Simulation-Based Bi-Selective Opening Security for Public Key Encryption

Junzuo Lai[1,⋆], Rupeng Yang[2,⋆], Zhengan Huang[3,⋆], and Jian Weng[1]

[1] College of Information Science and Technology, Jinan University, Guangzhou, China
laijunzuo@gmail.com, cryptjweng@gmail.com
[2] Department of Computer Science, The University of Hong Kong, Hong Kong, China
orbbyrp@gmail.com
[3] Peng Cheng Laboratory, Shenzhen, China
zhahuang.sjtu@gmail.com

Abstract. Selective opening attacks (SOA) (for public-key encryption, PKE) concern such a multi-user scenario, where an adversary adaptively corrupts some fraction of the users to break into a subset of honestly created ciphertexts, and tries to learn the information on the messages of some unopened (but potentially related) ciphertexts. Until now, the notion of selective opening attacks is only considered in two settings: sender selective opening (SSO), where part of senders are corrupted and messages together with randomness for encryption are revealed; and receiver selective opening (RSO), where part of receivers are corrupted and messages together with secret keys for decryption are revealed.

In this paper, we consider a more natural and general setting for selective opening security. In the setting, the adversary may adaptively corrupt part of senders and receivers *simultaneously*, and get the plaintext messages together with internal randomness for encryption and secret keys for decryption, while it is hoped that messages of uncorrupted parties remain protected. We denote it as Bi-SO security since it is reminiscent of Bi-Deniability for PKE.

We first formalize the requirement of Bi-SO security by the simulation-based (SIM) style, and prove that some practical PKE schemes achieve SIM-Bi-SO-CCA security in the random oracle model. Then, we suggest a weak model of Bi-SO security, denoted as SIM-wBi-SO-CCA security, and argue that it is still meaningful and useful. We propose a generic construction of PKE schemes that achieve SIM-wBi-SO-CCA security in the standard model and instantiate them from various standard assumptions. Our generic construction is built on a newly presented primitive, namely, universal$_\kappa$ hash proof system with key equivocability, which may be of independent interest.

Keywords: Public Key Encryption, Multi-User Security, Selective Opening Security, Simulation-Based Security, Chosen-Ciphertext Security

⋆ Corresponding author.

1 Introduction

Public key encryption (PKE) is a fundamental tool to protect messages sent over a public channel. Usually, a PKE scheme is used in an open system with multi-users. The system contains multiple, say n, users, each with a public key/secret key pair, i.e., there are n public keys in the system. Anyone (even not registered in the system) can send messages over the public channel to a user securely via encrypting the message under the user's public key. Thus, each public key will be used for multiple, say k, times during the lifetime of the system.

Selective Opening Attacks. Currently, the standard security for PKE schemes is the so-called "Chosen-ciphertext attack (CCA) security", which allows the attacker to learn the decryption of its selected ciphertexts. Generally, PKE schemes are designed to guarantee security of all messages in the system against a CCA attacker under the assumption that internal status of all users are properly protected. This assumption, however, will be challenged in some real-world scenarios:

- The attacker may corrupt the senders and learn their messages and the encryption randomness.
- The attacker may corrupt the receivers and learn their secret keys. With the receivers' secret keys, the attacker is able to decrypt all ciphertexts sent to the receivers and obtain the messages.

While it is hopeless to protect those opened messages, one natural question is whether the unopened messages are still well protected. The above attacks are called selective opening attacks. Surprisingly, it is proved that standard security notion (i.e., CCA security) is *not* able to guarantee security against selective opening attacks (SO security) [2, 18, 17].

The notion of SO security for PKE was firstly formalized by Bellare et al. [3] at EUROCRYPT 2009. To date, two settings have been considered for SO security: sender corruption [3] and receiver corruption [2]. In the sender corruption setting, part of senders are corrupted, with the corruption exposing their coins and messages. In the receiver corruption setting, part of receivers are corrupted, with corruption exposing their secret keys and messages. We denote SO security in the sender-corruption setting and in the receiver-corruption setting by SSO security and RSO security, respectively.

Furthermore, for each setting, there are two types of definitions for SO security: indistinguishability-based (IND) SO security and simulation-based (SIM) SO security. IND-SO security requires that no efficient ad-

versary can distinguish the uncorrupted users' ciphertexts from the encryption of fresh messages, which are sampled according to a conditional probability distribution (conditioned on the opened ciphertexts, which means the ciphertexts of the corrupted parties). In other words, IND-SO security requires that the considered message distributions should be efficiently conditionally re-samplable [3]. SIM-SO security requires that anything, which can be computed efficiently from the ciphertexts, the opened messages as well as the corrupted information, can also be computed efficiently only with the opened messages. SIM-SO security imposes no limitation on the message distributions.

Motivations. Previous works on SIM-SO-CCA secure PKE schemes only provide *either* sender selective opening security [3, 9, 16, 20, 26, 14, 25, 27, 21], *or* receiver selective opening security [2, 12, 23, 19, 11, 32]. However, it is rarely possible to predict whether the attacker will corrupt the senders or the receivers beforehand in practice. Moreover, most of the previous works about RSO security only focused on the single-challenge setting, i.e., each public key can only be used *once* to produce a *single ciphertext*. This is very unrealistic in practice.[4]

Based on the above facts, the following question is raised naturally: *How to define security models to capture the practical requirements of selective opening security in the multi-user scenario, and provide secure PKE schemes in the new models?*

Our Contributions. In this paper, for a multi-user system with multiple public keys where each public key will be used multiple times, we give a new security definition of SO security, denoted as SIM-Bi-SO-CCA security. In the security model, the adversary may adaptively corrupt some fraction of senders and receivers *simultaneously*, and get the plaintext messages together with internal randomness for encryption and secret keys for decryption, while it is hoped that messages of uncorrupted parties remain protected. (The definition is reminiscent of Bi-Deniability [29] for PKE.) We prove that some practical PKE schemes achieve SIM-Bi-SO-CCA security in the random oracle model.

Then, we suggest a weak model of SIM-Bi-SO-CCA security, denoted as SIM-wBi-SO$_k$-CCA security ($k \in \mathbb{N}$), where (i) the adversary has to specify whether it is going to corrupt the senders or the receivers after receiving the public keys and before seeing the challenge ciphertexts, and

[4] Very recently, Yang et al. [32] formalized the notion of RSO security in the multi-challenge setting. But their work only considers the receiver corruption setting.

(ii) if the adversary chooses to corrupt some fraction of the receivers, it is just allowed to corrupt the receivers whose public keys are employed for encryption *at most k times*. We stress that the weak model is still meaningful and useful because it provides the original SIM-SSO-CCA security and SIM-RSO-CCA security *simultaneously*. Furthermore, we show that SIM-wBi-SO$_k$-CCA security is strictly stronger than SIM-SSO-CCA security and SIM-RSO-CCA security. We also stress that the recently proposed SIM-RSO$_k$-CCA security notion [32] is a special case of our SIM-wBi-SO$_k$-CCA security.

Finally, we propose a generic construction of PKE that achieves SIM-wBi-SO$_k$-CCA security in the standard model and instantiate it from various standard assumptions. Our generic construction is built on a new variant of hash proof system (HPS), which should additionally satisfy the universal$_{k+1}$ property and key equivocability. The technical overview of the generic construction is given in Sec. 4.1. We also explore the existence of universal$_{k+1}$ HPS with key equivocability and provide instantiations from either the DDH assumption or the DCR assumption.

Related works. Since proposed by Bellare et al. in [3], selective opening secure PKE has been extensively studied.

For SSO security, Bellare et al. in [3] firstly showed that any lossy encryption is IND-SSO-CPA secure. IND-SSO-CCA secure PKE schemes were constructed from All-But-N lossy trapdoor functions [13] or All-But-Many lossy trapdoor functions [16, 25, 5, 21]. If this lossy encryption has an efficient opener, then the resulting PKE scheme can be proven to be SIM-SSO-CCA secure as shown in [3]. Fehr et al. [9] showed an approach, employing extended hash proof system and cross-authentication code (XAC), to build SIM-SSO-CCA secure PKE schemes. As pointed out in [20], a stronger property of XAC is needed to make the proof rigorous. Following this line of research, a generic construction of SIM-SSO-CCA seucre PKE, from a special kind of key encapsulation mechanism (KEM) and a strengthened XAC, was proposed in [26] and then extended to achieve tight security in [27]. As showed in [14, 15], some practical PKE constructions also enjoy SIM-SSO-CCA security.

For RSO security, Hazay et al. [12] showed that SIM-RSO-CPA secure PKE can be built from non-committing encryption for receiver (NCER) [6], and IND-RSO-CPA secure PKE can be built from a tweaked variant of NCER. IND-RSO-CCA secure PKE schemes were proposed in [23]. SIM-RSO-CCA secure PKE was constructed using indistinguishability obfuscation (iO) in [22], and constructed based on standard computa-

tional assumptions in [11, 19]. Recently, Yang et al. [32] formalized the notion of multi-challenge RSO security (RSO_k security), proved that SIM-RSO security is not enough to guarantee SIM-RSO_k security ($k > 1$), and showed SIM-RSO_k-CPA/CCA secure PKE constructions.

Roadmap. In the rest part of this work, we give some preliminaries in Sec. 2. We introduce the formal definitions for SIM-Bi-SO-CCA security and SIM-wBi-SO_k-CCA security ($k \in \mathbb{N}$), and show that SIM-wBi-SO_k-CCA security is strictly stronger than SIM-SSO-CCA and SIM-RSO-CCA security in Sec. 3. Next, we introduce the main building block, namely, universal_κ HPS with key equivocability, and present a generic construction of PKE scheme that achieves SIM-wBi-SO_k-CCA security in the standard model in Sec. 4. Finally, we show that some practical PKE schemes achieve SIM-Bi-SO-CCA security in the random oracle model, in Sec. 5.

2 Preliminaries

Notations. Throughout this paper, let $\lambda \in \mathbb{N}$ denote the security parameter. For $n \in \mathbb{N}$, let $[n]$ denote the set $\{1, 2, \cdots, n\}$. For a finite set $\mathcal{S}$, we use $|\mathcal{S}|$ to denote the size of $\mathcal{S}$; we use $s \leftarrow \mathcal{S}$ to denote the process of sampling s uniformly from $\mathcal{S}$. For a distribution Dist, $x \leftarrow \mathsf{Dist}$ denotes the process of sampling x from Dist.

We use boldface to denote vectors, e.g., $\mathbf{x}$. We use $\mathbf{x}[i]$ to denote the i-th component of $\mathbf{x}$.

For a probabilistic algorithm $\mathcal{A}$, let $\mathcal{R}_\mathcal{A}$ denote the randomness space of $\mathcal{A}$. We let $y \leftarrow \mathcal{A}(x; r)$ denote the process of running $\mathcal{A}$ on input x and inner randomness $r \in \mathcal{R}_\mathcal{A}$ and outputting y. We write $y \leftarrow \mathcal{A}(x)$ for $y \leftarrow \mathcal{A}(x; r)$ with uniformly chosen $r \in \mathcal{R}_\mathcal{A}$. We write PPT for probabilistic polynomial-time. For a function $f(\lambda)$, we write that $f(\lambda) \leq \mathsf{negl}(\lambda)$ if it is negligible.

For two distributions Dist_1 and Dist_2, the statistical distance between Dist_1 and Dist_2 is defined as

$$\Delta(\mathsf{Dist}_1, \mathsf{Dist}_2) := \frac{1}{2} \sum_x \left| \Pr_{X_1 \leftarrow \mathsf{Dist}_1}[X_1 = x] - \Pr_{X_2 \leftarrow \mathsf{Dist}_2}[X_2 = x] \right|.$$

We say that Dist_1 and Dist_2 are statistically indistinguishable (denoted by $\mathsf{Dist}_1 \overset{s}{\approx} \mathsf{Dist}_2$), if $\Delta(\mathsf{Dist}_1, \mathsf{Dist}_2)$ is negligible.

Collision-resistant hash. We recall the definition of collision-resistant hash function here.

Definition 1. (Collision-resistant hash function). A family of *collision-resistant hash function* $\mathcal{H}$, with domain Dom and range Rge, is a family of functions having the following property: for any PPT algorithm $\mathcal{A}$, its advantage $\mathtt{Adv}^{\mathrm{CR}}_{\mathcal{H},\mathcal{A}}(\lambda) := \Pr[\mathsf{H} \leftarrow \mathcal{H}; (x, x') \leftarrow \mathcal{A}(\mathsf{H}) : x \neq x' \bigwedge \mathsf{H}(x) = \mathsf{H}(x')]$ is negligible.

Efficiently samplable and explainable domain. In this paper, some of the domains are required to be efficiently samplable and explainable [9]. We recall its definition as follows.

