Anonymous Public Key Encryption under Corruptions

Zhengan Huang[1], Junzuo Lai[2(✉)], Shuai Han[3(✉)], Lin Lyu[4(✉)], and Jian Weng[2]

[1] Peng Cheng Laboratory, Shenzhen, China
zhahuang.sjtu@gmail.com
[2] College of Information Science and Technology, Jinan University, Guangzhou, China
{laijunzuo,cryptjweng}@gmail.com
[3] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China
dalen17@sjtu.edu.cn
[4] Bergische Universität Wuppertal, Wuppertal, Germany
lin.lyu@uni-wuppertal.de

Abstract. Anonymity of public key encryption (PKE) requires that, in a multi-user scenario, the PKE ciphertexts do not leak information about which public keys are used to generate them. Corruptions are common threats in the multi-user scenario but anonymity of PKE under corruptions is less studied in the literature. In TCC 2020, Benhamouda et al. first provide a formal characterization for anonymity of PKE under a specific type of corruption. However, no known PKE scheme is proved to meet their characterization.

To the best of our knowledge, all the PKE application scenarios which require anonymity also require confidentiality. However, in the work by Benhamouda et al., different types of corruptions for anonymity and confidentiality are considered, which can cause security pitfalls. What's worse, we are not aware of any PKE scheme which can provide both anonymity and confidentiality under the same types of corruptions.

In this work, we introduce a new security notion for PKE called ANON-RSO$_k$&C security, capturing anonymity under corruptions. We also introduce SIM-RSO$_k$&C security which captures confidentiality under the same types of corruptions. We provide a generic framework of constructing PKE scheme which can achieve the above two security goals simultaneously based on a new primitive called key and message non-committing encryption (KM-NCE). Then we give a general construction of KM-NCE utilizing a variant of hash proof system (HPS) called Key-Openable HPS. We also provide Key-Openable HPS instantiations based on the matrix decisional Diffie-Hellman assumption. Therefore, we can obtain various concrete PKE instantiations achieving the two security goals in the standard model with *compact* ciphertexts. Furthermore, for some PKE instantiation, its security reduction is *tight*.

1 Introduction

Anonymity of PKE under corruptions. The (single-user) IND-CCA security has been the de facto standard security for public-key encryption (PKE) schemes and is the target security of NIST PKE standardization for the next decades. It provides message confidentiality under CCA attacks. Meanwhile, *anonymity* is another security requirement for PKE and is not provided by the IND-CCA security. Roughly speaking, anonymity of PKE requires that, in a multi-user scenario, the PKE ciphertexts do not leak information about which public keys are used to generate them. The IK-CPA/CCA security given by Bellare et al. [2] is the first formalization of anonymity of PKE.

In such multi-user scenarios, multiple key pairs are generated, potentially correlated plaintexts are encrypted and sent to many receivers. Both the secret keys and the encrypted messages could be leaked due to accidents and/or adversarial attacks, which affects both the confidentiality and the anonymity of the PKE scheme. Researchers capture such threats by formalizing different types of *corruptions* in different multi-user scenarios. Many efforts have been made to establish confidentiality under corruptions and the study to selective-opening attacks are such examples.

However, anonymity of PKE under corruptions is much less studied. To the best of our knowledge, it is not considered until recently by Benhamouda et al. [5] in TCC 2020. They propose anonymity against selective-opening for PKE which is the first (and, to the best of our knowledge, also the only) formal definition of anonymity for PKE under corruptions. We will call this security as ANON-COR (anonymity under corruptions) security in this work. The ANON-COR security defined in [5] is as follows. Given n public keys of n users, an adversary submits t messages of its choice, and then receives t challenge ciphertexts, which are encryptions of the t messages under t distinct random public keys out of the n user public keys. Next, the adversary can adaptively corrupt $Q < n$ users one at a time, obtaining their secret keys. (We will call such kind of corruption as *post-challenge user corruption*.) ANON-COR security requires that no feasible adversary can corrupt more than $\frac{Q}{n} + \epsilon$ (for some constant $\epsilon > 0$) fraction of the ciphertext-encrypting keys with non-negligible probability.

Unfortunately, no known PKE scheme is proved to have ANON-COR security. Actually, Benhamouda et al. [5] only prove that their suggested PKE scheme achieves a simplified version of ANON-COR security (where the adversary is restricted to corrupt some users at once) and conjecture that it also achieves the ANON-COR security. They leave constructing an ANON-COR secure PKE scheme as an interesting problem.

Furthermore, we think the ANON-COR security is restricted in the following sense.

- Non-adaptive. The ANON-COR security is non-adaptive in the sense that the adversary is *not* allowed to obtain any user secret key *before* seeing the challenge ciphertexts. This restricts its application scenario since, in the real-world, some users may be fully controlled by the adversary from the very beginning and the adversary may corrupt other users at any time.

– Single-challenge. The ANON-COR security considers a single-challenge setting where each public key is used *only once* to encrypt a single challenge message. This restriction limits its application scenario since, in practice, each public key is often used multiple times (for example, the application scenario in [5][1]).

Thus, we raise the following research question.

> *Q1: For PKE schemes, can we provide an achievable security formalization which provides anonymity under more adaptive corruptions in the multi-challenge setting?*

Anonymity and confidentiality under the same types of corruptions. We are not aware of any application scenario which only requires anonymity but not confidentiality of PKE schemes[2]. To the best of our knowledge, all the PKE application scenarios in the real world which require anonymity also require confidentiality. As an example, Benhamouda et al. [5] consider a blockchain application scenario which requires both of the two security guarantees. However, Benhamouda et al. capture the two security guarantees under *different* types of corruptions. More precisely, as shown in [5, Section 2.6], the scheme $\mathcal{E}_1$ requires both anonymity under post-challenge user corruption (ANON-COR security) and confidentiality under *the receiver selective opening (RSO)* corruption.

Although the ANON-COR security is called "anonymous against selective-opening" in [5], we want to note that the post-challenge user corruption considered in ANON-COR security is different from the RSO corruption considered for confidentiality. The RSO corruption [3,14] considers an adversary, after seeing many challenge ciphertexts for different receivers (together with their public keys), is able to open a subset of the challenge ciphertexts (via corrupting a subset of the receivers to obtain their secret keys and received messages). However, the ANON-COR adversary is not able to specify some challenge ciphertexts and open them.

When the two security guarantees (anonymity and confidentiality) are both required, it is more desirable to capture them under the *same* types of corruptions. Taking [5] as an example, where anonymity and confidentiality are both required for the scheme $\mathcal{E}_1$ in [5], it does not make sense for the adversary to attack anonymity *only* using the post-challenge user corruption and attack

[1] In the Committee-Selection phase of the evolving-committee proactive secret sharing scheme considered in [5], some users are selected as committee members. Each committee member will encrypt one fresh secret key using its long term public key ($\mathsf{ct} \leftarrow \mathcal{E}_1.\mathsf{Enc}_{\mathsf{pk}}(\mathsf{esk})$). Since the same user may be selected as a committee member multiple times, the user's public key may be used multiple times to encrypt multiple messages.

[2] Actually, it does not make sense to *only* consider the anonymity of some PKE without considering its confidentiality. If confidentiality can be sacrificed, one can trivially achieve anonymity by assigning the identity map as the encryption and decryption algorithm, so that the ciphertext equals the message and is independent of any public key.

confidentiality *only* using the RSO corruption. Actually, there is no anonymity guarantee under the RSO corruption and no confidentiality guarantee under the post-challenge user corruption. This implies that, when the adversary is able to use both post-challenge user corruption and RSO corruption, it is possible that neither anonymity nor confidentiality holds for the PKE scheme. Consequently, when the two security guarantees are required under corruptions, they should be captured under the same types of corruptions.

Unfortunately, we are not aware of any PKE schemes which can provide the two security guarantees under the same types of corruptions. Thus, we raise our second research question.

> *Q2: Can we construct a PKE scheme which provides both anonymity and confidentiality under the same types of corruptions?*

We answer the above two research questions affirmatively in this work.

Our contributions. In this work:

- We formalize the notion of *ANONymity under Receiver Selective Opening attacks (in the k-challenge setting), adaptive user Corruptions and Chosen Plaintext / Ciphertext Attacks*, which we call ANON-RSO$_k$&C-CPA/CCA security for short. To capture confidentiality under the same types of corruptions, we also formalize the notion of SIM-RSO$_k$&C-CPA/CCA security.
- We provide a generic framework of constructing PKE schemes, achieving both ANON-RSO$_k$&C-CCA security and SIM-RSO$_k$&C-CCA security (we denote them as AC-RSO$_k$&C-CCA security for simplicity), based on a new primitive called *key and message non-committing encryption* (KM-NCE).
- We give a general construction of KM-NCE utilizing a variant of hash proof system (HPS) [9] which we call *Key-Openable HPS*.
- Finally, we provide Key-Openable HPS instantiations from the matrix decisional Diffie-Hellman (MDDH) assumption [10].

When plugging the HPS instantiations into the general construction framework, we can obtain an AC-RSO$_k$&C-CCA secure PKE scheme in the standard model which provides anonymity and confidentiality simultaneously under both adaptive user corruptions and RSO corruptions. Moreover, our scheme enjoys the properties that 1) the ciphertext is *compact* (i.e., ciphertext overhead[3] is the size of a constant number of group elements [15], or more generally, is independent of the message length [12]), and 2) the security reduction is *tight*[4]. To the best of our knowledge, our scheme is the first PKE scheme achieving anonymity under adaptive corruptions (which is stronger than the ANON-COR security), thus solving the problem raised by Benhamouda et al. [5] in TCC 2020. Also, our scheme is the first PKE scheme achieving RSO$_k$-CCA security in the standard model with compact ciphertexts and tight security.

[3] Ciphertext overhead means the ciphertext bitlength minus plaintext bitlength [15].

[4] Tight reduction means that the security loss of the reduction is independent of the number of users, the number of challenges and the number of queries raised by the adversary.

AC-RSO$_k$&C security derived from KM-NCE. We take the approach of non-committing encryption [7,8,12] to achieve AC-RSO$_k$&C security. We introduce a new primitive called *key and message non-committing encryption* (KM-NCE), which is some kind of "message & public key-non-committing" encryption. Informally, KM-NCE allows one to generate fake ciphertexts via a fake encryption algorithm, and enables one to open k fake ciphertexts to any k messages under any public key (by showing an appropriate secret key) via an opening algorithm.

We formalize two security properties for KM-NCE. One is a single-user and k-challenge security notion called KMNC$_k$-CPA/CCA security (c.f., Definition 4), and the other is robustness (c.f., Definition 5). Intuitively, KMNC$_k$-CPA/CCA security requires that the real secret key together with k real ciphertexts (encrypting k messages chosen by the adversary) should be computationally indistinguishable from the opened secret key and k fake ciphertexts.

KM-NCE serves as our core technical tool, and we show that KMNC$_k$-CPA/CCA secure and robust KM-NCE implies AC-RSO$_k$&C-CPA/CCA secure PKE. Due to the relative simplicity of KMNC$_k$-CPA/CCA security (single-user, no simulator) in comparison to AC-RSO$_k$&C-CPA/CCA security (multi-user, simulation-based), it is easier and conceptually simpler to construct KM-NCE and prove its security first than constructing AC-RSO$_k$&C-CPA/CCA secure PKE directly.

