ but not rejected in $Game_2$. Then we have $|Adv^2_{\mathcal{A}} - Adv^3_{\mathcal{A}}| \leq Pr[E]$. Let Γ^* be the random variable (C_0^*, Y^*), Γ be the random variable (C_0, Y).

Case 1: $C_0 = C_0^*$.

- $\phi(sk) = sk$. According to the κ-entropic property, given pk and a random $C_0^* \in \mathcal{X}\backslash\mathcal{L}$, $H_\infty(\Lambda_{sk}(C_0^*)) = H_\infty(Y^*) \geq \kappa$, thus $H_\infty(\Gamma^*) \geq \kappa$, then we can get that $SD((\mathcal{H}, pk, \mathcal{H}(\Gamma^*)), (\mathcal{H}, pk, U_l)) \leq 2^{(l-\kappa)/2}$ from the leftover hash lemma. And according to the INT-OT property of the SE scheme, for a uniformly chosen $\bar{K} \in U_l$, given a valid symmetric ciphertext C_1^*, the probability that an adversary can generate a $C_1 \neq C_1^*$ s.t. $\mathcal{D}(\bar{K}, C_1) \neq \perp$ is bounded by $Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}}$, so in this case the adversary can produce a ciphertext s.t. $\mathcal{D}(K^*, C_1) \neq \perp$ with probability at most $Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}} + 2^{(l-\kappa)/2} < Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}} + 2^{l-(\kappa-1)/2}$.
- $\phi(sk) \neq sk$ and $C_0' = T_1(pp, pk, \phi, C_0) \notin \mathcal{L}$. From Lemma 6 it can be seen that $\Pr[Y = Y^*] = \delta$, hence $\Pr[\Gamma = \Gamma^*] = \delta$, where δ is negligible under the CFP assumption. We have $H_\infty(Y^*) \geq \kappa$, similarly, since $C_0' \notin \mathcal{L}$, according to the κ-entropic property, $H_\infty(\Lambda_{sk}(C_0')) \geq \kappa$, and Y is determined by C_0 and $\Lambda_{sk}(C_0')$, hence $H_\infty(Y) \geq \kappa$ and $H_\infty(\Gamma) \geq \kappa$. From Lemma 3 we know:

  $$SD((pk, \mathcal{H}, \mathcal{H}(\Gamma^*), \mathcal{H}(\Gamma)), (pk, \mathcal{H}, \mathcal{H}(\Gamma^*), U_l)) \leq 2^{l-(\kappa-1)/2} + \delta.$$

  And according to the INT-OT property of the SE scheme, for a uniformly chosen $\bar{K} \in U_l$, given a valid symmetric ciphertext C_1^*, the probability that an adversary can generate a $C_1 \neq C_1^*$ s.t. $\mathcal{D}(\bar{K}, C_1) \neq \perp$ is bounded by $Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}}$, so in this case the adversary can produce a ciphertext s.t. $\mathcal{D}(K, C_1) \neq \perp$ with probability at most $Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}} + Adv^{\text{CFP}}_{\mathcal{C}} + 2^{l-(\kappa-1)/2}$.

Case 2: $C_0 \neq C_0^*$, and $C_0' = T_1(pp, pk, \phi, C_0) \notin \mathcal{L}$. Since $C_0 \neq C_0^*$, $\Gamma \neq \Gamma^*$. And as discussed above we have $H_\infty(Y^*) \geq \kappa$. Since $C_0' \notin \mathcal{L}$, according to the κ-entropic property, $H_\infty(\Lambda_{sk}(C_0')) \geq \kappa$, and Y is determined by C_0 and $\Lambda_{sk}(C_0')$, hence $H_\infty(Y) \geq \kappa$ and $H_\infty(\Gamma) \geq \kappa$. From Lemma 3 we know:

$$SD((pk, \mathcal{H}, \mathcal{H}(\Gamma^*), \mathcal{H}(\Gamma)), (pk, \mathcal{H}, \mathcal{H}(\Gamma^*), U_l)) \leq 2^{l-(\kappa-1)/2}.$$