Definition 2. (Efficiently samplable and explainable domain). *We say that a domain* Dom *is* efficiently samplable and explainable*, if there are two PPT algorithms* $(\mathsf{Sample}, \mathsf{Explain})$*:*

- $\mathsf{Sample}(\mathsf{Dom}; r)$: *On input a domain* Dom *with uniformly sampled* $r \leftarrow \mathcal{R}_{\mathsf{Sample}}$*,* Sample *outputs an element which is uniformly distributed over* Dom*.*
- $\mathsf{Explain}(\mathsf{Dom}, x)$: *On input* Dom *and* $x \in \mathsf{Dom}$*,* $\mathsf{Explain}$ *outputs* r *which is uniformly distributed over the set* $\{r \in \mathcal{R}_{\mathsf{Sample}} \mid \mathsf{Sample}(\mathsf{Dom}; r) = x\}$*.*

This notion can be relaxed by allowing a negligibly small error probability (which includes that sampling algorithms may produce near-uniform output).

Cross-authentication code. The notion of ℓ-cross-authentication code (XAC) was proposed by Fehr et al. [9], and later adapted to strong and semi-unique XAC in [24].

Definition 3. (ℓ-Cross-authentication code). For $\ell \in \mathbb{N}$, an ℓ-cross-authentication code (ℓ-XAC) XAC, associated with a key space $\mathcal{XK}$ and a tag space $\mathcal{XT}$, consists of three PPT algorithms (XGen, XAuth, XVer). Algorithm $\mathsf{XGen}(1^\lambda)$ generates a uniformly random key $K \in \mathcal{XK}$, deterministic algorithm $\mathsf{XAuth}(K_1, \cdots, K_\ell)$ produces a tag $T \in \mathcal{XT}$, and deterministic algorithm $\mathsf{XVer}(K, T)$ outputs $b \in \{0, 1\}$. The following properties are required:

- **Correctness:** For all $i \in [\ell]$, $\mathsf{fail}_{\mathsf{XAC}}(\lambda) := \Pr[\mathsf{XVer}(K_i, \mathsf{XAuth}(K_1, \cdots, K_\ell)) \neq 1]$ is negligible, where $K_1, \cdots, K_\ell \leftarrow \mathsf{XGen}(1^\lambda)$ in the probability.

- **Security against impersonation and substitution attacks:** $\mathtt{Adv}^{\mathrm{IMP}}_{\mathsf{XAC}}(\lambda)$ and $\mathtt{Adv}^{\mathrm{SUB}}_{\mathsf{XAC}}(\lambda)$ as defined below are both negligible: $\mathtt{Adv}^{\mathrm{IMP}}_{\mathsf{XAC}}(\lambda) := \max_{i,T'} \Pr[K \leftarrow \mathsf{XGen}(1^\lambda) : \mathsf{XVer}(K, T') = 1]$, where the max is over all $i \in [\ell]$ and $T' \in \mathcal{XT}$, and

$$\mathtt{Adv}^{\mathrm{SUB}}_{\mathsf{XAC}}(\lambda) := \max_{i,K_{\neq i},F} \Pr\left[\begin{array}{l} K_i \leftarrow \mathsf{XGen}(1^k) \\ T = \mathsf{XAuth}((K_j)_{j\in[\ell]}) : \\ T' \leftarrow F(T) \end{array} \begin{array}{c} T' \neq T \bigwedge \\ \mathsf{XVer}(K_i, T') = 1 \end{array}\right],$$

  where the max is over all $i \in [\ell]$, all $K_{\neq i} := (K_j)_{j\neq i} \in \mathcal{XK}^{\ell-1}$ and all possibly randomized functions $F : \mathcal{XT} \to \mathcal{XT}$.

Definition 4. (Strong and semi-unique ℓ-XAC). For $\ell \in \mathbb{N}$, we say that an ℓ-XAC XAC is strong and semi-unique, if it has the following two properties:

- **Strongness:** There is a PPT algorithm ReSamp, which takes $i \in [\ell]$, $K_{\neq i}$ and T as input (where $K_1, \cdots, K_\ell \leftarrow \mathsf{XGen}(1^\lambda)$ and $T = \mathsf{XAuth}((K_j)_{j\in[\ell]})$) and outputs K'_i, such that K'_i and K_i are statistically indistinguishable, i.e.,

$$\begin{aligned} \mathtt{StD}^{\mathrm{STRN}}_{\mathsf{XAC}}(\lambda) &:= \Delta(K'_i, K_i) \\ &= \frac{1}{2} \sum_{K\in\mathcal{XK}} \left|\Pr[K'_i = K|(K_{\neq i}, T)] - \Pr[K_i = K|(K_{\neq i}, T)]\right| \end{aligned}$$

  is negligible, where the probabilities are taken over $K_i \leftarrow \mathsf{XGen}(1^\lambda)$, conditioned on $(K_{\neq i}, T)$, and the randomness of ReSamp.
- **Semi-uniqueness:** The key space $\mathcal{XK}$ can be written as $\mathcal{K}_a \times \mathcal{K}_b$. Given a tag $T \in \mathcal{XT}$ and $K_a \in \mathcal{K}_a$, there is at most one $K_b \in \mathcal{K}_b$ such that $\mathsf{XVer}((K_a, K_b), T) = 1$.

3 Bi-SO Security for PKE

Previous security notions of SOA for PKE only consider *either* sender corruption setting *or* receiver corruption setting. We consider a more natural and general setting for selective opening security. In the setting, the adversary may adaptively corrupt part of senders and receivers *simultaneously*. We denote it as Bi-SO security since it is reminiscent of Bi-Deniability [29] for PKE.

For a multi-user system with multiple public keys where each public key will be used many times, we firstly give the most natural security

notion of Bi-SO security, denoted as SIM-Bi-SO-CCA security. Then, we suggest a weak model of SIM-Bi-SO-CCA security, denoted as SIM-wBi-SO_k-CCA security ($k \in \mathbb{N}$). The weak model is still meaningful and useful because it provides the original SIM-SSO-CCA security and SIM-RSO-CCA security *simultaneously*. Finally, for completeness, we show that SIM-wBi-SO_k-CCA security is strictly stronger than SIM-SSO-CCA and SIM-RSO-CCA security.

3.1 Security Definitions

Simulation-based Bi-SO security. In the Bi-SO setting, some of the senders and some of the receivers may be corrupted *simultaneously*, and each public key may be used to encrypt multiple messages. The formal definition is as follows.

Definition 5. (SIM-Bi-SO-CCA). *We say that a PKE scheme* $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$[5] *is* SIM-Bi-SO-CCA *secure, if for any PPT adversary* $\mathcal{A}$*, there exists a PPT simulator* $\mathcal{S}$*, such that for any PPT distinguisher* $\mathcal{D}$*,*

$$\begin{aligned}\mathtt{Adv}^{\text{SIM-Bi-SO-CCA}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},\mathcal{D}}(\lambda) := |\Pr[\mathcal{D}(\mathtt{Exp}^{\text{Bi-SO-real}}_{\mathsf{PKE},\mathcal{A}}(\lambda)) = 1] \\ - \Pr[\mathcal{D}(\mathtt{Exp}^{\text{Bi-SO-ideal}}_{\mathsf{PKE},\mathcal{S}}(\lambda)) = 1]|\end{aligned}$$

is negligible, where both $\mathtt{Exp}^{\text{Bi-SO-real}}_{\mathsf{PKE},\mathcal{A}}(\lambda)$ *and* $\mathtt{Exp}^{\text{Bi-SO-ideal}}_{\mathsf{PKE},\mathcal{S}}(\lambda)$ *are defined in Fig. 1.*

Note that in the real experiment, the total number of public keys and the times that each public key is used for encryption are completely determined by the adversary.

Remark 1 *One can generalize both SIM-Bi-SO-CCA and SIM-wBi-*SO_k*-CCA security to a new version that the adversary is allowed to make multiple selective opening queries* adaptively*. We stress that all the PKE constructions presented in this paper also achieve the generalized security.*

[5] Note that both SIM-Bi-SO-CCA and SIM-wBi-SO_k-CCA security capture the security requirements in a multi-user scenario, where multiple public/secret key pairs are involved. In this setting, some global information is needed to be generated by a global algorithm Setup, as done in previous works about multi-user security, such as [1].

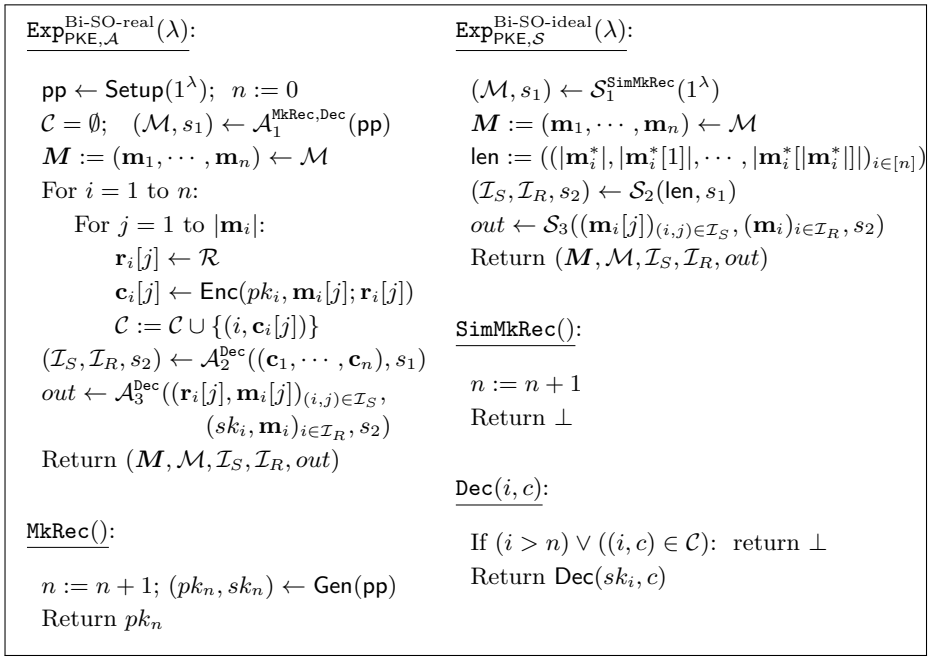

Fig. 1 Experiments for defining SIM-Bi-SO-CCA security of PKE. In these two experiments, we require that $\mathcal{I}_S \subset \{(i,j) \mid i \in [n], j \in [|\mathbf{m}_i|]\}$ and $\mathcal{I}_R \subset [n]$.

Simulation-based weak Bi-SO security. Now we introduce a weak model of SIM-Bi-SO-CCA security, which we denote as SIM-wBi-SO$_k$-CCA security ($k \in \mathbb{N}$). The differences between these two security models are that in the real experiment of SIM-wBi-SO$_k$-CCA security: (i) the adversary has to specify whether it is going to corrupt some fraction of the senders *or* the receivers, *before seeing the challenge ciphertexts*; (ii) if the adversary chooses to corrupt some fraction of the receivers, it is just allowed to corrupt the receivers whose public keys are used for encryption *at most k times*. The formal definition is as follows.

Definition 6. (SIM-wBi-SO$_k$-CCA). *For any $k \in \mathbb{N}$, we say that a PKE scheme* $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* SIM-wBi-SO$_k$-CCA *secure, if for any PPT adversary $\mathcal{A}$, there exists a PPT simulator $\mathcal{S}$, such that for any PPT distinguisher $\mathcal{D}$,*

$$\mathtt{Adv}^{\text{SIM-wBi-SO}_k\text{-CCA}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},\mathcal{D}}(\lambda) := |\Pr[\mathcal{D}(\mathtt{Exp}^{\text{wBi-SO-real}}_{\mathsf{PKE},\mathcal{A},k}(\lambda)) = 1] - \Pr[\mathcal{D}(\mathtt{Exp}^{\text{wBi-SO-ideal}}_{\mathsf{PKE},\mathcal{S},k}(\lambda)) = 1]|$$

is negligible, where both $\mathtt{Exp}^{\text{wBi-SO-real}}_{\mathsf{PKE},\mathcal{A},k}(\lambda)$ *and* $\mathtt{Exp}^{\text{wBi-SO-ideal}}_{\mathsf{PKE},\mathcal{S},k}(\lambda)$ *are defined in Fig. 2.*

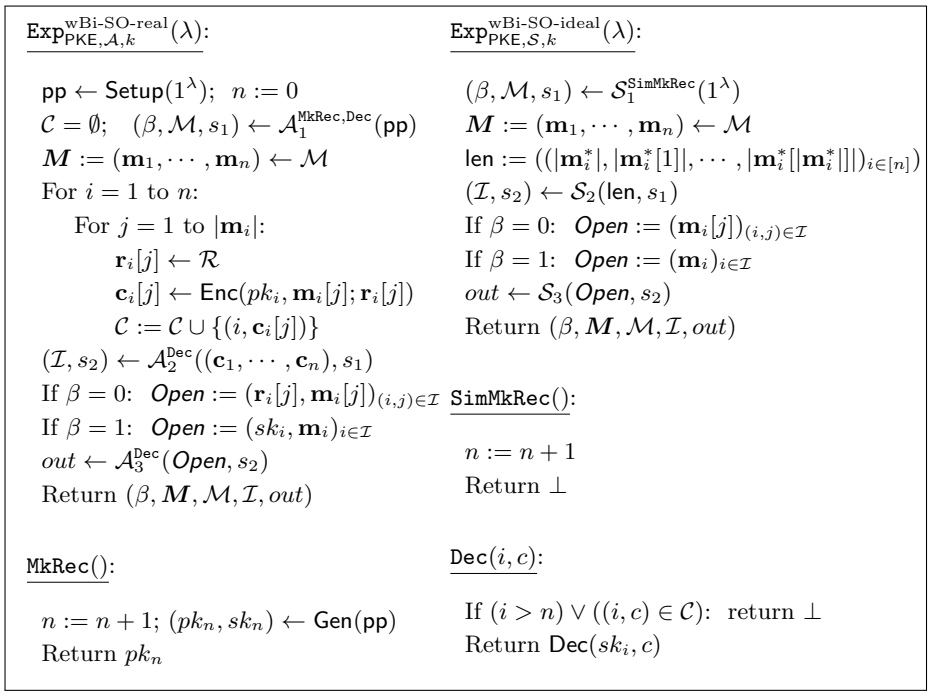

Fig. 2 Experiments for defining SIM-wBi-SO$_k$-CCA security. Here in both $\mathtt{Exp}^{\text{wBi-SO-real}}_{\mathsf{PKE},\mathcal{A},k}(\lambda)$ and $\mathtt{Exp}^{\text{wBi-SO-ideal}}_{\mathsf{PKE},\mathcal{S},k}(\lambda)$, we require that (i) $\beta \in \{0, 1\}$, and (ii) when $\beta = 0$, $\mathcal{I} \subset \{(i, j) \mid i \in [n], j \in [|\mathbf{m}_i|]\}$, and when $\beta = 1$, $\mathcal{I} \subset \{i \in [n] \mid |\mathbf{m}_i| \leq k\}$.