Generic construction of KM-NCE. To construct KM-NCE, we propose a new building block called *Key-Openable HPS*, by equipping Hash Proof System (HPS) [9] with a hashing key opening algorithm HOpen_k. Informally, given k instances, k hash values and the random coins used to sample them, a projection key (public key of HPS), and a corresponding hashing key (secret key of HPS) as the input, HOpen_k can output another hashing key such that 1) the outputted hashing key corresponds to the same projection key and 2) the given k hash values are exactly hash values of the k instances under the outputted hashing key. We also define some new properties for the key-openable HPS, including *openability*$_k$ (c.f., Definition 9) and *universality*$_{k+1}$ (c.f., Definition 10). By using key-openable HPS as an essential building block, we present a generic construction of KMNC$_k$-CCA secure KM-NCE.

Instantiations. For concrete instantiations, we provide key-openable HPS instantiations based on the MDDH assumption. Due to the good versatility of the MDDH assumption, we can obtain various concrete instantiations of KM-NCE. Plugging the concrete instantiations into our general framework, we obtain AC-RSO$_k$&C-CCA secure PKE schemes with *compact* ciphertexts in the standard model. For some concrete PKE instantiation, we can even *tightly* prove its AC-RSO$_k$&C-CCA security.

Related works. The anonymity of PKE is first formalized by Bellare et al. [2] and they call it "key-privacy". Many follow up works continue research in this direction, such as [13,1,21]. Anonymity for PKE under corruptions is firstly considered by Benhamouda et al. [5].

The IND-CCA security in the multi-user setting with adaptive user corruptions except challenge is given in [4,20]. Lee et al. [20] propose the first PKE

scheme in the random oracle model with tight IND-CCA security reduction in the multi-user setting with adaptive user corruptions except challenge.

In the research area of receiver selective opening (RSO) corruption for PKE, Bellare et al. [3] point out that IND-CPA security does not imply SIM-RSO-CPA security. Hazay et al. [14] show that RSO security can be achieved from variants of non-committing encryption. Subsequent works [18,19,12,16] consider CCA security in the RSO setting and provide PKE schemes with RSO-CCA security. Yang et al. [23] consider RSO-CCA security in the multi-challenge setting. SIM-RSO-CCA secure PKE schemes with compact ciphertexts are proposed by Hara et al. [12] and Huang et al. [16].

2 Preliminaries

We assume that the security parameter λ is an (implicit) input to all algorithms. For any positive integer n, we use $[n]$ to denote the set $\{1, \cdots, n\}$. For a finite set $\mathcal{S}$, we use $|\mathcal{S}|$ to denote the size of $\mathcal{S}$. For random variables $\mathcal{X}$ and $\mathcal{Y}$ over a finite set $\mathcal{S}$, their statistical distance is $\Delta(\mathcal{X}, \mathcal{Y}) := \frac{1}{2} \sum_{s \in \mathcal{S}} |\Pr[\mathcal{X} = s] - \Pr[\mathcal{Y} = s]|$.

We recall the formal definitions of PKE, collision-resistant hash functions and universal hash functions together with the leftover hash lemma in the full version [17].

3 Anonymity and Confidentiality under Corruptions

In this section, we firstly introduce the notion of Anonymity under Receiver Selective Opening attacks (in the multi-challenge setting), adaptive user Corruptions and Chosen Plaintext / Ciphertext Attacks, which we call ANON-RSO$_k$&C-CPA/CCA security ($k \in \mathbb{N}$). Then, we introduce the notion of SIM-RSO$_k$&C-CPA/CCA security ($k \in \mathbb{N}$), to capture confidentiality under the same types of corruptions. Finally, we also introduce the notion of AC-RSO$_k$&C-CPA/CCA security, to capture ANON-RSO$_k$&C-CPA/CCA security and SIM-RSO$_k$&C-CPA/CCA security in one notion for convenience.

3.1 Anonymity under Corruptions

ANON-RSO$_k$&C security. We formalize a simulation-based anonymity definition under receiver selective opening attacks and adaptive user corruptions, which we call ANON-RSO$_k$&C security ($k \in \mathbb{N}$).

Informally speaking, assume that there are n users, and that a PPT adversary is allowed to (i) adaptively corrupt the users (i.e., obtaining their secret keys) at any time, and (ii) make receiver selective opening queries (i.e., obtaining the corresponding secret keys and the challenge messages) after seeing a challenge ciphertext vector of length $t < n$. ANON-RSO$_k$&C security requires that whatever the adversary (seeing the challenge ciphertext vector) deduces about which public keys are used to generate the challenge ciphertext vector, can also be deduced without seeing any challenge ciphertexts.

Formal definition is as follows.

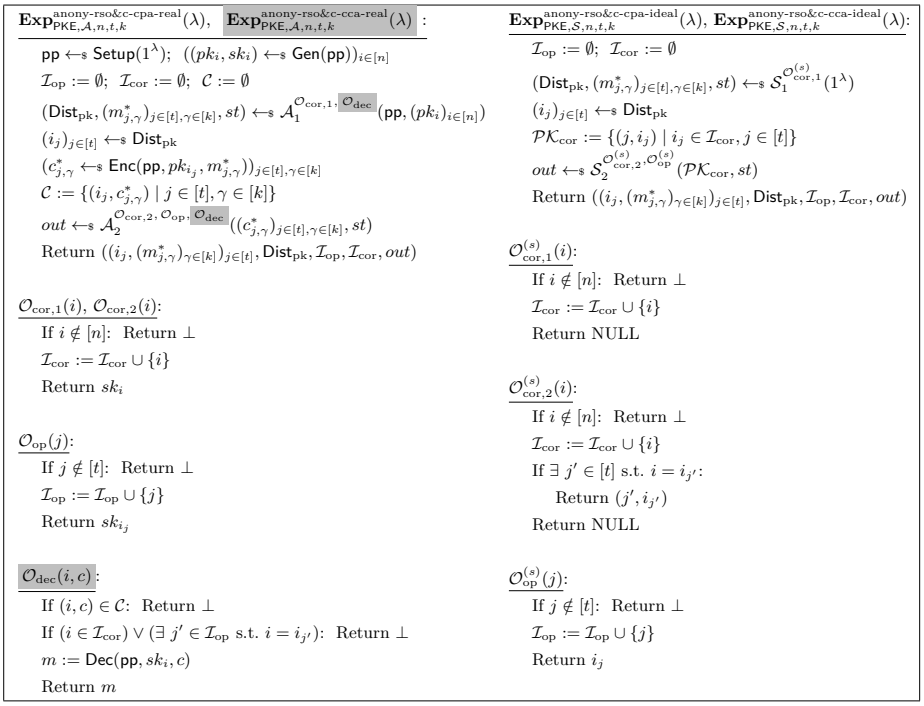

Fig. 1 Experiments for defining ANON-RSO$_k$&C-CPA/CCA security of scheme PKE.

Definition 1. (ANON-RSO$_k$&C-CPA/CCA). *A PKE scheme* $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* ANON-RSO$_k$&C-ATK secure *(where* ATK $\in \{\text{CPA}, \text{CCA}\}$ *and* $k \in \mathbb{N}$ *is a constant), if for any polynomially bounded* n, t *(where* $0 < t \le n$*), and any PPT adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$*, there is a PPT simulator* $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$*, such that for any PPT distinguisher* $\mathcal{D}$*, the advantage* $\mathbf{Adv}^{\text{anon-rso\&c-atk}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},\mathcal{D},n,t,k}(\lambda) :=$

$$\left|\Pr[\mathcal{D}(\mathbf{Exp}^{\text{anon-rso\&c-atk-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)) = 1] - \Pr[\mathcal{D}(\mathbf{Exp}^{\text{anon-rso\&c-atk-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda)) = 1]\right|$$

is negligible, where $\mathbf{Exp}^{\text{anon-rso\&c-atk-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$ *and* $\mathbf{Exp}^{\text{anon-rso\&c-atk-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda)$ *are defined in Fig. 1, and* atk $\in \{\text{cpa}, \text{cca}\}$*. In both of the experiments, we require that for all* $\mathsf{Dist}_{\text{pk}}$ *output by* $\mathcal{A}_1$ *and* $\mathcal{S}_1$*, it holds that (1)* $\mathsf{Dist}_{\text{pk}}$ *is efficiently samplable, and (2) for all* $(i_j)_{j\in[t]} \leftarrow\!\!\$\ \mathsf{Dist}_{\text{pk}}$*,* $i_{j_1} \neq i_{j_2}$ *for any distinct* $j_1, j_2 \in [t]$*.*

Remark 1. Our security notion ANON-RSO$_k$&C-CPA/CCA grants the adversary multiple, adaptive opening queries (i.e., $\mathcal{O}_{\text{op}}$), like [6].

Remark 2. In $\mathbf{Exp}^{\text{anon-rso\&c-atk-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$ where atk $\in \{\text{cpa}, \text{cca}\}$, there are totally n public keys $(pk_i)_{i\in[n]}$, and only t of them (i.e., $(pk_{i_j})_{j\in[t]}$) are used to generate the challenge ciphertexts $(c^*_{j,\gamma})_{j\in[t],\gamma\in[k]}$. Note that (i) by querying the opening oracle $\mathcal{O}_{\text{op}}$ on $j \in [t]$ directly, $\mathcal{A}$ can obtain sk_{i_j} corresponding to some specified

$(c^*_{j,\gamma})_{\gamma\in[k]}$; (ii) by querying the corruption oracle $\mathcal{O}_{\text{cor},1}$ or $\mathcal{O}_{\text{cor},2}$, $\mathcal{A}$ can obtain some corresponding secret keys of the n public keys, but cannot ask for the secret key corresponding to some specified $c^*_{j,\gamma}$ since it may not know the value of i_j.

ANON-RSO$_k$&C-CPA $\Rightarrow$ ANON-COR. We show that ANON-RSO$_k$&C-CPA security implies the ANON-COR security [5].

Informally, the experiment for defining ANON-COR security is as follows. At the beginning, the challenger generates n public keys $(pk_i)_{i\in[n]}$, and sends them to an adversary $\mathcal{A}$. After receiving t ($t < n$) messages from $\mathcal{A}$, the challenger randomly samples t distinct public keys from $(pk_i)_{i\in[n]}$, uses them to encrypt the t messages respectively, and sends the t ciphertexts back to $\mathcal{A}$. Then, $\mathcal{A}$ can access to a corruption oracle adaptively, by querying it on any $i \in [n]$ and receiving sk_i as a response. Denote by Q the total number of corruption queries made by $\mathcal{A}$. ANON-COR security requires that for any $\epsilon > 0$ and any $\lambda < t$, $Q < n(1-\epsilon)$, no PPT adversary $\mathcal{A}$ can compromise more than $\frac{Q}{n} + \epsilon$ fraction of the ciphertext-encrypting keys with non-negligible probability. Formal definition of ANON-COR security is given in the full version [17].