According to the INT-OT property of the SE scheme, for a uniformly chosen $\bar{K} \in U_l$, given a valid symmetric ciphertext C_1^*, the probability that an adversary can generate a $C_1 \neq C_1^*$ s.t. $\mathcal{D}(\bar{K}, C_1) \neq \perp$ is bounded by $Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}}$, so in this case the adversary can produce a ciphertext s.t. $\mathcal{D}(K, C_1) \neq \perp$ with probability at most $Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}} + 2^{l-(\kappa-1)/2}$.

From the above analysis, we can see that

$$|Adv^2_{\mathcal{A}} - Adv^3_{\mathcal{A}}| \leq q(2^{l-(\kappa-1)/2} + Adv^{\text{CFP}}_{\mathcal{C}} + Adv^{\text{INT-OT}}_{\mathcal{D},\text{SE}}).$$

□

Lemma 8. *Assume that $\mathcal{HS}$ is a family of 4-wise independent hash functions, then $|Adv^3_{\mathcal{A}} - Adv^4_{\mathcal{A}}| \leq 2^{(l-k)/2}$.*

Proof. Since in both $Game_3$ and $Game_4$, all decryption queries are rejected except those $(\phi, (C_0, C_1))$ satisfying $C'_0 \in \mathcal{L}$, and the value of $\Lambda_{\phi(sk)}(C_0) = T_2(pp, \phi, \Lambda_{sk}(C'_0), C_0)$ is completely determined by pk, ϕ and C_0, so $\Lambda_{\phi(sk)}(C_0)$ leaks no more information about sk than pk. As a result, conditioned on the decryption answers, it still holds that $H_\infty(Y^*) \geq \kappa$ and $H_\infty(\Gamma^*) \geq \kappa$. Then from the leftover hash lemma, $SD((\mathcal{H}, pk, \mathcal{H}(\Gamma^*)), (\mathcal{H}, pk, U_l)) \leq 2^{(l-\kappa)/2}$, so $|Adv^3_{\mathcal{A}} - Adv^4_{\mathcal{A}}| \leq 2^{(l-k)/2}$. □

Lemma 9. *Suppose that there exists a PPT adversary $\mathcal{A}$ such that $Adv^4_{\mathcal{A}} = \epsilon$, then there exists a PPT adversary $\mathcal{B}$ with the same advantage in breaking the IND-OT security of the SE scheme.*

Proof. $\mathcal{B}$ chooses random $sk \in \mathcal{SK}$, computes $pk = \mu(sk)$ and sends pk to $\mathcal{A}$.

Whenever $\mathcal{A}$ submits $(\phi, C), \mathcal{B}$ simply runs the decryption oracle with the secret key $\phi(sk)$.

When $\mathcal{A}$ submits $(m_0, m_1), \mathcal{B}$ sends (m_0, m_1) to its challenger and receives C^*_1. Then $\mathcal{B}$ chooses random $C^*_0 \in \mathcal{X} \backslash \mathcal{L}$ and responds with $C^* = (C^*_0, C^*_1)$.

When $\mathcal{A}$ outputs b', $\mathcal{B}$ outputs b'. □

4 Instantiations

In the following we give three instantiations from the DDH, QR and HR assumptions, wherein the one based on the DDH assumption is the same as that in [18], so our construction can be seen as a generalization and high level understanding of schemes in [18]. And the schemes based on the QR and DCR assumptions can be seen as applications of our general approach.

4.1 Instantiation from DDH

Decisional Diffie-Hellman Assumption (DDH). Let $\mathcal{G}$ denote a group generation algorithm, which takes in a security parameter λ and outputs a prime p and a group description G of order p.