In both $\mathtt{Exp}^{\text{wBi-SO-real}}_{\mathsf{PKE},\mathcal{A},k}(\lambda)$ and $\mathtt{Exp}^{\text{wBi-SO-ideal}}_{\mathsf{PKE},\mathcal{S},k}(\lambda)$, we use $\beta = 0$ (resp. $\beta = 1$) to represent that adversary $\mathcal{A}$/simulator $\mathcal{S}$ chooses to corrupt some of the senders (resp. receivers). We stress that in $\mathtt{Exp}^{\text{wBi-SO-real}}_{\mathsf{PKE},\mathcal{A},k}(\lambda)$, when $\mathcal{A}_1$ outputs $\beta = 0$, the parameter k puts no restrictions on sender corruptions $\mathcal{I}$; and when $\mathcal{A}_1$ outputs $\beta = 1$, $\mathcal{A}_2$ is allowed to corrupt the receivers whose public keys are used for encryption at most k times (i.e., $\mathcal{I} \subset \{i \in [n] \mid |\mathbf{m}_i| \leq k\}$).

Note that the original SIM-SSO-CCA security [13, 9] and SIM-RSO-CCA security [11, 19] are both special cases of SIM-wBi-SO$_k$-CCA security. Specifically, the original SIM-SSO-CCA security is SIM-wBi-SO$_k$-CCA security when $\mathcal{A}_1$ always outputs $\beta = 0$ and queries the $\mathtt{MkRec}$ oracle on-

ly once[6], and the original SIM-RSO-CCA security is SIM-wBi-SO$_k$-CCA security when $\mathcal{A}_1$ always outputs $\beta = 1$ and $|\mathbf{m}_1| = \cdots = |\mathbf{m}_n| = 1$ (note that the latter implicitly suggests $k = 1$). Hence, for a SIM-wBi-SO$_k$-CCA secure PKE scheme, it achieves the original SIM-SSO-CCA and SIM-RSO-CCA (and even SIM-RSO$_k$-CCA) security *simultaneously*.

Very recently, Yang et al. [32] introduced an enhanced security notion of RSO, *SIM-RSO$_k$-CCA security* ($k \in \mathbb{N}$), for PKE. We notice that their SIM-RSO$_k$-CCA security is a special case of SIM-wBi-SO$_k$-CCA security as well. Specifically, SIM-RSO$_k$-CCA security is SIM-wBi-SO$_k$-CCA security when $\mathcal{A}_1$ always outputs $\beta = 1$.

3.2 Separation of SIM-wBi-SO$_k$-CCA and SIM-SSO-CCA & SIM-RSO-CCA

Now we show that SIM-wBi-SO$_k$-CCA security is *strictly* stronger than SIM-SSO-CCA security and SIM-RSO-CCA security. Our conclusion is derived from the fact that SIM-wBi-SO$_k$-CCA security implies SIM-SSO-CCA and SIM-RSO-CCA security simultaneously, and SIM-SSO-CCA and SIM-RSO-CCA security do not imply each other. Actually, we have stronger conclusions:

(1) Supposing that the κ-Linear assumption holds ($\kappa \in \mathbb{N}$), SIM-SSO-CCA security does not imply SIM-RSO-*CPA* security;
(2) Supposing that the DDH or DCR assumption holds, SIM-RSO-CCA security does not imply SIM-SSO-*CPA* security.

SIM-SSO-CCA$\not\Rightarrow$SIM-RSO-CPA. Bellare et al. [2] introduced the notion of *decryption verifiability* for PKE, and showed that assuming the existence of a family of collision-resistant hash functions, which can be constructed under the discrete-logarithm assumption [10], any decryption-verifiable PKE scheme is not SIM-RSO-CPA secure [2, Theorem 5.1][7].

Informally, a PKE scheme $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ is called *decryption-verifiable*, if it is infeasible to generate $(pk, sk_0, sk_1, c, m_0, m_1)$ such that (i) $m_0 \neq m_1$, (ii) both sk_0 and sk_1 are valid secret keys corresponding to pk, and (iii) $\mathsf{Dec}(sk_0, c) = m_0$ and $\mathsf{Dec}(sk_1, c) = m_1$. We

[6] The SIM-SSO-CPA security notion presented in [4] allows the adversary to query the `MkRec` oracle multiple times.

[7] Both [2, Theorem 5.1] and [2, Theorem 4.1] only hold in the the auxiliary input model (i.e., in the experiments defining SIM-RSO-CPA and SIM-SSO-CPA security, both the adversary and the simulator get an auxiliary input). So do our counterexamples in this section. These counterexamples may be modified with the technique proposed in [2, Sec. 6] to drop the auxiliary inputs.

note that (i) and (iii) implicitly suggest that $sk_0 \neq sk_1$. In other words, for any PKE scheme, if each of its public key uniquely determines its corresponding secret key, then it must be decryption-verifiable.

We notice that the κ-Linear-based SIM-SSO-CCA secure PKE scheme proposed by Liu and Paterson [26] is such a decryption-verifiable PKE scheme. Generally, a public key of the κ-Linear-based Liu-Paterson scheme is of the form $(g^y, (g^{x_\theta}, g^{x_\theta \alpha_\theta}, g^{x_\theta \beta_\theta})_{\theta \in [\kappa]})$, where g is a generator of a cyclic group $\mathbb{G}$ of prime order q and $(y, (x_\theta, \alpha_\theta, \beta_\theta)_{\theta \in [\kappa]}) \in (\mathbb{Z}_q)^{3\kappa+1}$, and the corresponding secret key is $(\alpha_\theta, \beta_\theta, x_\theta^{-1} y)_{\theta \in [\kappa]}$. It's obvious that the public key uniquely determines its corresponding secret key. So the κ-Linear-based Liu-Paterson scheme is decryption-verifiable. According to [2, Theorem 5.1], we conclude that assuming the existence of a family of collision-resistant hash functions, the κ-Linear-based Liu-Paterson scheme is not SIM-RSO-CPA secure.

For completeness, we recall the formal definition of decryption verifiability [2] and the κ-Linear-based Liu-Paterson scheme [26] in the full version of this paper.

SIM-RSO-CCA$\not\Rightarrow$SIM-SSO-CPA. As pointed out in [2, Theorem 4.1], the DDH-based Cramer-Shoup scheme [7] is not SIM-SSO-CPA secure. On the other hand, Huang et al. [19] and Hara et al. [11] showed that this PKE scheme (for single-bit message) achieves SIM-RSO-CCA security. This fact suggests that when the DDH assumption holds, SIM-RSO-CCA security does not imply SIM-SSO-CPA security. With similar analysis, this conclusion can be extended to the case that the DCR assumption holds.

4 PKE with SIM-wBi-SO$_k$-CCA Security

In this section, we propose a PKE scheme achieving SIM-wBi-SO$_k$-CCA security. We firstly introduce a new primitive, universal$_\kappa$ HPS with key equivocability for any polynomially bounded function κ, and provide concrete constructions for it from the DDH assumption and the DCR assumption respectively. Then, with this new primitive as a building block, we show our PKE construction and prove that it meets SIM-wBi-SO$_k$-CCA security in the standard model.

In order to make our idea more understandable, we firstly provide a technique overview before going into the details.

4.1 Technique Overview

In the real experiment of SIM-wBi-SO$_k$-CCA security, the bit β is used to indicate whether the adversary wants to corrupt some fraction of the senders ($\beta = 0$) or the receivers ($\beta = 1$), and the adversary does not specify the value of β until it sees public keys $(pk_i)_{i\in[n]}$ via querying the oracle $\texttt{MkRec}$. Hence, to prove SIM-wBi-SO$_k$-CCA security, when $\beta = 0$, we need to somehow generate malformed ciphertexts for $(pk_i)_{i\in[n]}$, such that they can be opened in the sense of SSO (i.e., exposing the messages and the corresponding randomness to the adversary); and when $\beta = 1$, we need to somehow generate malformed ciphertexts for $(pk_i)_{i\in[n]}$, such that they can be opened in the sense of RSO (i.e., exposing the messages and the corresponding secret keys to the adversary).

Our scheme, encrypting ℓ-bit messages, is inspired by the works of [9, 20, 24]. The public/secret key pair is ℓ pairs of public and secret keys (i.e., $(hpk_\gamma, hsk_\gamma)_{\gamma\in[\ell]}$) of a hash proof system (HPS) HPS [8]. Informally, to encrypt a message $m = (m_1, \cdots, m_\ell) \in \{0,1\}^\ell$, the encryption algorithm sets that for each $\gamma \in [\ell]$,

$$\begin{cases} \text{If } m_\gamma = 0: \ x_\gamma \leftarrow \mathcal{X};\ K_\gamma \leftarrow \mathcal{K}_{sp} \\ \text{If } m_\gamma = 1: \ x_\gamma \leftarrow \mathcal{L};\ K_\gamma = \mathsf{PubEv}(hpk_\gamma, x_\gamma, w_\gamma) \end{cases}$$

where $\mathcal{L} \subset \mathcal{X}$ and $\mathcal{X}$ are both finite sets generated with a hard subset membership problem, PubEv is the public evaluation algorithm of HPS, w_γ is a witness for $x_\gamma \in \mathcal{L}$, and $\mathcal{K}_{sp}$ is the range of PubEv. Then, we use a strengthened cross-authentication code (XAC) to "glue" $x_1, \cdots, x_\ell$ together, obtaining a XAC tag T. So the generated ciphertext corresponding to m is $c = (x_1, \cdots, x_\ell, T)$. To decrypt a ciphertext $c = (x_1, \cdots, x_\ell, T)$, the decryption algorithm firstly computes that $(\overline{K}_\gamma = \mathsf{SecEv}(hsk_\gamma, x_\gamma))_{\gamma\in[\ell]}$, where SecEv is the secret evaluation algorithm of HPS, and then for each $\gamma \in [\ell]$, sets $\overline{m}_\gamma = 1$ if and only if T is verified correctly by $\overline{K}_\gamma$ (via the verification algorithm of XAC).

Now we turn to the security proof. In order to prove SIM-wBi-SO$_k$-CCA security, we need to construct a PPT simulator $\mathcal{S}$, such that the ideal experiment and the real experiment are indistinguishable. In particular, we need to generate some malformed ciphertexts (before seeing the real messages), such that they are computationally indistinguishable from the real challenge ciphertexts, and meanwhile can be efficiently opened according to the value of β.

If $\beta = 0$, we need to generate malformed ciphertexts $c = (x_1, \cdots, x_\ell, T)$, and then open them according to the real messages $m = (m_1, \cdots, m_\ell)$,

by providing random coins which can be used to encrypt the real messages to recover the malformed ciphertexts. We generate the malformed ciphertexts with encryptions of ℓ ones, i.e., for each $\gamma \in [\ell]$, $x_\gamma \leftarrow \mathcal{L} \subset \mathcal{X}$ and $K_\gamma = \mathsf{PubEv}(hpk_\gamma, x_\gamma, w_\gamma) \subset \mathcal{K}_{sp}$. Hence, after generating these malformed ciphertexts, to open a ciphertext, for each $\gamma \in [\ell]$, if the real message bit $m_\gamma = 1$, the random coin (i.e., w_γ) employed to generate (x_γ, K_γ) can be returned directly; if $m_\gamma = 0$, return the random coin which is generated by explaining x_γ as a random element sampled from $\mathcal{X}$, and explaining K_γ as a random key sampled from $\mathcal{K}_{sp}$.