Note that any ANON-COR adversary can be seen as an ANON-RSO$_k$&C-CPA adversary $\mathcal{A}$ which (i) ignores $(c^*_{j,\gamma})_{2\le\gamma\le k}$ for all $j \in [t]$ if $k > 1$, (ii) does not query $\mathcal{O}_{\text{cor},1}$ or $\mathcal{O}_{\text{op}}$, (iii) queries $\mathcal{O}_{\text{cor},2}$ Q times, and (iv) the output distribution $\mathsf{Dist}_{\text{pk}}$ always samples t distinct indexes $i_1, \cdots, i_t$ uniformly random from $[n]$. The fraction of the ciphertext-encrypting keys that ANON-COR adversary compromises over $(pk_{i_j})_{j\in[t]}$ can be computed directly from experiment $\mathbf{Exp}^{\text{anon-rso\&c-cpa-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$. ANON-RSO$_k$&C-CPA security guarantees that there is a simulator $\mathcal{S}$ such that $\mathbf{Exp}^{\text{anon-rso\&c-cpa-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda)$ and $\mathbf{Exp}^{\text{anon-rso\&c-cpa-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$ are indistinguishable. Note that in $\mathbf{Exp}^{\text{anon-rso\&c-cpa-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda)$, $\mathcal{S}$ has no information about $(i_j)_{j\in[t]}$ except for the responses obtained via querying $\mathcal{O}^{(s)}_{\text{cor},1}$, $\mathcal{O}^{(s)}_{\text{cor},2}$. Hence, the fraction of the "ciphertext-encrypting" indexes that $\mathcal{S}$ compromises over $(i_j)_{j\in[t]}$ is nearly $\frac{Q}{n}$. Therefore, the indistinguishability between $\mathbf{Exp}^{\text{anon-rso\&c-cpa-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda)$ and $\mathbf{Exp}^{\text{anon-rso\&c-cpa-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$ implies the advantage of the ANON-COR adversary is negligible.

3.2 Confidentiality under Corruptions

SIM-RSO$_k$&C security. In order to capture confidentiality under the same corruptions which are considered in ANON-RSO$_k$&C security, we introduce a new security notion, called SIM-RSO$_k$&C security. We stress that SIM-RSO$_k$&C security is similar to SIM-RSO$_k$ security [23], except that the SIM-RSO$_k$&C adversary is allowed to corrupt the receivers *at any time* (i.e., even before seeing the challenge ciphertexts).

Informally, assume that there are n users, and that a PPT adversary is allowed to (i) adaptively corrupt the users (i.e., obtaining their secret keys) at any time, and (ii) make receiver selective opening queries (i.e., obtaining the corresponding secret keys and the challenge messages) after seeing a challenge

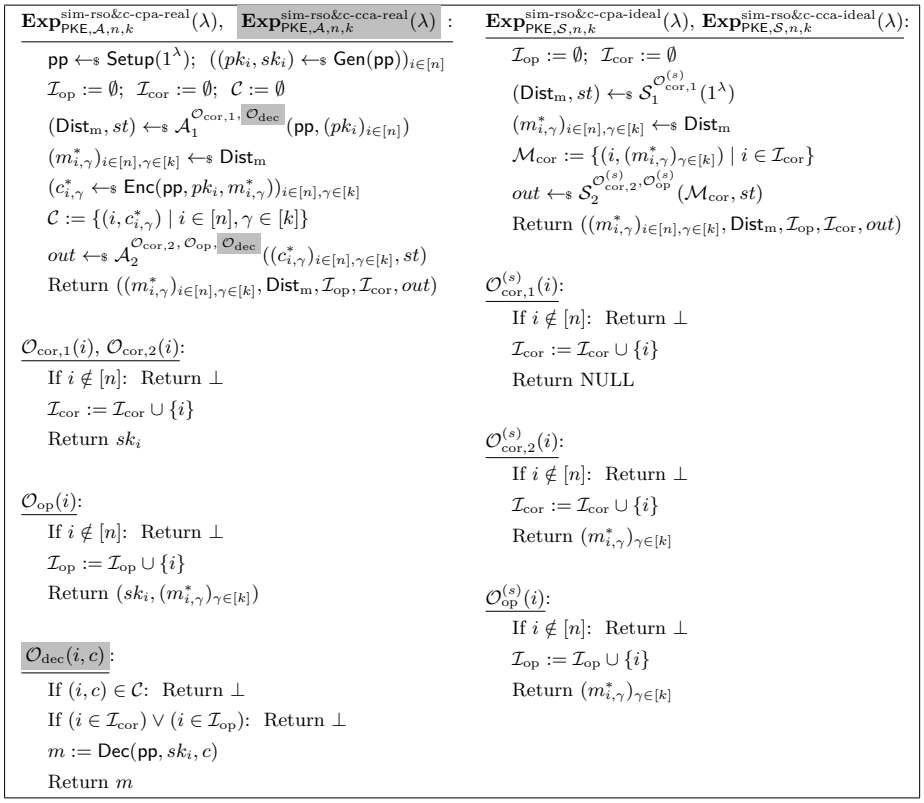

Fig. 2 Experiments for defining SIM-RSO$_k$&C-CPA/CCA security of scheme PKE.

ciphertext vector of length n. SIM-RSO$_k$&C security requires that whatever the adversary (seeing the challenge ciphertext vector) deduces about the challenge messages, can also be deduced without seeing any challenge ciphertexts.

Formal definition is as follows.

Definition 2. (SIM-RSO$_k$&C-CPA/CCA). *A PKE scheme* $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* SIM-RSO$_k$&C-ATK secure *(where* $\text{ATK} \in \{\text{CPA}, \text{CCA}\}$ *and* $k \in \mathbb{N}$ *is a constant), if for any polynomially bounded* $n > 0$*, and any PPT adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$*, there is a PPT simulator* $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$*, such that for any PPT distinguisher* $\mathcal{D}$*, the advantage* $\mathbf{Adv}^{\text{sim-rso\&c-atk}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},\mathcal{D},n,k}(\lambda) :=$

$$\left|\Pr[\mathcal{D}(\mathbf{Exp}^{\text{sim-rso\&c-atk-real}}_{\mathsf{PKE},\mathcal{A},n,k}(\lambda)) = 1] - \Pr[\mathcal{D}(\mathbf{Exp}^{\text{sim-rso\&c-atk-ideal}}_{\mathsf{PKE},\mathcal{S},n,k}(\lambda)) = 1]\right|$$

is negligible, where $\mathbf{Exp}^{\text{sim-rso\&c-atk-real}}_{\mathsf{PKE},\mathcal{A},n,k}(\lambda)$ *and* $\mathbf{Exp}^{\text{sim-rso\&c-atk-ideal}}_{\mathsf{PKE},\mathcal{S},n,k}(\lambda)$ *are defined in Fig. 2, and* $\text{atk} \in \{\text{cpa}, \text{cca}\}$*. In both of the experiments, we require that for all* Dist_{m} *output by* $\mathcal{A}_1$ *and* $\mathcal{S}_1$*,* Dist_{m} *is efficiently samplable.*

SIM-RSO$_k$&C-ATK $\Rightarrow$ SIM-RSO$_k$-ATK. We claim that SIM-RSO$_k$&C-ATK security (ATK $\in \{\mathrm{CPA}, \mathrm{CCA}\}$) implies simulation-based RSO security in the multi-challenge setting (i.e., SIM-RSO$_k$-ATK security) [23].

Generally, SIM-RSO$_k$-ATK security requires that for any PPT adversary $\mathcal{A}$ in the real experiment of SIM-RSO$_k$-ATK, there is a simulator $\mathcal{S}$, such that the final output of the ideal experiment and that of the real experiment are indistinguishable. Standard SIM-RSO-ATK security [14,12,16] is a special case of SIM-RSO$_k$-ATK security (i.e., $k = 1$). For completeness, formal definition of SIM-RSO$_k$-ATK security is given in the full version [17].

The reason that SIM-RSO$_k$&C-ATK security implies SIM-RSO$_k$-ATK security is as follows. Note that any SIM-RSO$_k$-ATK adversary $\mathcal{A}$ can be seen as a SIM-RSO$_k$&C-ATK adversary which does not query the corruption oracles $\mathcal{O}_{\mathrm{cor},1}, \mathcal{O}_{\mathrm{cor},2}$. SIM-RSO$_k$&C-ATK security guarantees the existence of a simulator $\mathcal{S}'$, such that the final output of the ideal experiment and that of the real experiment are indistinguishable. Hence, for the final output of the ideal experiment $((m^*_{i,\gamma})_{i\in[n],\gamma\in[k]}, \mathsf{Dist}_{\mathrm{m}}, \mathcal{I}_{\mathrm{op}}, \mathcal{I}_{\mathrm{cor}}, out)$, it also holds that $\mathcal{I}_{\mathrm{cor}} = \emptyset$ (i.e., $\mathcal{S}'$ has never queried $\mathcal{O}^{(s)}_{\mathrm{cor},1}, \mathcal{O}^{(s)}_{\mathrm{cor},2}$). Hence, a SIM-RSO$_k$-ATK simulator $\mathcal{S}$ can be constructed from $\mathcal{S}'$.

3.3 Combining Anonymity and Confidentiality under Corruptions

We introduce the notion of AC-RSO$_k$&C-CPA/CCA security, to capture ANON-RSO$_k$&C-CPA/CCA security and SIM-RSO$_k$&C-CPA/CCA security in one notion for convenience.

Informally, assume that there are n users, and that a PPT adversary is allowed to (i) adaptively corrupt the users (i.e., obtaining their secret keys) at any time, and (ii) make receiver selective opening queries (i.e., obtaining the corresponding secret keys and the challenge messages) after seeing a challenge ciphertext vector of length $t < n$. AC-RSO$_k$&C security requires that whatever the adversary (seeing the challenge ciphertext vector) deduces about which public keys or messages are used to generate the challenge ciphertext vector, can also be deduced without seeing any challenge ciphertexts.

Formal definition is as follows.