Run $\mathcal{G}(1^\lambda)$ to get (p, G), and randomly choose $g_1, g_2 \in G, r \neq w \in \mathbb{Z}_p$. Set $Z_0 = (g_1^r, g_2^r), Z_1 = (g_1^r, g_2^w)$. The advantage of $\mathcal{A}$ is defined as

$$Adv^{DDH}_{\mathcal{A}} = \Big| \Pr[\mathcal{A}(g_1, g_2, Z_1) = 1] - \Pr[\mathcal{A}(g_1, g_2, Z_0) = 1] \Big|.$$

Definition 7 (DDH). *We say that $\mathcal{G}$ satisfies the DDH assumption if for any PPT algorithm $\mathcal{A}$, $Adv^{DDH}_{\mathcal{A}}$ is negligible in λ.*

We recall the projective HPS constructed by Cramer and Shoup [11], of which the corresponding subset membership problem is based on the DDH assumption. Run $\mathcal{G}(1^\lambda)$ to get (p, G), and let

g_1, g_2 be two independent generators. Here the master trapdoor is $w := log_{g_1} g_2$ Define $\mathcal{X} = G^2$ and $\mathcal{L} = \{(g_1^r, g_2^r) : r \in \mathbb{Z}_p\}$. The value r is a witness of $L \in \mathcal{L}$. Let $\mathcal{SK} = \mathbb{Z}_p^2, \mathcal{PK} = G$ and $\mathcal{Y} = G$. For $sk = (sk_1, sk_2) \in \mathbb{Z}_p^2$, define $\mu(sk) = pk = g_1^{sk_1} g_2^{sk_2}$. For $X = (X_1, X_2) \in \mathcal{X}$, define

$$\Lambda_{sk}(X) = X_1^{sk_1} X_2^{sk_2}. \tag{1}$$

Then given $pk = \mu(sk), L \in \mathcal{L}$ and a witness $r \in \mathbb{Z}_p$, the public evaluation algorithm $Pub(pk, L, r)$ can compute $Y = \Lambda_{sk}(L)$ as $Y = pk^r$. Correctness can be easily verified by the definition of μ and eq. (1).

As stated in [20], in the above HPS, $H_\infty(\Lambda_{sk}(X)|pk, X) = log_2(|G|)$ for $X \in \mathcal{X}\backslash\mathcal{L}$.

It is easy to see that the CFP holds under the DDH assumption. For an adversary $\mathcal{B}$ which receives $D = (g_1, g_2, \hat{g_1}, \hat{g_2})$ and its task is to decide whether D is a DDH tuple. $\mathcal{B}$ chooses random $r \neq w \in \mathbb{Z}_p$, computes $X_1 = g_1^r, X_2 = g_2^w$ and sends $X = (X_1, X_2)$ to $\mathcal{A}$. If $\mathcal{A}$ can output $sk \neq \hat{sk}$ and $\Lambda_{sk}(X) = \Lambda_{\hat{sk}}(X)$, that is, $g_1^{r sk_1} g_2^{w sk_2} = g_1^{r \hat{sk_1}} g_2^{w \hat{sk_2}}$, then one can compute a σ such that $g_2 = g_1^\sigma$, and hence decide whether D is a DDH tuple by checking whether the equation $\hat{g_2} = \hat{g_1}^\sigma$ holds.

Here we define $\phi_{a_1,a_2,b_1,b_2}(sk_1, sk_2) = (a_1 sk_1 + b_1, a_2 sk_2 + b_2)$ and $X' = T_1(pp, pk, \phi, X) = (X_1^{a_1}, X_2^{a_2})$, $T_2(pp, \phi, \Lambda_{sk}(X'), X) = \Lambda_{sk}(X') X_1^{b_1} X_2^{b_2} = X_1^{a_1 sk_1 + b_1} X_2^{a_2 sk_2 + b_2}$. The correctness can be easily verified.