Now, we show that a real challenge ciphertext can be substituted with the malformed ciphertext without changing the adversary's view significantly. For $\gamma = 1$ to ℓ,

1) We modify the decryption procedure of the decryption oracle, such that it does not make use of hsk_γ. More specifically, for a decryption query $c' = (x'_1, \cdots, x'_\ell, T')$, if $x'_\gamma \notin \mathcal{L}$, the decryption oracle directly sets $\overline{m}_\gamma = 0$. The statistical properties of HPS and strengthened XAC guarantee that this modification does not change the adversary's view significantly.
2) If $m_\gamma = 0$, the randomly sampled K_γ is replaced with $K_\gamma = \mathsf{SecEv}(hsk_\gamma, x_\gamma)$. The perfect universality of HPS guarantees that this change is imperceptible to the adversary.
3) If $m_\gamma = 0$, K_γ is updated again via the resampling algorithm of strengthened XAC. The statistical property of strengthened XAC guarantees that this modification does not change the adversary's view significantly.
4) The decryption procedure of the decryption oracle is changed to work with the original decryption rules. The statistical properties of HPS and strengthened XAC guarantee that this modification is imperceptible to the adversary.
5) If $m_\gamma = 0$, $x_\gamma \leftarrow \mathcal{L}$ instead of uniformly sampling from $\mathcal{X}$. The underlying subset membership problem of HPS guarantees that this change is also imperceptible to the adversary.

Note that these substitutions only consider the situation that a single public key is used to encrypt a single message. Fortunately, we can extend it to the situation that there are n public keys (for any $n \in \mathbb{N}$), and each public key is employed to encrypt multiple messages.

If $\beta = 1$, we need to generate malformed ciphertexts, and then open them according to the real messages, by providing valid secret keys which can be used to decrypt the malformed ciphertexts to obtain the messages.

Note that a public key of this scheme is of the form $pk = (hpk_1, \cdots, hpk_\ell)$, and the corresponding secret key is $sk = (hsk_1, \cdots, hsk_\ell)$. Hence, informally, what we need is to generate a malformed ciphertext without seeing the message, such that for any message $m = (m_1, \cdots, m_\ell) \in \{0, 1\}^\ell$, we can generate some secret key $sk' = (hsk'_1, \cdots, hsk'_\ell)$ satisfying that (i) sk' is a valid secret key corresponding to pk (i.e., for all $\gamma \in [\ell]$, hsk'_γ is a valid HPS secret key corresponding to hpk_γ); (ii) decrypting the malformed ciphertext with sk' will lead to m.

We try to generate such a malformed ciphertext $c = (x_1, \cdots, x_\ell, T)$. For each $\gamma \in [\ell]$, if $x_\gamma \in \mathcal{L}$ (with a witness w_γ), all the HPS secret keys corresponding to hpk_γ will lead to the same $\widetilde{K}_\gamma = \mathsf{PubEv}(hpk_\gamma, x_\gamma, w_\gamma) = K_\gamma$. In other words, for any fixed ciphertext $(\cdots, x_\gamma, \cdots, T)$, no matter what the secret key is, the decryption of this ciphertext will lead to the same $\overline{m}_\gamma$. So it's impossible to open the malformed ciphertext successfully when $m_\gamma = 1 - \overline{m}_\gamma$. Hence, our malformed ciphertexts focus on the case $c = (x_1, \cdots, x_\ell, T)$ that $x_1, \cdots, x_\ell \in \mathcal{X} \backslash \mathcal{L}$. On the other hand, if K_γ is uniformly sampled, it seems unlikely to decrypt the ciphertext to recover the original message when $m_\gamma = 1$ due to the property of XAC. So our malformed ciphertexts further focus on the case $c = (x_1, \cdots, x_\ell, T)$ that for all $\gamma \in [\ell]$, $x_\gamma \in \mathcal{X} \setminus \mathcal{L}$ and $K_\gamma = \mathsf{SecEv}(hsk_\gamma, x_\gamma)$.

We stress that in the real experiment of SIM-wBi-SO$_k$-CCA security, the adversary is just allowed to corrupt the receivers whose public keys are used for encryption at most k times. So for simplicity, here we only consider the case that $pk = (hpk_1, \cdots, hpk_\ell)$ is used to encrypt *exactly* k messages (i.e., $m_j = (m_{j,1}, \cdots, m_{j,\ell}) \in \{0,1\}^\ell$ $(j \in [k])$). More specifically, for each $\gamma \in [\ell]$, hsk_γ is used k times (note that we use sk to generate the malformed ciphertexts), generating k ciphertext parts (i.e., $K_{1,\gamma} = \mathsf{SecEv}(hsk_\gamma, x_{1,\gamma}), \cdots, K_{k,\gamma} = \mathsf{SecEv}(hsk_\gamma, x_{k,\gamma})$). In other words, to generate the k malformed ciphertexts, for each $\gamma \in [\ell]$, we need to

(i) compute $\mathsf{SecEv}(hsk_\gamma, x_{1,\gamma}), \cdots, \mathsf{SecEv}(hsk_\gamma, x_{k,\gamma})$ for some $x_{1,\gamma}, \cdots, x_{k,\gamma} \in \mathcal{X} \setminus \mathcal{L}$ before seeing the messages;
(ii) generate a HPS secret key hsk'_γ such that $\mathsf{SecEv}(hsk'_\gamma, x_{j,\gamma}) = \mathsf{SecEv}(hsk_\gamma, x_{j,\gamma})$ if $m_{j,\gamma} = 1$, and $\mathsf{SecEv}(hsk'_\gamma, x_{j,\gamma}) \neq \mathsf{SecEv}(hsk_\gamma, x_{j,\gamma})$ if $m_{j,\gamma} = 0$.

However, there is no algorithm for HPS which can generate two HPS secret keys (i.e. hsk_γ and hsk'_γ) meeting the above requirements. Therefore, we introduce the following new property, which we call "key equivocability", of HPS. Informally, we require that there is an efficient algorithm $\mathsf{SampHsk}$ and a trapdoor td, such that for any $x_1, \cdots, x_k \in \mathcal{X} \setminus \mathcal{L}$, the

following two distribution ensembles, Dist_0^k and Dist_1^k, are statistically indistinguishable:

$$\begin{aligned}\mathsf{Dist}_0^k := \{(hsk, K_1, \cdots, K_k, hpk) \big| & hsk \leftarrow \mathcal{SK};\ hpk = \mu(hsk); \\ & \forall j \in [k]: \\ & \quad K_j \leftarrow \mathcal{K}_{sp} \quad \text{if } m_j = 0; \\ & \quad K_j = \mathsf{SecEv}(hsk, x_j) \quad \text{if } m_j = 1\}, \quad (1)\end{aligned}$$

$$\begin{aligned}\mathsf{Dist}_1^k := \{(hsk', K_1, \cdots, K_k, hpk) \big| & hsk \leftarrow \mathcal{SK};\ hpk = \mu(hsk); \\ & (K_j = \mathsf{SecEv}(hsk, x_j))_{j\in[k]}; \\ & hsk' \leftarrow \mathsf{SampHsk}(hsk, \mathsf{td}, \{x_j\}_{j\in[k]})\}. \quad (2)\end{aligned}$$

We stress that this property requires that no information about hsk beyond hpk is leaked. Similar to the proof of case $\beta = 0$, we introduce a modification to the decryption oracle before employing the key equivocability of HPS in order to make sure that nothing about hsk beyond hpk is leaked. For any decryption query $(x'_1, \cdots, x'_\ell, T')$ and any γ, if $x'_\gamma \in \mathcal{X} \setminus \mathcal{L}$, the decryption oracle sets $\overline{m}_\gamma = 0$ directly. However, we note that in the SIM-wBi-SO$_k$-CCA security model, each public key is used to encrypt k messages. As a result, hsk may be employed k times, i.e., to compute $\mathsf{SecEv}(hsk, x_1), \cdots, \mathsf{SecEv}(hsk, x_k)$ for some $x_1, \cdots, x_k$. So the perfect universality$_2$ of HPS [8] is not enough to guarantee that the modification to the decryption oracle is imperceptible to the adversary. To solve this problem, we introduce another property, *perfect universality*$_{k+1}$, for HPS. Roughly speaking, HPS is called perfectly universal$_{k+1}$, if for any $x_1, \cdots, x_{k+1} \in \mathcal{X} \setminus \mathcal{L}$ and any $K' \in \mathcal{K}_{sp}$, even given $(hpk, \mathsf{SecEv}(hsk, x_1), \cdots, \mathsf{SecEv}(hsk, x_k))$, the probability that $\mathsf{SecEv}(hsk, x_{k+1}) = K'$ is $\frac{1}{|\mathcal{K}_{sp}|}$.

With the help of this new variant of HPS, we can use algorithm $\mathsf{SampHsk}$ to open the aforementioned equivocable ciphertexts $c = (x_1, \cdots, x_\ell, T)$ where for each $\gamma \in [\ell]$, $x_\gamma \in \mathcal{X} \setminus \mathcal{L}$ and $K_\gamma = \mathsf{SecEv}(hsk_\gamma, x_\gamma)$, successfully. Now, we show that a real challenge ciphertext can be substituted with the malformed ciphertext without changing the adversary's view significantly. A high-level description of the substitution is presented as follows.

1) We use the secret keys to generate the challenge ciphertexts, instead of the public keys. The statistical property of HPS guarantees that this change is imperceptible to the adversary.
2) All the $x_{j,\gamma}$ $(j \in [k], \gamma \in [\ell])$ are sampled from $\mathcal{X} \setminus \mathcal{L}$, instead of being sampled from $\mathcal{L}$ (when $m_{j,\gamma} = 1$). The underlying subset membership

problem of HPS guarantees that this change is also imperceptible to the adversary.

3) Note that $sk = (hsk_1, \cdots, hsk_\ell)$ is employed to encrypt $m_j = (m_{j,1}, \cdots, m_{j,\ell}) \in \{0,1\}^\ell$ $(j \in [k])$, and specifically, for each $\gamma \in [\ell]$, hsk_γ is used to handle $m_{1,\gamma}, \cdots, m_{k,\gamma}$, as shown in Fig. 3. For each $\gamma \in [\ell]$, employ hsk_γ to compute $K_{j,\gamma}$ when $m_{j,\gamma} = 0$ (for all $j \in [k]$). The key equivocability of HPS guarantees that this modification does not change the adversary's view significantly.

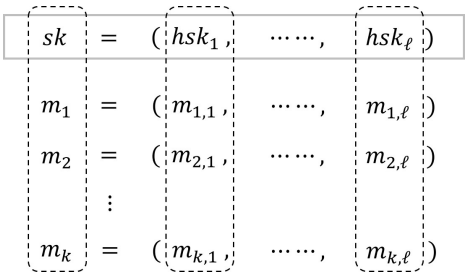

Fig. 3 Relations among sk and $m_1, \cdots, m_k$

4.2 Universal$_\kappa$ Hash Proof System with Key Equivocability

Now we introduce the main building block, namely, universal$_\kappa$ HPS with key equivocability, for any polynomially bounded κ, and show concrete constructions for it.

The definition. For any polynomially bounded function κ, we provide a definition of universal$_\kappa$ HPS with key equivocability, which enhances the standard HPS [8] with key equivocability and universal$_\kappa$ property. It works on a strengthened version of subset membership problem SSMP, which defines some additional languages and provides a trapdoor to recognize elements from these languages.