Definition 3. (AC-RSO$_k$&C-CPA/CCA). *A PKE scheme* $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is* AC-RSO$_k$&C-ATK secure *(where* $\mathrm{ATK} \in \{\mathrm{CPA}, \mathrm{CCA}\}$ *and* $k \in \mathbb{N}$ *is a constant), if for any polynomially bounded* n, t *(where* $0 < t \leq n$*), and any PPT adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$*, there is a PPT simulator* $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$*, such that for any PPT distinguisher* $\mathcal{D}$*, the advantage* $\mathbf{Adv}^{\text{ac-rso\&c-atk}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},\mathcal{D},n,t,k}(\lambda) :=$

$$\left|\Pr[\mathcal{D}(\mathbf{Exp}^{\text{ac-rso\&c-atk-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)) = 1] - \Pr[\mathcal{D}(\mathbf{Exp}^{\text{ac-rso\&c-atk-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda)) = 1]\right|$$

is negligible, where $\mathbf{Exp}^{\text{ac-rso\&c-atk-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$ *and* $\mathbf{Exp}^{\text{ac-rso\&c-atk-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda)$ *are defined in Fig. 3, and* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca}\}$*. In both of the experiments, we require that for all* Dist *output by* $\mathcal{A}_1$ *and* $\mathcal{S}_1$*, it holds that (1)* Dist *is efficiently samplable, and (2) for all* $(i_j, (m^*_{j,\gamma})_{\gamma\in[k]})_{j\in[t]} \leftarrow_{\$} \mathsf{Dist}$*,* $i_{j_1} \neq i_{j_2}$ *for any distinct* $j_1, j_2 \in [t]$*.*

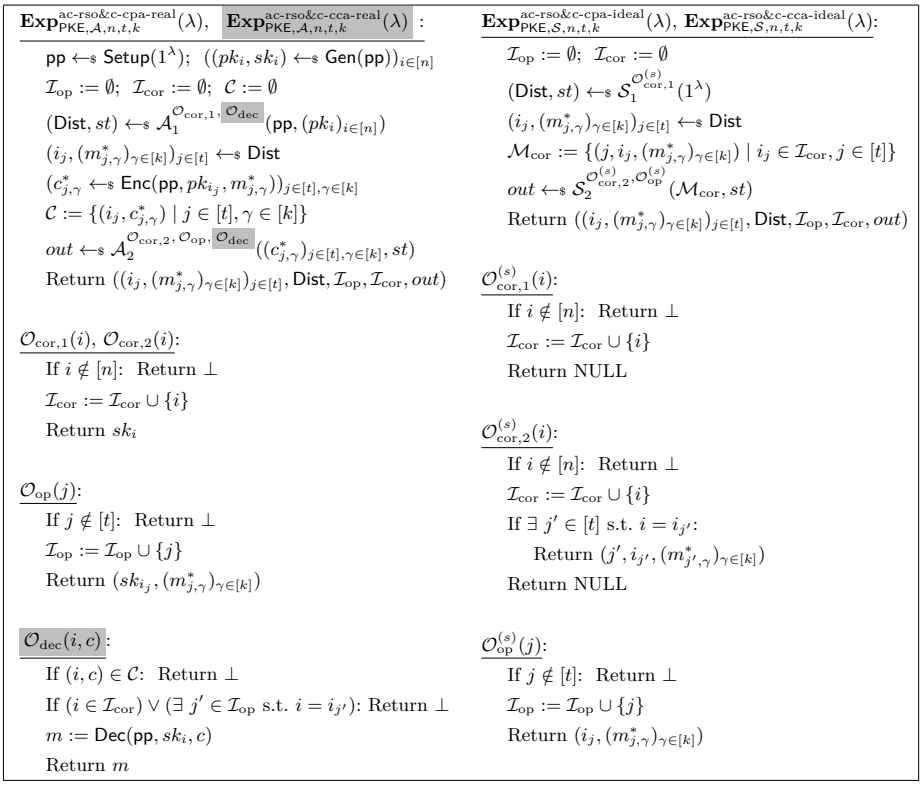

Fig. 3 Experiments for defining AC-RSO$_k$&C-CPA/CCA security of scheme PKE.

Note that, AC-RSO$_k$&C security can be easily simplified to guarantee only ANON-RSO$_k$&C security (when the adversary chooses a distribution Dist that has no entropy in the message part) and can also be simplified to guarantee only SIM-RSO$_k$&C security (by letting $n = t$).

4 AC-RSO$_k$&C Secure PKE from KM-NCE

In this section, we introduce a new primitive called key and message non-committing encryption (KM-NCE), and two security requirements, KMNC$_k$-CPA/CCA and robustness, for it. Then, we show that KMNC$_k$-CPA/CCA secure and robust KM-NCE implies AC-RSO$_k$&C-CPA/CCA secure PKE.

4.1 Key and Message Non-Committing Encryption

Now we provide the definition of key and message non-committing encryption (KM-NCE) and security properties for this primitive. Informally, a KM-NCE scheme is a PKE scheme with the property that there is a way to generate fake

ciphertexts without any public key, such that any k fake ciphertexts can be later opened to any k messages (by showing an appropriate secret key). This primitive is an extension of receiver non-committing encryption (RNCE) in [8,14,12]. Generally speaking, the main differences between KM-NCE and RNCE are that (i) KM-NCE is defined in the k-challenge setting, for some constant k, and (ii) the algorithm, generating fake ciphertexts, of KM-NCE does not take any public key as input, while that of RNCE needs the public key.

For $k \in \mathbb{N}$, a key and message non-committing encryption scheme $\mathsf{KM\text{-}NCE}$ in the k-challenge setting, with a message space $\mathcal{M}$, consists of six PPT algorithms $(\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Fake}, \mathsf{Open}_k)$.

- Setup: The setup algorithm, given a security parameter 1^λ, outputs a public parameter pp.
- Gen: The key generation algorithm, given pp, outputs a public key pk, a secret key sk and a trapdoor key tk.
- Enc: The encryption algorithm, given pp, pk and a message $m \in \mathcal{M}$, outputs a ciphertext c.
- Dec: The (deterministic) decryption algorithm, given pp, sk and c, outputs $m \in \mathcal{M} \cup \{\perp\}$.
- Fake: The fake encryption algorithm, given pp, outputs a fake ciphertext c' and a trapdoor td.
- Open_k: The opening algorithm, given $(\mathsf{pp}, tk, pk, sk)$, k fake ciphertexts $(c'_\gamma)_{\gamma\in[k]}$, k trapdoors $(td_\gamma)_{\gamma\in[k]}$ correponding to $(c'_\gamma)_{\gamma\in[k]}$, and k messages $(m_\gamma)_{\gamma\in[k]}$, outputs a secret key sk'.

For KM-NCE, standard correctness is required. Formally, we require that for any pp generated by Setup, any (pk, sk, tk) generated by $\mathsf{Gen}(\mathsf{pp})$ and any $m \in \mathcal{M}$, it holds that $\mathsf{Dec}(\mathsf{pp}, sk, \mathsf{Enc}(\mathsf{pp}, pk, m)) = m$.

Definition 4. (KMNC_k-CPA/CCA). *For $k \in \mathbb{N}$, a KM-NCE scheme* $\mathsf{KM\text{-}NCE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Fake}, \mathsf{Open}_k)$*, in the k-challenge setting, is* KMNC_k-ATK secure *(where* $\mathrm{ATK} \in \{\mathrm{CPA}, \mathrm{CCA}\}$*), if for any PPT adversary* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$*, the advantage* $\mathbf{Adv}^{\text{kmnc-atk}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda) :=$

$$\left|\Pr[\mathbf{Exp}^{\text{kmnc-atk-real}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda) = 1] - \Pr[\mathbf{Exp}^{\text{kmnc-atk-sim}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda) = 1]\right|$$

is negligible, where experiment $\mathbf{Exp}^{\text{kmnc-atk-real}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda)$ *and* $\mathbf{Exp}^{\text{kmnc-atk-sim}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda)$ *are defined in Fig. 4, and* $\mathrm{atk} \in \{\mathrm{cpa}, \mathrm{cca}\}$.

We also define a statistical robustness for $\mathsf{KM\text{-}NCE}$.

Definition 5 (Robustness). *A KM-NCE scheme* $\mathsf{KM\text{-}NCE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Fake}, \mathsf{Open}_k)$*, in the k-challenge setting ($k \in \mathbb{N}$), is* robust*, if the probability* $\boldsymbol{\epsilon}^{\text{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda) :=$

$$\Pr\left[\begin{array}{c}\mathsf{pp} \leftarrow_\$ \mathsf{Setup}(1^\lambda), (pk, sk, tk) \leftarrow_\$ \mathsf{Gen}(\mathsf{pp}), \\ (c, td) \leftarrow_\$ \mathsf{Fake}(\mathsf{pp})\end{array} : \mathsf{Dec}(\mathsf{pp}, sk, c) \neq \perp\right]$$

is negligible.

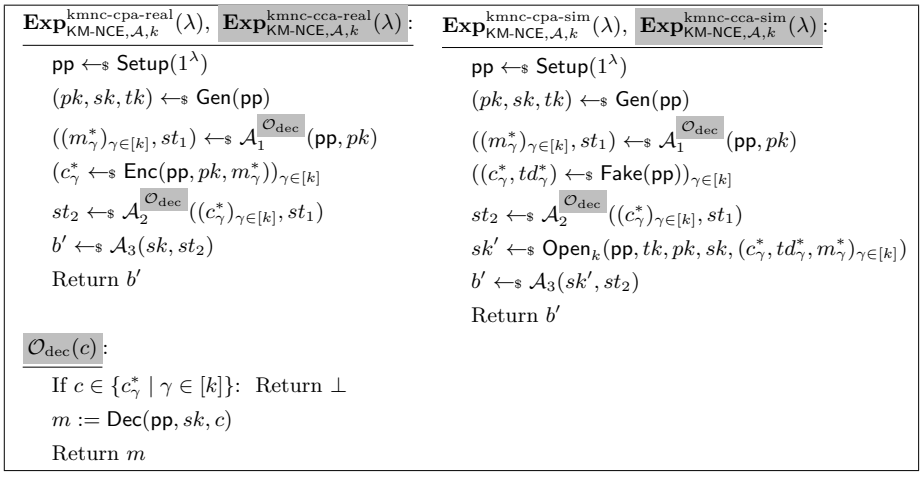

Fig. 4 Experiments for defining KMNC$_k$-CPA/CCA security of scheme KM-NCE.

4.2 Generic Construction of AC-RSO$_k$&C Secure PKE from KM-NCE

In this section, we show that for $k \in \mathbb{N}$, a KMNC$_k$-CPA (resp. KMNC$_k$-CCA) secure and robust KM-NCE scheme implies an AC-RSO$_k$&C-CPA (resp. AC-RSO$_k$&C-CCA) secure PKE scheme. Specifically, we have the following theorem.

Theorem 1. *If a KM-NCE scheme* $\mathsf{KM\text{-}NCE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Fake}, \mathsf{Open}_k)$*, in the k-challenge setting ($k \in \mathbb{N}$), is KMNC$_k$-CPA (resp. KMNC$_k$-CCA) secure and robust, then* $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *is an AC-RSO$_k$&C-CPA (resp. AC-RSO$_k$&C-CCA) secure PKE scheme.*[5]

Proof of Theorem 1. We just prove that a KMNC$_k$-CCA secure and robust KM-NCE scheme implies an AC-RSO$_k$&C-CCA secure PKE scheme. The proof for the case of CPA is analogous and much easier, so we omit the details here.

Let n and t be arbitrary polynomials satisfying $0 < t \leq n$. Let $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ be any PPT adversary attacking $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ in the sense of AC-RSO$_k$&C-CCA, and $\mathcal{D}$ be any PPT distinguisher. Without loss of generality, we assume that $\mathcal{A}$ never repeats an oracle query. Specifically, we assume that if $\mathcal{A}_1$ has queried oracle $\mathcal{O}_{\text{cor},1}$ on some i, then $\mathcal{A}_2$ will not query $\mathcal{O}_{\text{cor},2}$ on i.

We proceed in a series of games.