$Keygen(pp)$	$Enc(pk, m)$	$Dec(sk, C)$
$pp = (\mathcal{H}, p, G, g_1, g_2)$	$r \leftarrow_R \mathbb{Z}_p^*; C_{01} = g_1^r, C_{02} = g_2^r$	Parse C as (C_{01}, C_{02}, C_1)
$sk_1, sk_2 \leftarrow_R \mathbb{Z}_p$	$K = \mathcal{H}(C_{01}, C_{02}, pk^r)$	$K = \mathcal{H}(C_{01}, C_{02}, C_{01}^{sk_1} C_{02}^{sk_2})$
$pk = g_1^{sk_1} g_2^{sk_2}$	$C_1 = \mathcal{E}(K, m)$	Return $\{m, \perp\} \leftarrow \mathcal{D}(K, C_1)$
Return (sk, pk)	Return $C = (C_{01}, C_{02}, C_1)$	

Fig.1. PKE scheme $\mathrm{HE}_1 = (Keygen, Enc, Dec)$ [18].

Instantiations from the HR assumption [23, 18] can be got similarly.

4.2 Instantiation from QR

Quadratic Residuosity Assumption (QR). Let RSA_{gen} denote an RSA generation algorithm, which takes in a security parameter λ and outputs (P, Q, N, g) such that $N = PQ, P = 2p+1, Q = 2q+1$ for primes P, Q, p, q. Let J_N denote the subgroup of elements in $\mathbb{Z}_N^*$ with Jacobi symbol 1, and let QR_N denote the unique (cyclic) subgroup of $\mathbb{Z}_N^*$ of order pq. Let g denote the generator of QR_N.

Generally speaking, QR assumption means that it is difficult to distinguish a random element in QR_N from a random element in $J_N\backslash QR_N$. To formulate this notion precisely, run $RSA_{gen}(1^\lambda)$ to get (P, Q, N, g), and randomly choose $u_0 \in QR_N,\ u_1 \in J_N\backslash QR_N$. Master trapdoor here is (P, Q). The advantage of $\mathcal{A}$ is defined as

$$Adv_{\mathcal{A}}^{QR} = \Big| \Pr[\mathcal{A}(g, u_1) = 1] - \Pr[\mathcal{A}(g, u_0) = 1] \Big|.$$

Definition 8 (QR). *We say that RSA_{gen} satisfies the QR assumption if for any PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{QR}$ is negligible in λ.*

We recall the projective HPS constructed by Cramer and Shoup [11, 20], of which the corresponding subset membership problem is based on the QR assumption. Run $RSA_{gen}(1^{\lambda})$ to get (P, Q, N, g). Define $\mathcal{X} = J_N$ and $\mathcal{L} = QR_N = \{g^r : r \in \mathbb{Z}_{pq}\}$. The value r is a witness of $L \in \mathcal{L}$. Let $\mathcal{SK} = \mathbb{Z}_{[N/2]}^k, \mathcal{PK} = QR_N^k$ and $\mathcal{Y} = J_N^k$. For $sk = (s_1, ..., s_k) \in \mathbb{Z}_{[N/2]}^k$, define $\mu(sk) = pk = (pk_1, ..., pk_k) = (g^{s_1}, ..., g^{s_k})$. For $X \in \mathcal{X}$, define

$$\Lambda_{sk}(X) = (X^{s_1}, ..., X^{s_k}). \tag{2}$$

Then given $pk = \mu(sk), L \in \mathcal{L}$ and a witness $r \in \mathbb{Z}_{[N/4]}$, the public evaluation algorithm $Pub(pk, L, r)$ can compute $Y = (Y_1, ..., Y_k) = (pk_1^r, ..., pk_k^r)$.

For $X \in \mathcal{X} \backslash \mathcal{L}, H_{\infty}((X^{s_1}, ..., X^{s_k})|pk, X) = k$.