Definition 7 (Strengthened Subset Membership Problem). *A strengthened subset membership problem (SSMP)* SSMP *consists of five PPT algorithms* $(\mathsf{SSmpG}, \mathsf{SSmpX}, \mathsf{SSmpL}, \mathsf{SSmpLS}, \mathsf{SSmpChk})$*:*

– $\mathsf{SSmpG}(1^\lambda, k)$: *On input* 1^λ *and polynomially bounded* $k > 0$*, algorithm* SSmpG *outputs a system parameter* prm *and a trapdoor* td*. The parameter* prm *defines* $2k+2$ *sets* $(\mathcal{X}, \mathcal{L}, \mathcal{L}_1, \cdots, \mathcal{L}_{2k})$*, where* $\mathcal{X}$ *is an*

efficiently recognizable finite set, $\mathcal{L} \subset \mathcal{X}$, and $\mathcal{L}_1, \cdots, \mathcal{L}_{2k}$ are distinct subsets of $\mathcal{X} \setminus \mathcal{L}$. For simplicity of notation, we write

$$\mathsf{prm} = (\mathcal{X}, \mathcal{L}, \mathcal{L}_1, \ldots, \mathcal{L}_{2k})$$

when employing HPS *for* SSMP *to construct PKE schemes.*

- $\mathsf{SSmpX}(\mathsf{prm})$: *On input* prm, SSmpX *outputs a uniformly chosen $x \leftarrow \mathcal{X}$.*
- $\mathsf{SSmpL}(\mathsf{prm})$: *On input* prm, SSmpL *samples $x \leftarrow \mathcal{L}$ with randomness $w \in \mathcal{R}_{\mathsf{SSmpL}}$, and outputs (x, w). We say that w is a witness for $x \in \mathcal{L}$.*
- $\mathsf{SSmpLS}(\mathsf{prm}, i \in [2k])$: *On input* prm *and $i \in [2k]$,* SSmpLS *outputs a uniformly chosen $x_i \leftarrow \mathcal{L}_i$.*
- $\mathsf{SSmpChk}(\mathsf{prm}, \mathsf{td}, x)$: *On input* prm, td *and x,* SSmpChk *outputs an integer $[0, 2k]$ or an abort symbol $\perp$.*

Also, it satisfies the following properties:

- **Hardness.** *For all $i \in [2k]$, for any PPT distinguisher $\mathcal{D}$, the following advantages are all negligible,*

$$\mathtt{Adv}^{\text{HARD-1}}_{\mathsf{SSMP},\mathcal{D},i}(\lambda) := |\Pr[\mathcal{D}(\mathsf{prm}, x_{\mathcal{X}}) = 1] - \Pr[\mathcal{D}(\mathsf{prm}, x_i) = 1]|,$$

$$\mathtt{Adv}^{\text{HARD-2}}_{\mathsf{SSMP},\mathcal{D},i}(\lambda) := |\Pr[\mathcal{D}(\mathsf{prm}, x_{\mathcal{L}}) = 1] - \Pr[\mathcal{D}(\mathsf{prm}, x_i) = 1]|,$$

  where the probabilities are over $\mathsf{prm} \leftarrow \mathsf{SSmpG}(1^\lambda, k)$, $x_{\mathcal{X}} \leftarrow \mathsf{SSmpX}(\mathsf{prm})$, $(x_{\mathcal{L}}, w) \leftarrow \mathsf{SSmpL}(\mathsf{prm})$, and $x_i \leftarrow \mathsf{SSmpLS}(\mathsf{prm}, i)$. [8]
- **Sparseness.** *The probability*

$$\mathtt{Spar}_{\mathsf{SSMP}}(\lambda) := \Pr[(\mathsf{prm}, \mathsf{td}) \leftarrow \mathsf{SSmpG}(1^\lambda, k); x_{\mathcal{X}} \leftarrow \mathsf{SampX}(\mathsf{prm}) : x_{\mathcal{X}} \in \mathcal{L}]$$

  is negligible.
- **Explainability.** *The finite set $\mathcal{X}$ is an efficiently samplable and explainable domain (as defined in Definition 2).*
- **Sampling Correctness.** *Let $(\mathsf{prm}, \mathsf{td}) \leftarrow \mathsf{SSmpG}(1^\lambda, k)$. Then the distributions of the outputs of* $\mathsf{SSmpX}(\mathsf{prm})$, $\mathsf{SSmpL}(\mathsf{prm})$, *and* $\mathsf{SSmpLS}(\mathsf{prm}, i)$ *($i \in [2k]$) are statistically indistinguishable from uniform distributions over $\mathcal{X}$, $\mathcal{L}$ and $\mathcal{L}_i$ ($i \in [2k]$) respectively.*
- **Checking Correctness.** *For any $(\mathsf{prm}, \mathsf{td})$ generated by* SSmpG, *if $x \in \mathcal{L}$, then $\mathsf{SSmpChk}(\mathsf{prm}, \mathsf{td}, x) = 0$; if there exists $i \in [2k]$ s.t. $x \in \mathcal{L}_i$, then $\mathsf{SSmpChk}(\mathsf{prm}, \mathsf{td}, x) = i$; otherwise, $\mathsf{SSmpChk}(\mathsf{prm}, \mathsf{td}, x) = \perp$.*

[8] Note that a hard SSMP is also a hard SMP, since a simple hybrid argument shows that for any PPT distinguisher $\mathcal{D}$, $|\Pr[\mathcal{D}(\mathsf{prm}, x_{\mathcal{X}}) = 1] - \Pr[\mathcal{D}(\mathsf{prm}, x_{\mathcal{L}}) = 1]| \leq \mathtt{Adv}^{\text{HARD-1}}_{\mathsf{SSMP},\mathcal{D},1}(\lambda) + \mathtt{Adv}^{\text{HARD-2}}_{\mathsf{SSMP},\mathcal{D},1}(\lambda)$.

Remark 2 *The additional trapdoor, generated by* SSmpG*, will also be used in the key equivocability property (see Definition 10) of HPS.*

Definition 8 (Hash Proof System [8]). *A* hash proof system HPS *for a SSMP* SSMP *consists of three PPT algorithms* (PrmG, PubEv, SecEv)*:*

- $\mathsf{PrmG}(\mathsf{prm})$: *Given* prm*, which is generated by* $\mathsf{SSmpG}(1^\lambda, k)$ *and defines* $2k+2$ *sets* $(\mathcal{X}, \mathcal{L}, \mathcal{L}_1, \ldots, \mathcal{L}_{2k})$*, algorithm* PrmG *outputs a parameterized instance* $\mathsf{prmins} := (\mathcal{K}_{sp}, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \mu)$*, where* $\mathcal{K}_{sp}$*,* $\mathcal{SK}$*,* $\mathcal{PK}$ *are all finite sets,* $\Lambda_{(\cdot)} : \mathcal{X} \to \mathcal{K}_{sp}$ *is a family of hash functions indexed with secret hash key* $hsk \in \mathcal{SK}$*, and* $\mu : \mathcal{SK} \to \mathcal{PK}$ *is an efficiently computable function.*
- $\mathsf{SecEv}(hsk, x)$: *On input* $hsk \in \mathcal{SK}$ *and* $x \in \mathcal{X}$*, the* deterministic *secret evaluation algorithm* SecEv *outputs a hash value* $K = \Lambda_{hsk}(x) \in \mathcal{K}_{sp}$*.*
- $\mathsf{PubEv}(hpk, x, w)$: *On input* $hpk = \mu(hsk) \in \mathcal{PK}$*,* $x \in \mathcal{L}$ *and a witness* w *for* $x \in \mathcal{L}$*, the* deterministic *public evaluation algorithm* PubEv *outputs a hash value* $K = \Lambda_{hsk}(x) \in \mathcal{K}_{sp}$*.*

Also, it should be

- **Projective.** *For any* $hsk \in \mathcal{SK}$ *and any* $x \in \mathcal{L}$ *with witness* w*, the hash value* $\Lambda_{hsk}(x)$ *is uniquely determined by* $hpk = \mu(hsk)$ *and* x*, concretely, we require that* $\mathsf{SecEv}(hsk, x) = \mathsf{PubEv}(hpk, x, w)$*.*
- **Perfectly Universal.** *For all* prm *generated by* $\mathsf{SSmpG}(1^\lambda)$*, all possible* $\mathsf{prmins} \leftarrow \mathsf{PrmG}(\mathsf{prm})$*, all* $hpk \in \mathcal{PK}$*, all* $x \in \mathcal{X} \setminus \mathcal{L}$*, and all* $K \in \mathcal{K}_{sp}$*, the probability* $\Pr[\Lambda_{hsk}(x) = K \mid \mu(hsk) = hpk] = \frac{1}{\mathcal{K}_{sp}}$*, where the probability is over* $hsk \leftarrow \mathcal{SK}$*.*

Definition 8 is the same as the original definition of HPS in [8]. In our PKE construction, we further require that $\mathcal{K}_{sp}$ is efficiently samplable and explainable. Besides, we require HPS to have the following two properties.

Definition 9 (Perfectly Universal$_\kappa$). *For any polynomial* κ*, we say that* HPS *is* perfectly universal$_\kappa$*, if for all* prm *generated by* $\mathsf{SSmpG}(1^\lambda, k)$*, all possible* $\mathsf{prmins} \leftarrow \mathsf{PrmG}(\mathsf{prm})$*, all* $hpk \in \mathcal{PK}$*, all pairwise different* $x_1, \cdots, x_\kappa \in \mathcal{X} \setminus \mathcal{L}$*, and all* $K_1, \cdots, K_\kappa \in \mathcal{K}_{sp}$*,*

$$\Pr\left[\Lambda_{hsk}(x_\kappa) = K_\kappa \middle| \begin{array}{c} \mu(hsk) = hpk \\ \Lambda_{hsk}(x_1) = K_1, \cdots, \Lambda_{hsk}(x_{\kappa-1}) = K_{\kappa-1} \end{array}\right] = \frac{1}{|\mathcal{K}_{sp}|},$$

where the probability is over $hsk \leftarrow \mathcal{SK}$*.*

Definition 10 (Key Equivocability). *We say that* HPS *is* key equivocable*, if there is a PPT algorithm* SampHsk*, which takes* $(hsk, \mathsf{td}, x_1, \cdots, x_{2k})$ *as input and outputs another secret key* hsk'*, such that for all possible* $(\mathsf{prm}, \mathsf{td}) \leftarrow \mathsf{SSmpG}(1^\lambda, k)$*, all possible* $\mathsf{prmins} = (\mathcal{K}_{sp}, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \mu) \leftarrow \mathsf{PrmG}(\mathsf{prm})$*, all permutations* $\mathsf{P} : [2k] \to [2k]$*, and all* $(x_1, \cdots, x_{2k}) \in \mathcal{X}^{2k}$ *satisfying that* $x_i \in \mathcal{L}_{\mathsf{P}(i)}$*,* $\Delta(\mathsf{Dist}_0, \mathsf{Dist}_1)$ *is negligible, where* Dist_0 *and* Dist_1 *are defined in Fig. 4.*

$\underline{\mathsf{Dist}_0}$:	$\underline{\mathsf{Dist}_1}$:
$hsk \leftarrow \mathcal{SK};\ hpk = \mu(hsk)$	$hsk \leftarrow \mathcal{SK};\ hpk = \mu(hsk)$
For $i = 1$ to k :	For $i = 1$ to $2k$:
$\quad K_i = \mathsf{SecEv}(hsk, x_i)$	$\quad K_i = \mathsf{SecEv}(hsk, x_i)$
For $i = k+1$ to $2k$:	$hsk' \leftarrow \mathsf{SampHsk}(hsk, \mathsf{td}, x_1, \cdots, x_{2k})$
$\quad K_i \leftarrow \mathcal{K}_{sp}$	Return $(hsk', hpk, K_1, \cdots, K_{2k})$
Return $(hsk, hpk, K_1, \cdots, K_{2k})$	

Fig. 4 Distributions for defining key equivocability of HPS.

Instantiation from DDH. Now we present our instantiation of universal$_\kappa$ HPS with key equivocability from the DDH assumption. The definition of the DDH assumption will be recalled in Appendix A.

Let λ be the security parameter and let k, κ be positive integers that are polynomial in λ. Let $\mathbb{G}$ be a multiplicative cyclic group of prime order q and let g be a generator of $\mathbb{G}$. Let $\Gamma : \mathbb{G}^{2k+1} \to \mathbb{Z}_q^{2k+1}$ be an injective function, which can be extended from the injective function in the constructions of HPS in [8] directly.

We construct a strengthened subset membership problem $\mathsf{SSMP}_1 = (\mathsf{SSmpG}, \mathsf{SSmpX}, \mathsf{SSmpL}, \mathsf{SSmpLS}, \mathsf{SSmpChk})$ as follows:

- SSmpG. On input a security parameter λ and an integer k, the parameter generation algorithm first samples $a_i \leftarrow \mathbb{Z}_q$ and computes $g_i = g^{a_i}$ for $i \in [2k+1]$. Then it sets:

$$\mathcal{X} = \{u_1, \ldots, u_{2k+1} \mid \forall i \in [2k+1], u_i \in \mathbb{G}\}$$

$$\mathcal{L} = \{g_1^w, \ldots, g_{2k+1}^w \mid w \in \mathbb{Z}_q\}$$

and for $i \in [2k]$, it sets:

$$\mathcal{L}_i = \{g_1^{w_1}, \ldots, g_{2k+1}^{w_{2k+1}} \mid w, w' \in \mathbb{Z}_q, w \neq w',$$

$w_i = w', \forall j \in [2k+1] \backslash \{i\}, w_j = w\}$

The public parameter $\mathsf{prm} = (\mathbb{G}, q, g, g_1, \ldots, g_{2k+1})$ and the trapdoor $\mathsf{td} = (a_1, \ldots, a_{2k+1})$

- SSmpX. On input a public parameter $\mathsf{prm} = (\mathbb{G}, q, g, g_1, \ldots, g_{2k+1})$, the algorithm samples $u_i \leftarrow \mathbb{G}$ for $i \in [2k+1]$ and outputs $x = (u_1, \ldots, u_{2k+1})$.
- SSmpL. On input a public parameter $\mathsf{prm} = (\mathbb{G}, q, g, g_1, \ldots, g_{2k+1})$, the algorithm samples $w \leftarrow \mathbb{Z}_q$ and outputs $x = (g_1^w, \ldots, g_{2k+1}^w)$ and the witness w.
- SSmpLS. On input a public parameter $\mathsf{prm} = (\mathbb{G}, q, g, g_1, \ldots, g_{2k+1})$ and an integer $i \in [2k]$, the algorithm samples $w \leftarrow \mathbb{Z}_q$ and $w' \leftarrow \mathbb{Z}_q$ s.t. $w \neq w'$. Then it computes $u_j = g_j^w$ for $j \in [2k+1] \backslash \{i\}$ and $u_i = g_i^{w'}$ and outputs $(u_1, \ldots, u_{2k+1})$.
- $\mathsf{SSmpChk}$. On input a public parameter $\mathsf{prm} = (\mathbb{G}, q, g, g_1, \ldots, g_{2k+1})$, a trapdoor $\mathsf{td} = (a_1, \ldots, a_{2k+1})$, and $x = (u_1, \ldots, u_{2k+1})$, the algorithm first computes $v_j = u_j^{a_j^{-1}}$ for $j \in [2k+1]$. It outputs 0 if $v_1 = v_2 = \ldots = v_{2k+1}$. It outputs j if there exists some $j \in [2k]$ s.t. $v_\jmath = v_{\jmath'}$ for all $\jmath, \jmath' \in [2k] \backslash \{j\}$ and $v_j \neq v_{2k+1}$. Otherwise, it outputs $\perp$.