Game G_{-1}: This is exactly the $\mathbf{Exp}^{\text{ac-rso\&c-cca-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$ experiment, i.e., $\mathsf{G}_{-1} = \mathbf{Exp}^{\text{ac-rso\&c-cca-real}}_{\mathsf{PKE},\mathcal{A},n,t,k}(\lambda)$.

[5] For $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$, we require that (i) the public parameter pp generated by Setup can be used for multiple users, and (ii) Gen does not output tk (i.e., the key generation algorithm of PKE firstly invokes the key generation algorithm of KM-NCE to generate (pk, sk, tk), and then outputs (pk, sk), ignoring tk).

More specifically, in G_{-1}, the challenger firstly generates $\mathsf{pp} \leftarrow_{\$} \mathsf{Setup}(1^\lambda)$ and $((pk_i, sk_i, tk_i) \leftarrow_{\$} \mathsf{Gen}(\mathsf{pp}))_{i\in[n]}$, and sends $(\mathsf{pp}, (pk_i)_{i\in[n]})$ to $\mathcal{A}_1$. The challenger initiates $\mathcal{I}_{\text{op}} := \emptyset$ and $\mathcal{I}_{\text{cor}} := \emptyset$, and keeps track of all $\mathcal{A}$'s issued queries to $\mathcal{O}_{\text{cor},1}, \mathcal{O}_{\text{cor},2}, \mathcal{O}_{\text{op}}$ by maintaining these two sets. Then, the challenger answers $\mathcal{A}_1$'s $\mathcal{O}_{\text{cor},1}, \mathcal{O}_{\text{dec}}$ oracle queries with $(sk_i)_{i\in[n]}$. After receiving Dist, the challenger samples $(i_j, (m^*_{j,\gamma})_{\gamma\in[k]})_{j\in[t]} \leftarrow \mathsf{Dist}$, computes $(c^*_{j,\gamma} \leftarrow_{\$} \mathsf{Enc}(\mathsf{pp}, pk_{i_j}, m^*_{j,\gamma}))_{j\in[t],\gamma\in[k]}$, sets that $\mathcal{C} := \{(i_j, c^*_{j,\gamma}) \mid j \in [t], \gamma \in [k]\}$, and sends $(c^*_{j,\gamma})_{j\in[t],\gamma\in[k]}$ to $\mathcal{A}_2$. Then, the challenger continues to answer $\mathcal{A}_2$'s $\mathcal{O}_{\text{cor},2}, \mathcal{O}_{\text{op}}$, $\mathcal{O}_{\text{dec}}$ oracle queries with $(sk_i)_{i\in[n]}$. Finally, when $\mathcal{A}_2$ returns out, the challenger returns $((i_j, (m^*_{j,\gamma})_{\gamma\in[k]})_{j\in[t]}, \mathsf{Dist}, \mathcal{I}_{\text{op}}, \mathcal{I}_{\text{cor}}, out)$ as its final output.

Game G_0: Game G_0 is the same as G_{-1}, except that two sets $\mathcal{I}_{\text{op-sk}}$ and $\mathcal{I}_{\text{cor-sk}}$ are introduced in G_0. Informally, $\mathcal{I}_{\text{op-sk}}$ is introduced to ensure that if $\mathcal{A}_2$ submits a query $\mathcal{O}_{\text{cor},2}(i)$ such that the secret key corresponding to pk_i has already been given to $\mathcal{A}$ via oracle $\mathcal{O}_{\text{op}}$, then the challenger will directly return the secret key previously given to $\mathcal{A}_2$; $\mathcal{I}_{\text{cor-sk}}$ is introduced to ensure that if $\mathcal{A}_2$ submits a query $\mathcal{O}_{\text{op}}(j)$ such that the secret key corresponding to pk_{i_j} has already been exposed to $\mathcal{A}$ in a previous corruption query, then the challenger will directly return the secret key previously given to $\mathcal{A}_2$.

Specifically, the differences between G_0 and G_{-1} are as follows. The challenger additionally initiates $\mathcal{I}_{\text{op-sk}} := \emptyset$ and $\mathcal{I}_{\text{cor-sk}} := \emptyset$ at the beginning, and answers $\mathcal{A}$'s $\mathcal{O}_{\text{cor},1}, \mathcal{O}_{\text{cor},2}, \mathcal{O}_{\text{op}}$ oracle queries as below:

- on a query $\mathcal{O}_{\text{cor},1}(i)$ where $i \in [n]$, the challenger sets $\mathcal{I}_{\text{cor}} := \mathcal{I}_{\text{cor}} \cup \{i\}$ and $\mathcal{I}_{\text{cor-sk}} := \mathcal{I}_{\text{cor-sk}} \cup \{(i, sk_i)\}$, and returns sk_i to $\mathcal{A}_1$;
- on a query $\mathcal{O}_{\text{cor},2}(i)$ where $i \in [n]$, the challenger firstly sets $\mathcal{I}_{\text{cor}} := \mathcal{I}_{\text{cor}} \cup \{i\}$. If there is some $j' \in \mathcal{I}_{\text{op}}$ such that $i_{j'} = i$, then there must be some tuple $(j', i, \overline{sk}_i) \in \mathcal{I}_{\text{op-sk}}$, and in this case the challenger sets $\mathcal{I}_{\text{cor-sk}} := \mathcal{I}_{\text{cor-sk}} \cup \{(i, \overline{sk}_i)\}$, and returns $\overline{sk}_i$ to $\mathcal{A}_2$; otherwise, it sets $\mathcal{I}_{\text{cor-sk}} := \mathcal{I}_{\text{cor-sk}} \cup \{(i, sk_i)\}$, and returns sk_i to $\mathcal{A}_2$;
- on a query $\mathcal{O}_{\text{op}}(j)$ where $j \in [t]$, the challenger firstly sets $\mathcal{I}_{\text{op}} := \mathcal{I}_{\text{op}} \cup \{j\}$. If $i_j \in \mathcal{I}_{\text{cor}}$, there must be some tuple $(i_j, \overline{sk}_{i_j}) \in \mathcal{I}_{\text{cor-sk}}$, and in this case the challenger sets $\mathcal{I}_{\text{op-sk}} := \mathcal{I}_{\text{op-sk}} \cup \{(j, i_j, \overline{sk}_{i_j})\}$, and returns $\overline{sk}_{i_j}$ to $\mathcal{A}_2$; otherwise, it sets $\mathcal{I}_{\text{op-sk}} := \mathcal{I}_{\text{op-sk}} \cup \{(j, i_j, sk_{i_j})\}$, and returns sk_{i_j} to $\mathcal{A}_2$.

Since all the secret keys $(sk_i)_{i\in[n]}$ are generated at the beginning and will not be updated during the proceedings of G_{-1}, the modifications introduced in game G_0 do not change $\mathcal{A}$'s view. Hence, $\Pr[\mathcal{D}(\mathsf{G}_0) = 1] = \Pr[\mathcal{D}(\mathsf{G}_{-1}) = 1]$.

Game $\mathsf{G}_{\widehat{i}}$ ($\widehat{i} \in [n]$): For all $\widehat{i} \in [n]$, $\mathsf{G}_{\widehat{i}}$ is the same as $\mathsf{G}_{\widehat{i}-1}$, except that

(1) when generating the challenge ciphertexts, if there is some $j' \in [t]$ such that $(i_{j'} \notin \mathcal{I}_{\text{cor}}) \wedge (i_{j'} = \widehat{i})$, the challenger generates $(c^*_{j',\gamma})_{\gamma\in[k]}$ with algorithm Fake instead of Enc, i.e., $((c^*_{j',\gamma}, td^*_{j',\gamma}) \leftarrow_{\$} \mathsf{Fake}(\mathsf{pp}))_{\gamma\in[k]}$;
(2) for $\mathcal{A}_2$'s each $\mathcal{O}_{\text{cor},2}$ oracle query i, if there is some $j' \in [t]$ satisfying $(j' \notin \mathcal{I}_{\text{op}}) \wedge (i_{j'} = \widehat{i})$, the challenger returns $sk'_{i_{j'}} \leftarrow_{\$} \mathsf{Open}_k(\mathsf{pp}, tk_{i_{j'}}, pk_{i_{j'}}, sk_{i_{j'}}, (c^*_{j',\gamma}, td^*_{j',\gamma}, m^*_{j',\gamma})_{\gamma\in[k]})$ to $\mathcal{A}_2$; otherwise, it answers this query as in $\mathsf{G}_{\widehat{i}-1}$;

(3) for $\mathcal{A}_2$'s each $\mathcal{O}_{\mathrm{op}}$ oracle query j, if the corresponding i_j satisfies $(i_j \notin \mathcal{I}_{\mathrm{cor}}) \wedge (i_j = \widehat{i})$, the challenger returns $sk'_{i_j} \leftarrow_{\$} \mathsf{Open}_k(\mathsf{pp}, tk_{i_j}, pk_{i_j}, sk_{i_j}, (c^*_{j,\gamma}, td^*_{j,\gamma}, m^*_{j,\gamma})_{\gamma\in[k]})$ to $\mathcal{A}_2$; otherwise, it answers this query as in $\mathsf{G}_{\widehat{i}-1}$.

Game $\mathsf{G}_{n+\widehat{i}}$ ($\widehat{i} \in [n]$): For all $\widehat{i} \in [n]$, game $\mathsf{G}_{n+\widehat{i}}$ is the same as $\mathsf{G}_{n+\widehat{i}-1}$, except that for $\mathcal{A}_2$'s each $\mathcal{O}_{\mathrm{dec}}$ oracle query (i, c), if $(\exists(i_j, c^*_{j,\gamma}) \in \mathcal{C}$ s.t. $i_j = \widehat{i} \wedge c^*_{j,\gamma} = c) \wedge (i \notin \mathcal{I}_{\mathrm{cor}})$, the challenger returns $\perp$ to $\mathcal{A}_2$; otherwise, it answers this query as in game $\mathsf{G}_{n+\widehat{i}-1}$.

We present the following two lemmas whose proofs are given in the full version [17].

Lemma 1. *For each* $\widehat{i} \in [n]$, $|\Pr[\mathcal{D}(\mathsf{G}_{\widehat{i}}) = 1] - \Pr[\mathcal{D}(\mathsf{G}_{\widehat{i}-1}) = 1]| \leq \mathbf{Adv}^{\text{kmnc-cca}}_{\mathsf{KM\text{-}NCE},\mathcal{B},k}(\lambda)$ *for some PPT adversary* $\mathcal{B}$.

Lemma 2. *For each* $\widehat{i} \in [n]$, $|\Pr[\mathcal{D}(\mathsf{G}_{n+\widehat{i}}) = 1] - \Pr[\mathcal{D}(\mathsf{G}_{n+\widehat{i}-1}) = 1]| \leq t \cdot k \cdot \boldsymbol{\epsilon}^{\mathrm{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda)$.