The CFP can be easily deduced from the QR assumption similarly as the analysis in [8, 14]. For an adversary $\mathcal{B}$ which receives $D = (g, u)$ and its task is to decide whether $u \in QR_N$. $\mathcal{B}$ chooses random $r \in \mathbb{Z}_{[N/4]}$, computes $X = -g^r$ and sends X to $\mathcal{A}$. If $\mathcal{A}$ can output $sk \neq \hat{sk}$ which satisfy that $\Lambda_{sk}(X) = \Lambda_{\hat{sk}}(X)$. Then there must exists $s_i \neq \hat{s}_i$ such that $(-g^r)^{s_i} = (-g^r)^{\hat{s}_i}$ for some $1 \leq i \leq k$. Since with overwhelming probability g^r is a generator of QR_N, then with overwhelming probability $s_i = \hat{s}_i \mod pq$, so one can get the value of pq, hence factor N and decide whether $u \in QR_N$.

Here we define $\phi_{a_1,b_1,...,a_k,b_k}(sk) = (a_1 s_1 + b_1, ..., a_k s_k + b_k)$ and T_1 be the identity function, $T_2(pp, pk, \phi, Y, X) = (Y_1^{a_1} X_1^{b_1}, ..., Y_k^{a_k} X_k^{b_k})$. The correctness can be easily verified.

$Keygen(pp)$	$Enc(pk, m)$	$Dec(sk, C)$
$pp = (\mathcal{H}, P, Q, N, g)$	$r \leftarrow_R \mathbb{Z}_{[N/4]}; C_0 = g^r$	Parse C as (C_0, C_1)
for $i = 1$ to $4l$ do	$K = \mathcal{H}(C_0, pk_1^r, ..., pk_{4l}^r)$	$K = \mathcal{H}(C_0, C_0^{s_1}, ..., C_0^{s_{4l}})$
$s_i \leftarrow_R \mathbb{Z}_{[N/2]}; pk_i = g^{s_i}$	$C_1 = \mathcal{E}(K, m)$	
$pk = (pk_i), sk = (s_i)$	Return $C = (C_0, C_1)$	Return $\{m, \perp\} \leftarrow \mathcal{D}(K, C_1)$
Return (sk, pk)		

Fig.2. PKE scheme $\mathrm{HE}_2 = (Keygen, Enc, Dec)$. (Here we require $k = 4l$)

4.3 Instantiation from DCR

Decisional Composite Residuosity Assumption (DCR).[24] Let RSA_{gen} denote an RSA generation algorithm, which takes in a security parameter λ and outputs (P, Q, N) such that $N = PQ, P = 2p + 1, Q = 2q + 1$ for primes P, Q, p, q. Generally speaking, DCR assumption means that it is difficult to distinguish whether a randomly chosen element in $Z_{N^2}^*$ is an Nth power. To formulate this notion precisely, run $RSA_{gen}(1^{\lambda})$ to get (P, Q, N). Master trapdoor is (P, Q). The advantage of $\mathcal{A}$ is defined as

$$Adv_{\mathcal{A}}^{DCR} = \Big| \Pr[\mathcal{A}(N, r^N \bmod N^2) = 1] - \Pr[\mathcal{A}(N, r) = 1] \Big|.$$

Here r is chosen randomly from $\mathbb{Z}_{N^2}^*$.

Definition 9 (DCR). *We say that RSA_{gen} satisfies the DCR assumption if for all PPT algorithm $\mathcal{A}$, $Adv_{\mathcal{A}}^{DCR}$ is negligible in λ.*

We recall the projective HPS constructed by Cramer and Shoup [11], of which the corresponding subset membership problem is based on the DCR assumption. Run $RSA_{gen}(1^{\lambda})$ to get (P, Q, N). Define $\mathcal{X} = G_N \cdot G_{N'} \cdot I$, where G_τ is a cyclic group of order $\tau, N' = pq, I$ is the subgroup of $\mathbb{Z}_{N^2}^*$ generated by $(-1 \bmod N^2)$, $\mathcal{L} = G_{N'} \cdot I = \{g^r\}$, here r is the witness and $g = -\zeta^N$ can be seen as a random generator of $\mathcal{L}$, where $\zeta \leftarrow_R \mathbb{Z}_{N^2}^*$.