Also, we construct the HPS $\mathsf{HPS}_1 = (\mathsf{PrmG}, \mathsf{PubEv}, \mathsf{SecEv}, \mathsf{SampHsk})$ for SSMP_1 as follows:

- PrmG. On input a public parameter $\mathsf{prm} = (\mathbb{G}, q, g, g_1, \ldots, g_{2k+1})$, the algorithm defines $\mathcal{K}_{sp} = \mathbb{G}$, $\mathcal{SK} = \mathbb{Z}_q^{(2k+1)\times\kappa\times(2k+1)}$, and $\mathcal{PK} = \mathbb{G}^{(2k+1)\times\kappa}$.
  Then for any $hsk = (s_{h,i,j})_{h\in[2k+1],i\in[\kappa],j\in[2k+1]} \in \mathcal{SK}$ and any $x = (u_1, \ldots, u_{2k+1}) \in \mathcal{X}$, it defines the map Λ from $\mathcal{SK} \times \mathcal{X}$ to $\mathcal{K}_{sp}$ as

$$\Lambda_{hsk}(x) = \prod_{h\in[2k+1],i\in[\kappa],j\in[2k+1]} u_j^{s_{h,i,j}\cdot\alpha_h^{i-1}}$$

  where $(\alpha_1, \ldots, \alpha_{2k+1}) = \Gamma(x)$. Also, for any $hsk = (s_{h,i,j})_{h\in[2k+1],i\in[\kappa],j\in[2k+1]} \in \mathcal{SK}$, it defines the map μ from $\mathcal{SK}$ to $\mathcal{PK}$ as

$$\mu(hsk) = (p_{h,i})_{h\in[2k+1],i\in[\kappa]} = (\prod_{j\in[2k+1]} g_j^{s_{h,i,j}})_{h\in[2k+1],i\in[\kappa]}$$

- SecEv. On input a secret key $hsk = (s_{h,i,j})_{h\in[2k+1],i\in[\kappa],j\in[2k+1]} \in \mathcal{SK}$ and $x = (u_1, \ldots, u_{2k+1}) \in \mathcal{X}$, the secret evaluation algorithm outputs $K = \Lambda_{hsk}(x)$.

– PubEv. On input a public key $hpk = (p_{h,i})_{h\in[2k+1],i\in[\kappa]} \in \mathcal{PK}$, $x = (u_1, \ldots, u_{2k+1}) \in \mathcal{L}$ and a witness w, the public evaluation algorithm computes $(\alpha_1, \ldots, \alpha_{2k+1}) = \Gamma(x)$ and outputs $K = \prod_{h\in[2k+1],i\in[\kappa]} p_{h,i}^{w\cdot\alpha_h^{i-1}}$.
– $\mathsf{SampHsk}$. On input a secret key $hsk = (s_{h,i,j})_{h\in[2k+1],i\in[\kappa],j\in[2k+1]}$, a trapdoor $\mathsf{td} = (a_1, \ldots, a_{2k+1})$, and $2k$ inputs $(x_\ell = (u_{\ell,1}, \ldots, u_{\ell,2k+1}))_{\ell\in[2k]}$, the algorithm works as follows:
  1. For $\ell \in [2k]$, it computes $\boldsymbol{p}[\ell] = \mathsf{SSmpChk}(\mathsf{prm}, \mathsf{td}, x_\ell)$.
  2. It outputs $\perp$ if there exists $\ell \in [2k]$ s.t. $\boldsymbol{p}[\ell] \notin [2k]$ or there exist distinct $\ell_1, \ell_2 \in [2k]$ s.t. $\boldsymbol{p}[\ell_1] = \boldsymbol{p}[\ell_2]$.
  3. For $h \in [2k+1], i \in [\kappa], j \in \{\boldsymbol{p}[1], \ldots, \boldsymbol{p}[k]\}$, it sets $s'_{h,i,j} = s_{h,i,j}$.
  4. For $h \in [2k+1], i \in [\kappa], j \in \{\boldsymbol{p}[k+1], \ldots, \boldsymbol{p}[2k]\}$, it samples $s'_{h,i,j} \leftarrow \mathbb{Z}_q$.
  5. For $h \in [2k+1], i \in [\kappa]$, it sets $s'_{h,i,2k+1} = (\sum_{j\in[2k+1]} a_j s_{h,i,j} - \sum_{j\in[2k]} a_j s'_{h,i,j}) \cdot a_{2k+1}^{-1}$.
  6. It outputs $hsk' = (s'_{h,i,j})_{h\in[2k+1],i\in[\kappa],j\in[2k+1]}$.

Theorem 1. *Assuming the DDH assumption holds,* SSMP_1 *is a strengthened subset membership problem with hardness, sparseness, explainability, and correctness.*

Theorem 2. HPS_1 *is a perfect universal*$_\kappa$ *HPS with key equivocability.*

Proofs of Theorem 1 and Theorem 2 are provided in the full version.

Instantiation from DCR. We present our instantiation of universal$_\kappa$ HPS with key equivocability from the DCR assumption as follows. The definition of the DCR assumption will be recalled in Appendix A.

Let λ be the security parameter and let k, κ be positive integers that are polynomial in λ. We construct a strengthened subset membership problem $\mathsf{SSMP}_2 = (\mathsf{SSmpG}, \mathsf{SSmpX}, \mathsf{SSmpL}, \mathsf{SSmpLS}, \mathsf{SSmpChk})$ as follows:

– SSmpG. On input a security parameter λ and an integer k, the parameter generation algorithm first samples primes p', q', p, q s.t. $p = 2p' + 1$ and $q = 2q' + 1$. Then it computes $N = pq$ and $N' = p'q'$. Let $\mathbb{Z}_{N^2}^* = \mathbb{G}_N \cdot \mathbb{G}_{N'} \cdot \mathbb{G}_2 \cdot \mathbb{T}$, where $\mathbb{G}_N, \mathbb{G}_{N'}, \mathbb{G}_2, \mathbb{T}$ are defined as in Appendix A. Define $\mathbb{X} = \mathbb{G}_N \cdot \mathbb{G}_{N'} \cdot \mathbb{T}$ and $\mathbb{L} = \mathbb{G}_{N'} \cdot \mathbb{T}$. Define $\chi : \mathbb{Z}_{N^2} \to \mathbb{Z}_N$ as $\chi(a) = \lfloor a/N \rfloor$. Let $\Gamma : \mathbb{X}^{2k} \to \mathbb{Z}_{\lfloor N^2/2 \rfloor}^{2k}$ be an injective function, which can be extended from the injective function in the constructions of HPS in [8] directly. Also, let $g \in \mathbb{Z}_{N^2}^*$ be a fixed generator of $\mathbb{L}$.

Then it sets:

$$\mathcal{X} = \{u_1, \ldots, u_{2k} \mid \forall j \in [2k], u_j \in \mathbb{X}\},$$

$$\mathcal{L} = \{g^{r_1}, \ldots, g^{r_{2k}} \mid \forall j \in [2k], r_j \in \mathbb{Z}_{2N'}\},$$

and for $i \in [2k]$, it sets:

$$\mathcal{L}_i = \{u_1, \ldots u_{2k} \mid u_i \in \mathbb{X}\backslash\mathbb{L}, \forall j \in [2k]\backslash\{i\}, r_j \in \mathbb{Z}_{2N'}, u_j = g^{r_j}\}.$$

The public parameter $\mathsf{prm} = (N, g)$ and the trapdoor $\mathsf{td} = N'$.

- SSmpX. On input a public parameter $\mathsf{prm} = (N, g)$, the algorithm samples $u_j \leftarrow \mathbb{X}$ for $j \in [2k]$ and outputs $x = (u_1, \ldots, u_{2k})$.
- SSmpL. On input a public parameter $\mathsf{prm} = (N, g)$, the algorithm samples $r_j \leftarrow \mathbb{Z}_{\lfloor N/2 \rfloor}$ for $j \in [2k]$ and outputs $x = (g^{r_1}, \ldots, g^{r_{2k}})$ and the witness $(r_1, \ldots, r_{2k})$.
- SSmpLS. On input a public parameter $\mathsf{prm} = (N, g)$ and an integer $i \in [2k]$, the algorithm samples $r_j \leftarrow \mathbb{Z}_{\lfloor N/2 \rfloor}$ for $j \in [2k]\backslash\{i\}$ and $u_i \leftarrow \mathbb{X}$. Then it computes $u_j = g^{r_j}$ for $j \in [2k]\backslash\{i\}$ and outputs $x = (u_1, \ldots, u_{2k})$.
- $\mathsf{SSmpChk}$. On input a public parameter $\mathsf{prm} = (N, g)$, a trapdoor $\mathsf{td} = N'$, and $x = (u_1, \ldots, u_{2k})$, the algorithm first computes $v_j = u_j^{2N'}$ for $j \in [2k]$. It outputs 0 if $v_1 = v_2 = \ldots v_{2k} = 1$. It outputs j if there exists $j \in [2k]$ s.t. $v_\jmath = 1$ for all $\jmath \in [2k]\backslash\{j\}$ and $v_j \neq 1$. Otherwise, it outputs $\perp$.

Also, we construct the HPS $\mathsf{HPS}_2 = (\mathsf{PrmG}, \mathsf{PubEv}, \mathsf{SecEv}, \mathsf{SampHsk})$ for SSMP_2 as follows:

- PrmG. On input a public parameter $\mathsf{prm} = (N, g)$, the algorithm defines $\mathcal{K}_{SP} = \mathbb{Z}_N$, $\mathcal{SK} = \mathbb{Z}_{\lfloor N^2/2 \rfloor}^{(2k)\times(\kappa)\times(2k)}$, and $\mathcal{PK} = \mathbb{L}^{(2k)\times(\kappa)\times(2k)}$. Then for any $hsk = (s_{h,i,j})_{h\in[2k],i\in[\kappa],j\in[2k]} \in \mathcal{SK}$ and any $x = (u_1, \ldots, u_{2k}) \in \mathcal{X}$, it defines the map Λ from $\mathcal{SK} \times \mathcal{X}$ to $\mathcal{K}_{sp}$ as

$$\Lambda_{hsk}(x) = \chi\Big(\prod_{h\in[2k],i\in[\kappa],j\in[2k]} u_j^{s_{h,i,j}\cdot\alpha_h^{i-1}}\Big)$$

where $(\alpha_1, \ldots, \alpha_{2k}) = \Gamma(x)$. Also, for any $hsk = (s_{h,i,j})_{h\in[2k],i\in[\kappa],j\in[2k]} \in \mathcal{SK}$, it defines the map μ from $\mathcal{SK}$ to $\mathcal{PK}$ as

$$\mu(sk) = (p_{h,i,j})_{h\in[2k],i\in[\kappa],j\in[2k]} = (g^{s_{h,i,j}})_{h\in[2k],i\in[\kappa],j\in[2k]}.$$