Note that in game G_{2n}, (i) when generating the challenge ciphertexts, for each $j \in [t]$ such that $i_j \notin \mathcal{I}_{\mathrm{cor}}$, the corresponding challenge ciphertexts $(c^*_{j,\gamma})_{\gamma\in[k]}$ are generated with algorithm Fake; (ii) any $\mathcal{O}_{\mathrm{cor},2}$ oracle query $i \in [n]$ such that $i = i_{j'}$ for some $j' \notin \mathcal{I}_{\mathrm{op}}$ is answered with algorithm Open_k; (iii) any $\mathcal{O}_{\mathrm{op}}$ oracle query $j \in [t]$ such that $i_j \notin \mathcal{I}_{\mathrm{cor}}$ is answered with algorithms Open_k; (iv) any $\mathcal{O}_{\mathrm{dec}}$ oracle query (i, c) is answered with $\perp$ if there is some $j \in [t]$ and $\gamma \in [k]$ such that $(i_j, c^*_{j,\gamma} = c) \in \mathcal{C}$ and $c^*_{j,\gamma}$ is generated with algorithm Fake. Now, a PPT simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ can be constructed, which simulates G_{2n} perfectly for $\mathcal{A}$. Hence, we derive that

$$\mathbf{Exp}^{\text{ac-rso\&c-cca-ideal}}_{\mathsf{PKE},\mathcal{S},n,t,k}(\lambda) = \mathsf{G}_{2n}.$$

Due to space limitations, the detailed description of $\mathcal{S}$ will be given in the full version [17].

Therefore, $\mathbf{Adv}^{\text{ac-rso\&c-cca}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},\mathcal{D},n,t,k}(\lambda) = |\Pr[\mathcal{D}(\mathsf{G}_{-1}) = 1] - \Pr[\mathcal{D}(\mathsf{G}_{2n}) = 1]|$

$$\leq n \cdot \mathbf{Adv}^{\text{kmnc-cca}}_{\mathsf{KM\text{-}NCE},\mathcal{B}',k}(\lambda) + n \cdot t \cdot k \cdot \boldsymbol{\epsilon}^{\mathrm{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda) \tag{1}$$

for some PPT adversary $\mathcal{B}'$. This completes the proof of Theorem 1. ■

5 KM-NCE from Key-Openable Hash Proof System

In this section, we present a generic construction of KM-NCE that is needed in the AC-RSO$_k$&C secure PKE construction in Sect. 4.2. Our main building block is a new variant of Hash Proof System (HPS), called *Key-Openable HPS*. We firstly recall the definition of HPS from [9], and then formalize our new Key-Openable HPS. Next, we show how to construct KM-NCE from Key-Openable HPS. Jumping ahead, we will give concrete instantiations of Key-Openable HPS from the matrix decisional Diffie-Hellman assumption in Sect. 6.

5.1 Recall: Hash Proof System

In this subsection, we recall the formal definition of HPS according to [9]. For applications in constructing KM-NCE, we require that HPS has two parameter generation algorithms, a master parameter generation algorithm MPar and an (ordinary) parameter generation algorithm Par.

Definition 6 (Hash Proof System). *A hash proof system* $\mathsf{HPS} = (\mathsf{MPar}, \mathsf{Par}, \mathsf{Pub}, \mathsf{Priv})$ *consists of a tuple of PPT algorithms:*

- $\mathsf{mpar} \leftarrow_{\$} \mathsf{MPar}(1^\lambda)$*: The master parameter generation algorithm outputs a master public parameter* mpar*, which implicitly defines the universe set* $\mathcal{X}$ *and the hash value space* Π*.*

  We assume that there are PPT algorithms for sampling $x \leftarrow_{\$} \mathcal{X}$ *uniformly and sampling* $\pi \leftarrow_{\$} \Pi$ *uniformly. We require* mpar *to be an implicit input of other algorithms.*
- $\mathsf{par} \leftarrow_{\$} \mathsf{Par}(\mathsf{mpar})$*: The (ordinary) parameter generation algorithm takes* mpar *as input, and outputs an (ordinary) public parameter* par*, which implicitly defines* $(\mathcal{L}, \mathcal{SK}, \mathcal{PK}, \Lambda_{(\cdot)}, \alpha)$*, where* $\mathcal{L} \subseteq \mathcal{X}$ *is an NP-language,* $\mathcal{SK}$ *is the hashing key space,* $\mathcal{PK}$ *is the projection key space,* $\Lambda_{(\cdot)} : \mathcal{X} \longrightarrow \Pi$ *is a family of hash functions indexed by a hashing key* $\mathsf{sk} \in \mathcal{SK}$*, and* $\alpha : \mathcal{SK} \longrightarrow \mathcal{PK}$ *is the projection function.*

  We assume that $\Lambda_{(\cdot)}$ *and* α *are efficiently computable and there are PPT algorithms for sampling* $x \leftarrow_{\$} \mathcal{L}$ *uniformly together with a witness* w*, and sampling* $\mathsf{sk} \leftarrow_{\$} \mathcal{SK}$ *uniformly. We require* par *to be an implicit input of other algorithms.*
- $\pi \leftarrow \mathsf{Pub}(\mathsf{pk}, x, w)$*: The public evaluation algorithm outputs the hash value* $\pi = \Lambda_{\mathsf{sk}}(x) \in \Pi$ *of* $x \in \mathcal{L}$*, with the help of a projection key* $\mathsf{pk} = \alpha(\mathsf{sk})$ *and a witness* w *for* $x \in \mathcal{L}$*.*
- $\pi \leftarrow \mathsf{Priv}(\mathsf{sk}, x)$*: The private evaluation algorithm outputs the hash value* $\pi = \Lambda_{\mathsf{sk}}(x) \in \Pi$ *of* $x \in \mathcal{X}$*, directly using the hashing key* sk*.*

Perfect correctness *(a.k.a. projectiveness) of* HPS *requires that, for all possible* $\mathsf{mpar} \leftarrow_{\$} \mathsf{MPar}(1^\lambda)$ *and* $\mathsf{par} \leftarrow_{\$} \mathsf{Par}(\mathsf{mpar})$*, all hashing keys* $\mathsf{sk} \in \mathcal{SK}$ *with* $\mathsf{pk} := \alpha(\mathsf{sk})$ *the corresponding projection key, all* $x \in \mathcal{L}$ *with all possible witnesses* w*, it holds that* $\mathsf{Pub}(\mathsf{pk}, x, w) = \Lambda_{\mathsf{sk}}(x) = \mathsf{Priv}(\mathsf{sk}, x)$.

HPS is associated with a subset membership problem (SMP), which asks whether an element is uniformly chosen from $\mathcal{L}$ or $\mathcal{X}$. SMP can be extended to multi-fold SMP by considering multiple elements.

Definition 7 (Multi-fold SMP). *The multi-fold SMP related to* HPS *is hard, if for any PPT adversary* $\mathcal{A}$ *and any polynomial* Q*, it holds that* $\mathbf{Adv}^{Q\text{-msmp}}_{\mathsf{HPS},\mathcal{A}}(\lambda) := \left| \Pr[\mathcal{A}(\mathsf{mpar}, \mathsf{par}, \{x_\gamma\}_{\gamma\in[Q]}) = 1] - \Pr[\mathcal{A}(\mathsf{mpar}, \mathsf{par}, \{x'_\gamma\}_{\gamma\in[Q]}) = 1] \right| \leq \mathsf{negl}(\lambda)$*, where* $\mathsf{mpar} \leftarrow_{\$} \mathsf{MPar}(1^\lambda)$*,* $\mathsf{par} \leftarrow_{\$} \mathsf{Par}(\mathsf{mpar})$*,* $x_\gamma \leftarrow_{\$} \mathcal{L}$ *and* $x'_\gamma \leftarrow_{\$} \mathcal{X}$ *for each* $\gamma \in [Q]$.

Tag-based HPS. We recall a tag-based variant of HPS from [9,22], by allowing the hash functions $\Lambda_{(\cdot)}$ to have an additional element called label/tag as input. More precisely, in a tag-based HPS, the public parameter par also implicitly defines a tag space $\mathcal{T}$. Meanwhile, the hash functions $\Lambda_{(\cdot)}$, the public evaluation algorithm Pub and the private evaluation algorithm Priv also take a tag $\tau \in \mathcal{T}$ as input. Accordingly, perfect correctness requires $\mathsf{Pub}(\mathsf{pk}, x, w, \tau) = \Lambda_{\mathsf{sk}}(x, \tau) = \mathsf{Priv}(\mathsf{sk}, x, \tau)$ for all tags $\tau \in \mathcal{T}$.

5.2 Key-Openable HPS

We present the formal definition of our new *Key-Openable HPS*.

Definition 8 (Key-Openable Hash Proof System). *Let $k \in \mathbb{N}$. A key-openable hash proof system $\mathsf{HPS} = (\mathsf{MPar}, \mathsf{Par}, \mathsf{Pub}, \mathsf{Priv}, \mathsf{HOpen}_k)$ consists of a tuple of PPT algorithms:*

- *$(\mathsf{MPar}, \mathsf{Par}, \mathsf{Pub}, \mathsf{Priv})$ is a hash proof system as per Definition 6. Recall that the master parameter mpar output by $\mathsf{MPar}(1^\lambda)$ implicitly defines $(\mathcal{X}, \Pi)$, and there are PPT algorithms for sampling $x \leftarrow_\$ \mathcal{X}$ uniformly and sampling $\pi \leftarrow_\$ \Pi$ uniformly. We denote by $R_\mathcal{X}$ and R_Π the randomness spaces for sampling $x \leftarrow_\$ \mathcal{X}$ and $\pi \leftarrow_\$ \Pi$ respectively.*
- *In addition to public parameter par, $\mathsf{Par}(\mathsf{mpar})$ also outputs a trapdoor information td, which will be later used by HOpen_k.*
- *$\mathsf{sk}'/\perp \leftarrow_\$ \mathsf{HOpen}_k(\mathsf{td}, \mathsf{pk}, \mathsf{sk}, (x_\gamma, r_{x_\gamma}, \pi_\gamma, r_{\pi_\gamma})_{\gamma\in[k]})$: The hashing key opening algorithm takes as input the trapdoor td, a projection key $\mathsf{pk} \in \mathcal{PK}$, a hashing key $\mathsf{sk} \in \mathcal{SK}$ satisfying $\mathsf{pk} = \alpha(\mathsf{sk})$, and k tuples $(x_\gamma, r_{x_\gamma}, \pi_\gamma, r_{\pi_\gamma})_{\gamma\in[k]}$ where $x_\gamma \in \mathcal{X}$ with sampling randomness $r_{x_\gamma} \in R_\mathcal{X}$ and $\pi_\gamma \in \Pi$ with sampling randomness $r_{\pi_\gamma} \in R_\Pi$ for each $\gamma \in [k]$, and outputs another hashing key $\mathsf{sk}' \in \mathcal{SK}$ satisfying $\mathsf{pk} = \alpha(\mathsf{sk}')$ and $\pi_\gamma = \Lambda_{\mathsf{sk}'}(x_\gamma)$ for each $\gamma \in [k]$, or a special symbol $\perp$ indicating the failure of opening.*

Tag-based Key-Openable HPS. A key-openable $\mathsf{HPS} = (\mathsf{MPar}, \mathsf{Par}, \mathsf{Pub}, \mathsf{Priv}, \mathsf{HOpen}_k)$ is a tag-based key-openable HPS, if $(\mathsf{MPar}, \mathsf{Par}, \mathsf{Pub}, \mathsf{Priv})$ is a tag-based HPS (cf. Sect. 5.1), and HOpen_k also takes a set of tags $(\tau_\gamma)_{\gamma\in[k]}$ as input so that its output sk' satisfies $\mathsf{pk} = \alpha(\mathsf{sk}')$ and $\pi_\gamma = \Lambda_{\mathsf{sk}'}(x_\gamma, \tau_\gamma)$ for each $\gamma \in [k]$.