Let $\mathcal{SK} = \mathbb{Z}_{[N^2/2]}, \mathcal{PK} = G_{N'} \cdot I$ and $\mathcal{Y} = G_N \cdot G_{N'} \cdot I$. For $sk = s \in \mathbb{Z}_{[N^2/2]}$, define $\mu(sk) = pk = g^s$. For $X \in \mathcal{X}$, define

$$\Lambda_{sk}(X) = X^s. \tag{3}$$

Then given $pk = \mu(sk), L \in \mathcal{L}$ and a witness $r \in \mathbb{Z}_{[N/2]}$, the public evaluation algorithm $Pub(pk, L, r)$ can compute $Y = pk^r$.

For $X \in \mathcal{X} \backslash \mathcal{L}, H_\infty((X^s)|pk, X) = log_2(N)$.

The CFP can be easily deduced from the DCR assumption similarly as the analysis in [8, 14]. For an adversary $\mathcal{B}$ which receives $D = (N, u)$ and its task is to decide whether u is an Nth power. $\mathcal{B}$ chooses random $\zeta \in \mathbb{Z}_{N^2}^*, \alpha \in \mathbb{Z}_N^*, \beta \in \mathbb{Z}_{[N/4]}$, computes $X = -(1+N)^\alpha \zeta^{N\beta}$ and sends X to $\mathcal{A}$. If $\mathcal{A}$ can output $sk \neq \hat{sk}$ which satisfy that $\Lambda_{sk}(X) = \Lambda_{\hat{sk}}(X)$. Then there must be $(1+N)^{\alpha sk} = (1+N)^{\alpha \hat{sk}}$ and $(-\zeta^N)^{\beta sk} = (-\zeta^N)^{\beta \hat{sk}}$, then with overwhelming probability there is $sk = \hat{sk} \bmod pq$, thus $\mathcal{B}$ can factor N and solve the DCR problem.

Here we define $\phi_{a,b}(sk) = as + b$ and T_1 be the identity function, $T_2(pp, pk, \phi, Y, X) = Y^a X^b$. The correctness can be easily verified.

$Keygen(pp)$	$Enc(pk, m)$	$Dec(sk, C)$
$pp = (\mathcal{H}, P, Q, N, g)$	$r \leftarrow_R \mathbb{Z}_{[N/2]}; C_0 = g^r$	Parse C as (C_0, C_1)
$s \leftarrow_R \mathbb{Z}_{[N^2/2]}$	$K = \mathcal{H}(C_0, pk^r)$	$K = \mathcal{H}(C_0, C_0^s)$
$pk = g^s$	$C_1 = \mathcal{E}(K, m)$	
Return (sk, pk)	Return $C = (C_0, C_1)$	Return $\{m, \perp\} \leftarrow \mathcal{D}(K, C_1)$

Fig.3. PKE scheme $\mathrm{HE}_3 = (Keygen, Enc, Dec)$.

5 Conclusion

In this paper, we give a generic public key encryption construction secure against related key attacks from the projective HPS in the standard model, show the DDH based scheme in [18] fits our framework and give more instantiations based on other hard subset membership problems, like the QR and DCR assumptions. We require the HPS be κ-entropic and use a 4-wise independent hash function as a randomness extractor. Compared with previous works, our construction removed the use of one-time signatures, thus is more efficient.

Acknowledgments

We are very grateful to anonymous reviewers for their helpful comments. We also thank Yamin Liu for helpful discussions.