– SecEv. On input a secret key $hsk = (s_{h,i,j})_{h\in[2k],i\in[\kappa],j\in[2k]} \in \mathcal{SK}$ and $x = (u_1, \ldots, u_{2k}) \in \mathcal{X}$, the secret evaluation algorithm outputs $K = \Lambda_{hsk}(x)$.
– PubEv. On input a public key $hpk = (p_{h,i,j})_{h\in[2k],i\in[\kappa],j\in[2k]} \in \mathcal{PK}$, $x = (u_1, \ldots, u_{2k}) \in \mathcal{L}$ and a witness $(r_1, \ldots, r_{2k})$, the public evaluation algorithm computes $(\alpha_1, \ldots, \alpha_{2k}) = \Gamma(x)$ and outputs $K = \chi(\prod_{h\in[2k],i\in[\kappa],j\in[2k]} p_{h,i,j}^{r_j\cdot\alpha_h^{i-1}})$.
– $\mathsf{SampHsk}$. On input a secret key $hsk = (s_{h,i,j})_{h\in[2k],i\in[\kappa],j\in[2k]}$, a trapdoor $\mathsf{td} = N'$, and $2k$ inputs $(x_\ell = (u_{\ell,1}, \ldots, u_{\ell,2k}))_{\ell\in[2k]}$, the algorithm works as follows:
  1. For $\ell \in [2k]$, it computes $\boldsymbol{p}[\ell] = \mathsf{SSmpChk}(\mathsf{prm}, \mathsf{td}, x_\ell)$.
  2. It outputs $\perp$ if there exists $\ell \in [2k]$ s.t. $\boldsymbol{p}[\ell] \notin [2k]$ or there exist distinct $\ell_1, \ell_2 \in [2k]$ s.t. $\boldsymbol{p}[\ell_1] = \boldsymbol{p}[\ell_2]$.
  3. For $h \in [2k], i \in [\kappa], j \in \{\boldsymbol{p}[1], \ldots, \boldsymbol{p}[k]\}$, it sets $s'_{h,i,j} = s_{h,i,j}$.
  4. For $h \in [2k], i \in [\kappa], j \in \{\boldsymbol{p}[k+1], \ldots, \boldsymbol{p}[2k]\}$, it samples $t \leftarrow \mathbb{Z}_N$ and uses the Chinese remainder theorem to compute $s'_{h,i,j} \in \mathbb{Z}_{2NN'}$ s.t. $s'_{h,i,j} = t \mod N$ and $s'_{h,i,j} = s_{h,i,j} \mod 2N'$.
  5. It outputs $hsk' = (s'_{h,i,j})_{h\in[2k],i\in[\kappa],j\in[2k]}$.

Theorem 3. *Assuming the DCR assumption holds,* SSMP_2 *is a strengthened subset membership problem with hardness, sparseness, explainability, and correctness.*

Theorem 4. HPS_2 *is a perfect universal*$_\kappa$ *HPS with key equivocability.*

Proofs of Theorem 3 and Theorem 4 are similar to proofs of Theorem 1 and Theorem 2. So, we omit the details here. Note that SSMP_2 only achieves a statistical sampling correctness while SSMP_1 achieves a perfect sampling correctness.

4.3 SIM-wBi-SO$_k$-CCA Secure PKE Construction

For any polynomially bounded function $k > 0$, we propose a PKE scheme achieving SIM-wBi-SO$_k$-CCA security. Our construction is built from a perfectly universal$_{k+1}$ HPS with key-equivocability, and a strong and semi-unique XAC. The details are as follows.

Let $\mathsf{SSMP} = (\mathsf{SSmpG}, \mathsf{SSmpX}, \mathsf{SSmpL}, \mathsf{SSmpLS}, \mathsf{SSmpChk})$ be a hard SSMP. Let $\mathsf{HPS} = (\mathsf{PrmG}, \mathsf{PubEv}, \mathsf{SecEv}, \mathsf{SampHsk})$ be a perfectly universal$_{k+1}$ and key equivocable HPS for SSMP, such that all the $\mathcal{K}_{sp}$ generated by PrmG can be written as $\mathcal{K}_a \times \mathcal{K}_b$. For $\ell \in \mathbb{N}$ and any $\mathsf{prmins} = (\mathcal{K}_{sp}, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \mu)$ generated by PrmG, let $\mathsf{XAC}_{\mathsf{prmins}} = (\mathsf{XGen}, \mathsf{XAuth}, \mathsf{XVer}, \mathsf{ReSamp})$ be a strong and semi-unique $(\ell+1)$-XAC with key space $\mathcal{XK} =$

$\mathcal{K}_{sp} = \mathcal{K}_a \times \mathcal{K}_b$ and tag space $\mathcal{XT}$, and $\mathcal{H}_{\mathsf{prmins}} : (\mathcal{X} \times \mathcal{PK})^\ell \to \mathcal{K}_b$ be a family of collision-resistant hash functions. Our PKE scheme $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ (for ℓ-bit messages) is defined in Fig. 5.

$\underline{\mathsf{Setup}(1^\lambda)}$:
$(\mathsf{prm} := (\mathcal{X}, \mathcal{L}, \mathcal{L}_1, \cdots, \mathcal{L}_{2k}), \mathsf{td}) \leftarrow \mathsf{SSmpG}(1^\lambda, k)$
$\mathsf{prmins} = (\mathcal{K}_{sp} = \mathcal{K}_a \times \mathcal{K}_b, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \mu) \leftarrow \mathsf{PrmG}(\mathsf{prm})$; $\mathsf{H} \leftarrow \mathcal{H}_{\mathsf{prmins}}$; $K_a \leftarrow \mathcal{K}_a$
Return $\mathsf{pp} := (\mathsf{prm}, \mathsf{prmins}, \mathsf{H}, K_a)$

$\underline{\mathsf{Gen}(\mathsf{pp})}$:
Parse $\mathsf{prmins} = (\mathcal{K}_{sp}, \mathcal{SK}, \mathcal{PK}, \mathcal{T}, \Lambda_{(\cdot)}, \mu)$
$(hsk_\gamma)_{\gamma\in[\ell]} \leftarrow (\mathcal{SK})^\ell$; $(hpk_\gamma = \mu(hsk_\gamma))_{\gamma\in[\ell]}$; $pk := (hpk_\gamma)_{\gamma\in[\ell]}$; $sk := (hsk_\gamma)_{\gamma\in[\ell]}$
Return (pk, sk)

$\underline{\mathsf{Enc}(pk = (hpk_\gamma)_{\gamma\in[\ell]}, m)}$:
Parse $m = (m_1, \cdots, m_\ell) \in \{0,1\}^\ell$
$r := (r_\gamma^{(\mathcal{X})}, r_\gamma^{(\mathcal{K})}, w_\gamma)_{\gamma\in[\ell]} \leftarrow (\mathcal{R}_{\mathsf{SSmpX}} \times \mathcal{R}_{\mathsf{Sample}} \times \mathcal{R}_{\mathsf{SSmpL}})^\ell$
For $\gamma = 1$ to ℓ :
  If $m_\gamma = 0$: $x_\gamma \leftarrow \mathsf{SSmpX}(\mathsf{prm}; r_\gamma^{(\mathcal{X})})$; $K_\gamma \leftarrow \mathsf{Sample}(\mathcal{K}_{sp}; r_\gamma^{(\mathcal{K})})$
  If $m_\gamma = 1$: $x_\gamma \leftarrow \mathsf{SSmpL}(\mathsf{prm}; w_\gamma)$; $K_\gamma = \mathsf{PubEv}(hpk_\gamma, x_\gamma, w_\gamma)$
$K_b = \mathsf{H}(pk, x_1, \cdots, x_\ell)$; $K_{\ell+1} = (K_a, K_b)$; $T = \mathsf{XAuth}(K_1, \cdots, K_{\ell+1})$
Return $c = (x_1, \cdots, x_\ell, T)$

$\underline{\mathsf{Dec}(sk = (hsk_\gamma)_{\gamma\in[\ell]}, c = (x_1, \cdots, x_\ell, T))}$:
$\overline{K}_b = \mathsf{H}(pk, x_1, \cdots, x_l)$
If $\mathsf{XVer}((K_a, \overline{K}_b), T) = 0$: $\overline{m}_1 = \cdots = \overline{m}_\ell = 0$; return $\overline{m} = (\overline{m}_1, \cdots, \overline{m}_\ell)$
For $\gamma = 1$ to ℓ :
  $\overline{K}_\gamma = \mathsf{SecEv}(hsk_\gamma, x_\gamma)$; $\overline{m}_\gamma = \mathsf{XVer}(\overline{K}_\gamma, T)$
Return $\overline{m} = (\overline{m}_1, \cdots, \overline{m}_\ell)$

Fig. 5 Construction of PKE.

Correctness. For $\gamma \in [\ell]$, if $m_\gamma = 1$, then $\overline{K}_\gamma = K_\gamma$ by completeness of HPS, so $\overline{m}_\gamma = \mathsf{Xver}(\overline{K}_\gamma, \gamma, T) = 1$ except with probability $\mathsf{fail}_{\mathsf{XAC}}(\lambda)$ by correctness of XAC. On the other hand, if $m_\gamma = 0$, subset sparseness of SSMP and perfect universality of HPS guarantee that with overwhelming probability, $\overline{K}_\gamma$ is uniformly random, even given pk, c and m. In this case, $\overline{m}_\gamma = \mathsf{XVer}(\overline{K}_\gamma, T) = 0$ except with probability $\mathtt{Adv}^{\mathrm{IMP}}_{\mathsf{XAC}}(\lambda)$. So, correctness of PKE follows by a union bound over $\gamma \in [\ell]$.

Security. Formally, we have the following theorem, the formal proof of which is provided in the full version.

Theorem 5. *For any polynomial function $k > 0$,* PKE *is SIM-wBi-SO$_k$-CCA secure.*

5 PKE with SIM-Bi-SO-CCA Security

In [14], Heuer et al. showed that a generic construction of DHIES [31] meets SIM-SSO-CCA security in the random oracle model. In this section, we show that a variant of the generic construction actually achieves SIM-Bi-SO-CCA security in the random oracle model.

Building blocks. We simply recall the definitions of key encapsulation mechanism (KEM) and message authentication code (MAC) as follows.

Key Encapsulation Mechanism. A KEM scheme, associated with a session key space $\mathcal{K}_{\mathsf{KEM}}$ and a ciphertext space $\mathcal{C}_{\mathsf{KEM}}$, is a tuple of PPT algorithms $\mathsf{KEM} = (\mathsf{KemGen}, \mathsf{Encap}, \mathsf{Decap})$. The key generation algorithm KemGen takes 1^λ as input, and outputs a public/secret key pair (pk, sk). The encapsulation algorithm Encap takes pk as input, outputs $(K, c) \in \mathcal{K}_{\mathsf{KEM}} \times \mathcal{C}_{\mathsf{KEM}}$. The decapsulation algorithm Decap, taking sk and c as input, outputs a value in $\mathcal{K}_{\mathsf{KEM}} \cup \{\perp\}$. Standard correctness is required. Similar to [14], without loss of generality we assume that Encap uniformly samples $K \leftarrow \mathcal{K}_{\mathsf{KEM}}$. We also assume that $|\mathcal{K}_{\mathsf{KEM}}| \geq 2^\lambda$ and $|\mathcal{C}_{\mathsf{KEM}}| \geq 2^\lambda$.

We say that KEM has *unique encapsulations*, if for any (pk, sk) generated by KemGen, and for any ciphertexts c, c' satisfying $\mathsf{Decap}(sk, c) = \mathsf{Decap}(sk, c') \neq \perp$, $c = c'$.

The security notion, one-way security in the presence of a plaintext-checking oracle (OW-PCA security) [28], is recalled in the full version.

Message Authentication Code. A MAC scheme, associated with a key space $\mathcal{K}_{\mathsf{MAC}}$, is a tuple of PPT algorithms $\mathsf{MAC} = (\mathsf{MacGen}, \mathsf{Auth}, \mathsf{Verf})$. The key generation algorithm MacGen takes 1^λ as input and outputs a key $K \in \mathcal{K}_{\mathsf{MAC}}$. The authentication algorithm Auth takes K and a message m as input, outputs a tag t. On input (K, m, t), the verification algorithm Verf outputs a bit $b' \in \{0, 1\}$. Standard correctness is also required here.

MAC is called deterministic, if Auth is deterministic. For a deterministic MAC, MAC is called *injective*, if Auth is an injective function (i.e., for any $K \in \mathcal{K}_{\mathsf{MAC}}$ and any $m \neq m'$, $\mathsf{Auth}(K, m) \neq \mathsf{Auth}(K, m')$).

The security notion of strong unforgeability under one-time chosen message attacks (sUF-OT-CMA security) is recalled in the full version.