Below we define a new statistical property for (tag-based) key-openable HPS, called *openability*$_k$. It stipulates the statistical indistinguishability between $(\mathsf{sk}^{(0)}, (\pi_\gamma^{(0)})_{\gamma\in[k]})$ and $(\mathsf{sk}^{(1)}, (\pi_\gamma^{(1)})_{\gamma\in[k]})$, where $\mathsf{sk}^{(0)}$ is a uniformly sampled hashing key, $\pi_\gamma^{(0)} = \Lambda_{\mathsf{sk}_0}(x_\gamma)$ for $x_\gamma \leftarrow_\$ \mathcal{X}$ with randomness r_{x_γ}, $\pi_\gamma^{(1)}$ is uniformly sampled from Π with randomness $r_{\pi_\gamma^{(1)}}$, and $\mathsf{sk}^{(1)}$ is generated by $\mathsf{HOpen}_k(\mathsf{td}, \mathsf{pk}, \mathsf{sk}^{(0)}, (x_\gamma, r_{x_\gamma}, \pi_\gamma^{(1)}, r_{\pi_\gamma^{(1)}})_{\gamma\in[k]})$. Here the subscript k indicates the opening of hashing key w.r.t. k hash values. For tag-based key-openable HPS, the adversary can additionally determine the tags $(\tau_\gamma)_{\gamma\in[k]}$ w.r.t. which the hash values are computed. It is not hard to see that this property implies the usual smoothness property of HPS [9] and also implies that $\mathcal{L}$ is a sparse subset of $\mathcal{X}$.

$\underline{\mathbf{Exp}^{\mathrm{open}_k}_{\mathsf{HPS},\mathcal{A}}(\lambda)}$:

$\mathsf{mpar} \leftarrow\!\!\$\ \mathsf{MPar}(1^\lambda)$, $(\mathsf{par}, \mathsf{td}) \leftarrow\!\!\$\ \mathsf{Par}(\mathsf{mpar})$. $\mathsf{sk} \leftarrow\!\!\$\ \mathcal{SK}$, $\mathsf{pk} := \alpha(\mathsf{sk})$.

For $\gamma \in [k]$, $x_\gamma \leftarrow\!\!\$\ \mathcal{X}$ with sampling randomness r_{x_γ}.

$\boxed{(\tau_\gamma)_{\gamma\in[k]} \leftarrow\!\!\$\ \mathcal{A}(\mathsf{mpar}, \mathsf{par}, \mathsf{td}, \mathsf{pk}, (x_\gamma, r_{x_\gamma})_{\gamma\in[k]})}$.

For $\gamma \in [k]$, $\pi^{(0)}_\gamma := \Lambda_{\mathsf{sk}}(x_\gamma, \boxed{\tau_\gamma})$.

For $\gamma \in [k]$, $\pi^{(1)}_\gamma \leftarrow\!\!\$\ \Pi$ with sampling randomness $r_{\pi^{(1)}_\gamma}$.

$\mathsf{sk}^{(0)} := \mathsf{sk}$. $\mathsf{sk}^{(1)} \leftarrow\!\!\$\ \mathsf{HOpen}_k(\mathsf{td}, \mathsf{pk}, \mathsf{sk}, (x_\gamma, r_{x_\gamma}, \pi^{(1)}_\gamma, r_{\pi^{(1)}_\gamma}, \boxed{\tau_\gamma})_{\gamma\in[k]})$.

$b \leftarrow\!\!\$\ \{0,1\}$.

$b' \leftarrow\!\!\$\ \mathcal{A}(\mathsf{mpar}, \mathsf{par}, \mathsf{td}, \mathsf{pk}, (x_\gamma, r_{x_\gamma}, \pi^{(b)}_\gamma)_{\gamma\in[k]}, \mathsf{sk}^{(b)})$.

If $b' = b$: Return 1; Else: Return 0.

Fig. 5 Experiment for defining the Openability$_k$ property of (tag-based) key-openable HPS, where the framed parts only appear in the experiment for tag-based HPS.

$\underline{\mathbf{Exp}^{\mathrm{univ}_{k+1}}_{\mathsf{HPS},\mathcal{A}}(\lambda)}$:

$\mathsf{mpar} \leftarrow\!\!\$\ \mathsf{MPar}(1^\lambda)$, $(\mathsf{par}, \mathsf{td}) \leftarrow\!\!\$\ \mathsf{Par}(\mathsf{mpar})$. $\mathsf{sk} \leftarrow\!\!\$\ \mathcal{SK}$, $\mathsf{pk} := \alpha(\mathsf{sk})$.

For $\gamma \in [k]$, $x_\gamma \leftarrow\!\!\$\ \mathcal{X}$.

$(\tau_\gamma)_{\gamma\in[k]} \leftarrow\!\!\$\ \mathcal{A}(\mathsf{mpar}, \mathsf{par}, \mathsf{pk}, (x_\gamma)_{\gamma\in[k]})$.

For $\gamma \in [k]$, $\pi_\gamma := \Lambda_{\mathsf{sk}}(x_\gamma, \tau_\gamma)$.

$(x, \tau, \pi) \leftarrow\!\!\$\ \mathcal{A}(\mathsf{mpar}, \mathsf{par}, \mathsf{pk}, (x_\gamma, \pi_\gamma)_{\gamma\in[k]})$.

If $(x \in \mathcal{X} \setminus \mathcal{L}) \ \wedge\ (\tau \notin \{\tau_\gamma\}_{\gamma\in[k]}) \ \wedge\ (\pi = \Lambda_{\mathsf{sk}}(x, \tau))$: Return 1; Else: Return 0.

Fig. 6 Experiment for the Universal$_{k+1}$ property of tag-based key-openable HPS.

Definition 9 (Openability$_k$). *A (tag-based) key-openable* HPS *is openable$_k$, if for any (unbounded) adversary $\mathcal{A}$, it holds that* $\boldsymbol{\epsilon}^{\mathrm{open}_k}_{\mathsf{HPS},\mathcal{A}}(\lambda) := |\Pr[\mathbf{Exp}^{\mathrm{open}_k}_{\mathsf{HPS},\mathcal{A}}(\lambda) = 1] - 1/2| \leq \mathsf{negl}(\lambda)$, *where* $\mathbf{Exp}^{\mathrm{open}_k}_{\mathsf{HPS},\mathcal{A}}(\lambda)$ *is defined in Fig. 5.*

Next we define a statistical property for tag-based HPS, called *universal$_{k+1}$*, which is an extension of the universal$_2$ property proposed in [9].

Definition 10 (Universal$_{k+1}$). *A tag-based key-openable* HPS *is universal$_{k+1}$, if for any (unbounded) adversary $\mathcal{A}$, it holds that* $\boldsymbol{\epsilon}^{\mathrm{univ}_{k+1}}_{\mathsf{HPS},\mathcal{A}}(\lambda) := \Pr[\mathbf{Exp}^{\mathrm{univ}_{k+1}}_{\mathsf{HPS},\mathcal{A}}(\lambda) = 1] \leq \mathsf{negl}(\lambda)$, *where* $\mathbf{Exp}^{\mathrm{univ}_{k+1}}_{\mathsf{HPS},\mathcal{A}}(\lambda)$ *is defined in Fig. 6.*

Finally, we define a statistical property, called *efficient randomness resampling on Π*, which demands that besides the (aforementioned) sampling algorithm of Π which samples uniform element $\pi \in \Pi$ with sampling randomness r_π, there is a randomness resampling algorithm ReSmp_Π that takes as input $\pi \in \Pi$ and outputs a sampling randomness r_π. These two ways of sampling/resampling are statistically indistinguishable.

Definition 11 (Efficient Randomness Resampling on Π). *The hash value space Π of* HPS *supports efficient randomness resampling, if there exists a PPT algorithm* ReSmp_Π, *s.t. the statistical distance* $\boldsymbol{\epsilon}^{\Pi\text{-resmp}}_{\mathsf{HPS}}(\lambda) := \Delta((\pi, r_\pi), (\pi', r'_{\pi'})) \leq \mathsf{negl}(\lambda)$, *where* $\mathsf{mpar} \leftarrow\!\!\$\ \mathsf{MPar}(1^\lambda)$, $\pi \leftarrow\!\!\$\ \Pi$ *with sampling randomness* r_π, $\pi' \leftarrow\!\!\$\ \Pi$ *and* $r'_{\pi'} \leftarrow\!\!\$\ \mathsf{ReSmp}_\Pi(\pi')$.

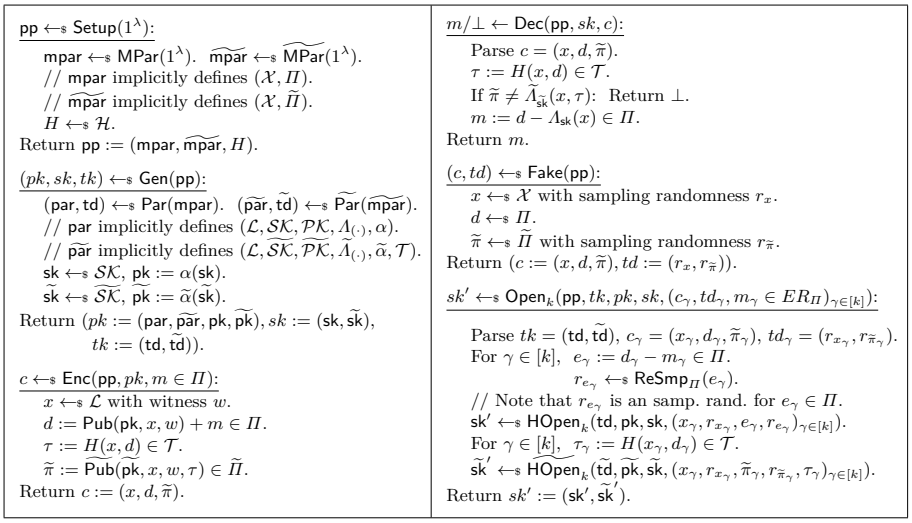

Fig. 7 Construct. of $\mathsf{KM\text{-}NCE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Fake}, \mathsf{Open}_k)$ from $\mathsf{HPS}, \widetilde{\mathsf{HPS}}, \mathcal{H}$.

5.3 Generic Construction of KM-NCE from Key-Openable HPS

The building blocks for constructing KM-NCE are as follows.