References

1. Bellare, M. and Cash, D.: Pseudorandom Functions and Permutations Provably Secure against Related-Key Attacks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 666-684. Springer, Heidelberg (2010)
2. Bellare, M., Cash, D. and Miller, R.: Cryptography Secure against Related-Key Attacks and Tampering. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 486-503. Springer, Heidelberg (2011). Also Cryptology ePrint Archive, Report 2011/252.
3. Bellare, M. and Kohno, T.: A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491-506. Springer, Heidelberg (2003)
4. Bellare, M. and Namprempre, C.: Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. In: Okamoto,T. (ed.) ASIACRYPT 2000, LNCS, vol. 1976, pp. 531-545. Springer, Heidelberg (2000)
5. Bellare, M., Patersom, K.G. and Thomson, S.: RKA Security beyond the Linear Barrier: IBE, Encryption and Signatures. In: Wang, X.and Sako, K.(eds.) ASIACRYPT 2012, LNCS, vol. 7658, pp. 331-348. Springer, Heidelberg (2012)
6. Biham, E.: New Types of Cryptanalytic Attacks Using Related Keys (Extended Abstract). In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 398-409. Springer, Heidelberg (1994)
7. Biham, E. and Shamir, A.: Differential Fault Analysis of Secret Key Cryptosystems. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 513-525. Springer, Heidelberg (1997)
8. Boneh, D.: Twenty Years of Attacks on the RSA Cryptosystem. (1999)
9. Boneh, D., DeMillo, R. A. and Lipton, R. J.: On the Importance of Checking Cryptographic Protocols for Faults (Extended Abstract). In: Fumy, W. (ed.) EUROCRYPT 1997. LNCS, vol. 1233, pp. 37-51. Springer, Heidelberg (1997)
10. Cramer, R. and Shoup, V.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attacks. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 13-25. Springer, Heidelberg (1998)
11. Cramer, R. and Shoup, V.: Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45-64. Springer, Heidelberg (2002)
12. Cramer, R. and Shoup, V.: Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Ciphertext Attack. SIAM J.Compt. 33(1), 167-226 (2003)
13. Damgård, I., Faust, S., Mukherjee, P. and Venturi, D.: Bounded Tamper Resilience: How to Go beyond the Algebraic Barrier. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 140-160. Springer, Heidelberg (2013)
14. Groth,J.: Cryptography in Subgroups of $\mathbb{Z}_n^*$. In: Kilian, J. (ed.) TCC 2005, LNCS, vol. 3378, pp. 50-65. Springer, Berlin, Germany (2005)
15. Håstad, J., Impagliazzo, R., Levin, L.A. and Luby, M.: A Pseudorandom Generator from any One-way Function. SIAM J. Comput, 28(4), 1364-1396 (1999)
16. Hofheinz, D. and Kiltz, E.: Secure Hybrid Encryption from Weakened Key Encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553-571. Springer, Heidelberg (2007)
17. Hofheinz, D. and Kiltz, E.: The Group of Signed Quadratic Residues and Applications. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 637-653. Springer, Heidelberg (2009)
18. Jia, D., Lu, X., Li, B. and Mei, Q.: RKA Secure PKE Based on the DDH and HR Assumptions. In: Susilo, W., Reyhanitabar, R. (eds.) ProvSec 2013. LNCS, vol. 8209, pp. 271-287. Springer, Heidelberg (2013)
19. Kalai, Y.T., Kanukurthi, B. and Sahai, A.: Cryptography with Tamperable and Leaky Memory. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 373-390. Springer, Heidelberg (2011)
20. Kiltz, E., Pietrzak, K., Stam, M. and Yung, M.: A New Randomness Extraction Paradigm for Hybrid Encryption. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 590-609. Springer, Heidelberg (2009). Also Cryptology ePrint Archive, 2008/304.
21. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT 1992. LNCS, vol. 718, pp. 196-208. Springer, Heidelberg (1993)

22. Kurosawa, K. and Desmedt, Y.: A New Paradigm of Hybrid Encryption Scheme. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 426-442. Springer, Heidelberg (2004)
23. Naccache, D. and Stern, J.: A New Public Key Cryptosystem based on Higher Residues. In CCS 1998, pp. 59-66. (1998)
24. Paillier, P.: Public-key Cryptosystems Based on Composite Degree Residuosity Classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223-238. Springer, Heidelberg (1999)
25. Wee, H.: Public Key Encryption against Related Key Attacks. In: Fischlin, M., Buchmann, J. and Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 262-279. Springer, Heidelberg (2012)