PKE Construction. Let $\mathsf{KEM} = (\mathsf{KemGen}, \mathsf{Encap}, \mathsf{Decap})$ be an OW-PCA secure KEM scheme, having unique encapsulations, associated with

$\underline{\mathsf{Setup}(1^\lambda):}$
Return $\mathsf{pp} := 1^\lambda$

$\underline{\mathsf{Gen}(\mathsf{pp} = 1^\lambda):}$
$(pk^{kem}, sk^{kem}) \leftarrow \mathsf{KemGen}(1^\lambda);\ pk := pk^{kem};\ sk := (pk^{kem}, sk^{kem})$
Return (pk, sk)

$\underline{\mathsf{Enc}(pk = pk^{kem}, m):}$
$r \leftarrow \mathcal{R}_{\mathsf{Encap}};\ (K, c^{kem}) \leftarrow \mathsf{Encap}(pk^{kem}; r);\ (K^{sym}, K^{mac}) = \mathsf{H}_{\mathrm{RO}}(K)$
$c^{sym} = K^{sym} \oplus m;\ t = \mathsf{Auth}(K^{mac}, (pk^{kem}, c^{kem}, c^{sym}))$
Return $c = (c^{kem}, c^{sym}, t)$

$\underline{\mathsf{Dec}(sk = (pk^{kem}, sk^{kem}), c = (c^{kem}, c^{sym}, t)):}$
$\overline{K} = \mathsf{Decap}(sk^{kem}, c^{kem});\ (\overline{K}^{sym}, \overline{K}^{mac}) = \mathsf{H}_{\mathrm{RO}}(\overline{K})$
If $\mathsf{Verf}(\overline{K}^{mac}, (pk^{kem}, c^{kem}, c^{sym}), t) = 0$: return $\perp$
Return $\overline{m} = c^{sym} \oplus \overline{K}^{sym}$

Fig. 6 Construction of $\mathsf{PKE}_{\mathsf{K\text{-}M}}$.

a session key space $\mathcal{K}_{\mathsf{KEM}}$ and a ciphertext space $\mathcal{C}_{\mathsf{KEM}}$, where Encap uniformly samples K, $|\mathcal{K}_{\mathsf{KEM}}| \geq 2^\lambda$ and $|\mathcal{C}_{\mathsf{KEM}}| \geq 2^\lambda$. Let $\mathsf{MAC} = (\mathsf{MacGen}, \mathsf{Auth}, \mathsf{Verf})$ be a deterministic, injective MAC scheme, associated with a key space $\mathcal{K}_{\mathsf{MAC}}$, achieving sUF-OT-CMA security. Let $\mathsf{H}_{\mathrm{RO}} : \mathcal{K}_{\mathsf{KEM}} \to \{0,1\}^\ell \times \mathcal{K}_{\mathsf{MAC}}$ be a hash function. Our PKE scheme $\mathsf{PKE}_{\mathsf{K\text{-}M}} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, associated with a message space $\{0,1\}^\ell$, is defined in Fig. 6.

The correctness analysis of this scheme is trivial. Now we turn to its security analysis. Formally, we have the following theorem. Note that, in our construction, a valid ciphertext contains a tag t generated on $(pk^{kem}, c^{kem}, c^{sym})$, where in [14], the tag t is only generated on c^{sym}. We stress that this crucial modification makes our construction achieve SIM-Bi-SO-CCA security. The intuition for the security proof and details are provided in the full version.

Theorem 6. *If* KEM *has unique encapsulations and is OW-PCA secure,* MAC *is deterministic, injective and sUF-OT-CMA secure, and* H_{RO} *is modeled as a random oracle, then* $\mathsf{PKE}_{\mathsf{K\text{-}M}}$ *is SIM-Bi-SO-CCA secure in the random oracle model.*

Acknowledgment. We thank Fangguo Zhang for the helpful discussions. We appreciate the anonymous reviewers for their valuable comments. This work was supported by the National Natural Science Foundation of China (Grant Nos. 61922036, U2001205, 61702125, 61802078, 61825203, U1736203, 61732021), Major Program of Guangdong Basic and Applied Research (Grant No. 2019B030302008), National Key Research

and Development Plan of China (Grant No. 2020YFB1005600), Guangdong Provincial Science and Technology Project (Grant No. 2017B010111005), and National Joint Engineering Research Center for Network Security Detection and Protection Technology.

References

1. Mihir Bellare, Alexandra Boldyreva, and Silvio Micali. Public-key encryption in a multi-user setting: Security proofs and improvements. In *EUROCRYPT*, pages 259–274. Springer, 2000.
2. Mihir Bellare, Rafael Dowsley, Brent Waters, and Scott Yilek. Standard security does not imply security against selective-opening. In *EUROCRYPT*, pages 645–662. Springer, 2012.
3. Mihir Bellare, Dennis Hofheinz, and Scott Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. In *EUROCRYPT*, pages 1–35. Springer, 2009.
4. Mihir Bellare and Scott Yilek. Encryption schemes secure under selective opening attack. Cryptology ePrint Archive, Report 2009/101, 2009. `https://eprint.iacr.org/2009/101`.
5. Xavier Boyen and Qinyi Li. All-but-many lossy trapdoor functions from lattices and applications. In *CRYPTO*, pages 298–331. Springer, 2017.
6. Ran Canetti, Shai Halevi, and Jonathan Katz. Adaptively-secure, non-interactive public-key encryption. In *TCC*, pages 150–168. Springer, 2005.
7. Ronald Cramer and Victor Shoup. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In *CRYPTO*, pages 13–25. Springer, 1998.
8. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT*, pages 45–64. Springer, 2002.
9. Serge Fehr, Dennis Hofheinz, Eike Kiltz, and Hoeteck Wee. Encryption schemes secure against chosen-ciphertext selective opening attacks. In *EUROCRYPT*, pages 381–402. Springer, 2010.
10. Oded Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.
11. Keisuke Hara, Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka. Simulation-based receiver selective opening cca secure pke from standard computational assumptions. In *Security and Cryptography for Networks*, pages 140–159. Springer, 2018.
12. Carmit Hazay, Arpita Patra, and Bogdan Warinschi. Selective opening security for receivers. In *ASIACRYPT*, pages 443–469. Springer, 2015.
13. Brett Hemenway, Benoît Libert, Rafail Ostrovsky, and Damien Vergnaud. Lossy encryption: Constructions from general assumptions and efficient selective opening chosen ciphertext security. In *ASIACRYPT*, pages 70–88. Springer, 2011.
14. Felix Heuer, Tibor Jager, Eike Kiltz, and Sven Schäge. On the selective opening security of practical public-key encryption schemes. In *PKC*, pages 27–51. Springer, 2015.
15. Felix Heuer and Bertram Poettering. Selective opening security from simulatable data encapsulation. In *ASIACRYPT*, pages 248–277. Springer, 2016.

16. Dennis Hofheinz. All-but-many lossy trapdoor functions. In *EUROCRYPT*, pages 209–227. Springer, 2012.
17. Dennis Hofheinz, Vanishree Rao, and Daniel Wichs. Standard security does not imply indistinguishability under selective opening. In *TCC*, pages 121–145. Springer, 2016.
18. Dennis Hofheinz and Andy Rupp. Standard versus selective opening security: Separation and equivalence results. In *TCC*, pages 591–615. Springer, 2014.
19. Zhengan Huang, Junzuo Lai, Wenbin Chen, Man Ho Au, Zhen Peng, and Jin Li. Simulation-based selective opening security for receivers under chosen-ciphertext attacks. *Designs, Codes and Cryptography*, 87(6):1345–1371, 2019.
20. Zhengan Huang, Shengli Liu, and Baodong Qin. Sender-equivocable encryption schemes secure against chosen-ciphertext attacks revisited. In *PKC*, pages 369–385. Springer, 2013.
21. Dingding Jia and Benoît Libert. So-cca secure pke from pairing based all-but-many lossy trapdoor functions. *Designs, Codes and Cryptography*, 89(5):895–923, 2021.
22. Dingding Jia, Xianhui Lu, and Bao Li. Receiver selective opening security from indistinguishability obfuscation. In *INDOCRYPT*, pages 393–410. Springer, 2016.
23. Dingding Jia, Xianhui Lu, and Bao Li. Constructions secure against receiver selective opening and chosen ciphertext attacks. In *CT-RSA*, pages 417–431. Springer, 2017.
24. Junzuo Lai, Robert H. Deng, Shengli Liu, Jian Weng, and Yunlei Zhao. Identity-based encryption secure against selective opening chosen-ciphertext attack. In *EUROCRYPT*, pages 77–92. Springer, 2014.
25. Benoît Libert, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. All-but-many lossy trapdoor functions and selective opening chosen-ciphertext security from lwe. In *CRYPTO*, pages 332–364. Springer, 2017.
26. Shengli Liu and Kenneth G. Paterson. Simulation-based selective opening cca security for pke from key encapsulation mechanisms. In *PKC*, pages 3–26. Springer, 2015.
27. Lin Lyu, Shengli Liu, Shuai Han, and Dawu Gu. Tightly sim-so-cca secure public key encryption from standard assumptions. In *PKC*, pages 62–92. Springer, 2018.
28. Tatsuaki Okamoto and David Pointcheval. React: Rapid enhanced-security asymmetric cryptosystem transform. In *CT-RSA*, pages 159–174. Springer, 2001.
29. Adam O'Neill, Chris Peikert, and Brent Waters. Bi-deniable public-key encryption. In *CRYPTO*, pages 525–542. Springer, 2011.
30. Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *EUROCRYPT*, pages 223–238. Springer, 1999.
31. Ron Steinfeld, Joonsang Baek, and Yuliang Zheng. On the necessity of strong assumptions for the security of a class of asymmetric encryption schemes. In *ACISP*, pages 241–256. Springer, 2002.
32. Rupeng Yang, Junzuo Lai, Zhengan Huang, Man Ho Au, Qiuliang Xu, and Willy Susilo. Possibility and impossibility results for receiver selective opening secure pke in the multi-challenge setting. In *ASIACRYPT*, pages 191–220. Springer, 2020.

A Cryptographic Assumptions

The DDH Assumption. Let $\mathbb{G}$ be a cyclic group of prime order q with a generator g. The DDH assumption requires that it is hard to distinguish (g^a, g^b, g^c) and (g^a, g^b, g^{ab}), where $a, b, c \leftarrow \mathbb{Z}_q$.

The DCR Assumption. Now, we recall the Decision Composite Residuosity (DCR) assumption [30] and some useful facts about it shown in [8].

Let p, q, p', q' be primes such that $p = 2p' + 1$ and $q = 2q' + 1$. Let $N = pq$ and $N' = p'q'$. Then the group $\mathbb{Z}_{N^2}^*$ can be decomposed as the direct product $\mathbb{G}_N \cdot \mathbb{G}_{N'} \cdot \mathbb{G}_2 \cdot \mathbb{T}$, where $\mathbb{G}_{N'}$ and $\mathbb{G}_2$ are cyclic groups of order N' and order 2 respectively; $\mathbb{G}_N$ is a cyclic group of order N generated by $\xi = (1 + N) \mod N^2$; and $\mathbb{T}$ is the order-2 subgroup of $\mathbb{Z}_{N^2}^*$ generated by $(-1 \mod N^2)$. Note that $\xi^a = (1 + aN) \mod N^2$ for $a \in \{0, 1, \cdots, N\}$.

The DCR assumption requires that it is hard to distinguish a random element in $\mathbb{Z}_{N^2}^*$ and a random element in $\mathbb{G}_{N'} \cdot \mathbb{G}_2 \cdot \mathbb{T}$.

Next, define $\mathbb{X} = \mathbb{G}_N \cdot \mathbb{G}_{N'} \cdot \mathbb{T}$. The set $\mathbb{X}$ is an efficiently samplable and explainable domain, where the sample algorithm and the explain algorithm work as follows:

- Sample: The sample algorithm proceeds as follows:
  1. For $i \in [1, 160]$:
     (a) $x \leftarrow \mathbb{Z}_{N^2}$
     (b) If the Jacobi symbol $(\frac{x}{N}) = 1$: **output** x.
  2. **Output** $\perp$.
- Explain: on input an element $x \in \mathbb{X}$, the explain algorithm proceeds as follows:
  1. Set r to be an empty string.
  2. For $i \in [1, 160]$:
     (a) Sample $b \leftarrow \{0, 1\}$.
     (b) If $b = 1$, append x to r and **outputs** r.
     (c) Otherwise, sample an element $x' \leftarrow \mathbb{Z}_{N^2}$ s.t. the Jacobi symbol $(\frac{x'}{N}) = -1$ and append x' to r.
  3. **Output** $\perp$.

Note that as $\frac{|\mathbb{X}|}{|\mathbb{Z}_{N^2}^*|} = 1/2$, the expected repetition in the sample algorithm is about 2 and the probability that the sample algorithm outputs $\perp$ is $\frac{1}{2^{160}}$, which is negligible. Also, it is easy to see the probability that the explain algorithm outputs $\perp$ is also $\frac{1}{2^{160}}$, which is negligible.

Also, define $\chi : \mathbb{Z}_{N^2} \to \mathbb{Z}_N$ as $\chi(a) = \lfloor a/N \rfloor$. For any fixed $x \in \mathbb{X}$, $\chi(x\xi^c)$ is uniform in $\mathbb{Z}_N$ if $c \leftarrow \mathbb{Z}_N$.

Finally, define $\mathbb{L} = \mathbb{G}_{N'} \cdot \mathbb{T}$. It is easy to create a generator g for $\mathbb{L}$ by first sampling a random element $\mu \in \mathbb{Z}_{N^2}^*$ and then computing $g = -\mu^{2N}$. Besides, the DCR assumption implies that a random element in $\mathbb{X}$ is computationally indistinguishable from a random element in $\mathbb{L}$.