- Let $\mathsf{HPS} = (\mathsf{MPar}, \mathsf{Par}, \mathsf{Pub}, \mathsf{Priv}, \mathsf{HOpen}_k)$ be a key-openable HPS, whose hash value space Π is an (additive) group and has an efficient randomness resampling algorithm ReSmp_Π.
- Let $\widetilde{\mathsf{HPS}} = (\widetilde{\mathsf{MPar}}, \widetilde{\mathsf{Par}}, \widetilde{\mathsf{Pub}}, \widetilde{\mathsf{Priv}}, \widetilde{\mathsf{HOpen}}_k)$ be a tag-based key-openable HPS, which shares same universe $\mathcal{X}$ and same language $\mathcal{L}$ with HPS.
- Let $\mathcal{H} = \{H : \mathcal{X} \times \Pi \to \mathcal{T}\}$ be a family of collision-resistant hash functions, where Π is the hash value space of HPS and $\mathcal{T}$ is the tag space of $\widetilde{\mathsf{HPS}}$.

We present the generic construction of $\mathsf{KM\text{-}NCE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Fake}, \mathsf{Open}_k)$ from HPS, $\widetilde{\mathsf{HPS}}$ and $\mathcal{H}$ in Fig. 7. The message space is Π. Note that our generic construction of KM-NCE from key-openable HPS is reminiscent of [11], which constructs PKE scheme from another variant of HPS (the so-called quasi-adaptive HPS).

The perfect correctness of $\mathsf{KM\text{-}NCE}$ follows from those of HPS and $\widetilde{\mathsf{HPS}}$ directly. Next, we show its KMNC_k-CCA security.

Theorem 2 (KMNC_k-CCA security of $\mathsf{KM\text{-}NCE}$). *Assume that (1)* HPS *is openable$_k$, has a hard multi-fold SMP, supports efficient randomness resampling on Π, (2)* $\widetilde{\mathsf{HPS}}$ *is universal$_{k+1}$ and openable$_k$, (3) $\mathcal{H}$ is collision-resistant. Then the* $\mathsf{KM\text{-}NCE}$ *in Fig. 7 is KMNC_k-CCA secure.*

Concretely, for any PPT adversary $\mathcal{A}$ against the KMNC_k-CCA security of $\mathsf{KM\text{-}NCE}$ *that makes at most Q_d decryption queries, there exist PPT adversaries*

$\mathcal{B}_1$, $\mathcal{B}_2$ and unbounded adversaries $\mathcal{B}_3$, $\mathcal{B}_4$, $\mathcal{B}_5$, s.t.

$$\begin{aligned}\mathbf{Adv}^{\text{kmnc-cca}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda) \leq\ & \mathbf{Adv}^{k\text{-msmp}}_{\mathsf{HPS},\mathcal{B}_1}(\lambda) + 2\cdot\mathbf{Adv}^{\text{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda) + 2Q_d\cdot\boldsymbol{\epsilon}^{\text{univ}_{k+1}}_{\widetilde{\mathsf{HPS}},\mathcal{B}_3}(\lambda) \\ &+\ 2\boldsymbol{\epsilon}^{\text{open}_k}_{\mathsf{HPS},\mathcal{B}_4}(\lambda) + 2\boldsymbol{\epsilon}^{\text{open}_k}_{\widetilde{\mathsf{HPS}},\mathcal{B}_5}(\lambda) + 2k\cdot\boldsymbol{\epsilon}^{\Pi\text{-resmp}}_{\mathsf{HPS}}(\lambda).\end{aligned} \tag{2}$$

Proof of Theorem 2. We prove the theorem by defining a sequence of games G_0-G_8, with $\mathsf{G}_0 = \mathbf{Exp}^{\text{kmnc-cca-real}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda)$ and $\mathsf{G}_8 = \mathbf{Exp}^{\text{kmnc-cca-sim}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda)$, and showing adjacent games indistinguishable. By $\Pr_i[\cdot]$ we denote the probability of a particular event occurring in game G_i.

Game G_0: This is the $\mathbf{Exp}^{\text{kmnc-cca-real}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda)$ experiment. Thus, $\Pr[\mathsf{G}_0 = 1] = \Pr[\mathbf{Exp}^{\text{kmnc-cca-real}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda) = 1]$.

In this game, when receiving $(m^*_\gamma)_{\gamma\in[k]}$ from $\mathcal{A}$, the challenger generates c^*_γ using the real encryption algorithm $\mathsf{Enc}(\mathsf{pp}, pk, m^*_\gamma)$. More precisely, it samples $x^*_\gamma \leftarrow_{\$} \mathcal{L}$ with witness w^*_γ, computes $d^*_\gamma := \mathsf{Pub}(\mathsf{pk}, x^*_\gamma, w^*_\gamma) + m^*_\gamma$, $\tau^*_\gamma := H(x^*_\gamma, d^*_\gamma)$, $\widetilde{\pi}^*_\gamma := \widetilde{\mathsf{Pub}}(\widetilde{\mathsf{pk}}, x^*_\gamma, w^*_\gamma, \tau^*_\gamma)$, and sets $c^*_\gamma := (x^*_\gamma, d^*_\gamma, \widetilde{\pi}^*_\gamma)$. It returns $(c^*_\gamma)_{\gamma\in[k]}$ to $\mathcal{A}$. When answering decryption queries $\mathcal{O}_{\text{dec}}(c)$ for $\mathcal{A}$ with $c = (x, d, \widetilde{\pi})$, the challenger computes $\tau := H(x, d)$, and outputs $\perp$ immediately if $c \in \{c^*_\gamma\}_{\gamma\in[k]} \vee \widetilde{\pi} \neq \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x, \tau)$. Otherwise, it computes $m := d - \Lambda_{\mathsf{sk}}(x)$ and returns m to $\mathcal{A}$. In the last step of this game, the challenger sends the real secret key $sk = (\mathsf{sk}, \widetilde{\mathsf{sk}})$ to $\mathcal{A}$.

Game G_1: It is the same as G_0, except that, for each $\gamma \in [k]$, when generating $c^*_\gamma = (x^*_\gamma, d^*_\gamma, \widetilde{\pi}^*_\gamma)$, the challenger computes d^*_γ and $\widetilde{\pi}^*_\gamma$ using $sk = (\mathsf{sk}, \widetilde{\mathsf{sk}})$ instead of using the witness w^*_γ of x^*_γ. Namely, $d^*_\gamma := \Lambda_{\mathsf{sk}}(x^*_\gamma) + m^*_\gamma$ and $\widetilde{\pi}^*_\gamma := \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x^*_\gamma, \tau^*_\gamma)$. By the perfect correctness of HPS and $\widetilde{\mathsf{HPS}}$, this change is conceptual. So $\Pr[\mathsf{G}_1 = 1] = \Pr[\mathsf{G}_0 = 1]$.

Game G_2: It is the same as G_1, except that, for each $\gamma \in [k]$, when generating $c^*_\gamma = (x^*_\gamma, d^*_\gamma, \widetilde{\pi}^*_\gamma)$, the challenger samples $x^*_\gamma \leftarrow_{\$} \mathcal{X}$ instead of $x^*_\gamma \leftarrow_{\$} \mathcal{L}$. Note that neither the witness w^*_γ of x^*_γ (if $x^*_\gamma \leftarrow_{\$} \mathcal{L}$) nor the sampling randomness $r_{x^*_\gamma}$ of x^*_γ (if $x^*_\gamma \leftarrow_{\$} \mathcal{X}$) is needed in G_1 and G_2, thus it is straightforward to construct a PPT adversary $\mathcal{B}_1$ against the multi-fold SMP, such that $|\Pr[\mathsf{G}_2 = 1] - \Pr[\mathsf{G}_1 = 1]| \leq \mathbf{Adv}^{k\text{-msmp}}_{\mathsf{HPS},\mathcal{B}_1}(\lambda)$.

Game G_3: It is the same as G_2, except that, when answering decryption queries $\mathcal{O}_{\text{dec}}(c)$ for $\mathcal{A}$ with $c = (x, d, \widetilde{\pi})$, the challenger adds a new rejection rule: it outputs $\perp$ immediately if $\tau \in \{\tau^*_\gamma\}_{\gamma\in[k]}$, where $\tau = H(x, d)$ and $\tau^*_\gamma = H(x^*_\gamma, d^*_\gamma)$ for each $\gamma \in [k]$.

Let Bad denote the event that $\mathcal{A}$ ever queries $\mathcal{O}_{\text{dec}}(c)$ with $c = (x, d, \widetilde{\pi})$, such that $(x, d) \notin \{(x^*_\gamma, d^*_\gamma)\}_{\gamma\in[k]}$ but $\tau \in \{\tau^*_\gamma\}_{\gamma\in[k]}$. We first show that G_2 and G_3 are identical if Bad does not occur, i.e., either $(x, d) = (x^*_{\gamma_0}, d^*_{\gamma_0})$ for some $\gamma_0 \in [k]$ or $\tau \notin \{\tau^*_\gamma\}_{\gamma\in[k]}$. In the case that $(x, d) = (x^*_{\gamma_0}, d^*_{\gamma_0})$ for some $\gamma_0 \in [k]$, $\mathcal{O}_{\text{dec}}(c)$ would be rejected both in G_2 and G_3 due to $c = c^*_{\gamma_0} \in \{c^*_\gamma\}_{\gamma\in[k]} \vee \widetilde{\pi} \neq \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x, \tau)$. In the case that $\tau \notin \{\tau^*_\gamma\}_{\gamma\in[k]}$, the new rejection rule added in G_3 does not apply, so $\mathcal{O}_{\text{dec}}(c)$ is the same in G_2 and G_3. Overall, G_2 and G_3 are identical when Bad does not occur, thus by the difference lemma, $|\Pr[\mathsf{G}_3 = 1] - \Pr[\mathsf{G}_2 = 1]| \leq \Pr_3[\mathsf{Bad}]$.

To bound $\Pr_3[\mathsf{Bad}]$, it is straightforward to construct a PPT adversary $\mathcal{B}_2$ against the collision resistance of $\mathcal{H}$, so that $\Pr_3[\mathsf{Bad}] \leq \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$. Consequently, $|\Pr[\mathsf{G}_3 = 1] - \Pr[\mathsf{G}_2 = 1]| \leq \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$.

Game G_4: It is the same as G_3, except that, when answering decryption queries $\mathcal{O}_{\mathrm{dec}}(c)$ for $\mathcal{A}$ with $c = (x, d, \widetilde{\pi})$, the challenger adds a second new rejection rule: it outputs $\perp$ immediately if $x \in \mathcal{X} \setminus \mathcal{L}$. We note that this new rule may not be PPT checkable, thus the challenger may not be PPT. This does not matter, since the following arguments (before this rule is removed) are statistical.

Let Forge denote the event that $\mathcal{A}$ ever queries $\mathcal{O}_{\mathrm{dec}}(c)$ with $c = (x, d, \widetilde{\pi})$, such that $\tau \notin \{\tau^*_\gamma\}_{\gamma\in[k]}$, $\widetilde{\pi} = \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x, \tau)$ but $x \in \mathcal{X} \setminus \mathcal{L}$. Clearly, G_3 and G_4 are identical unless Forge occurs, thus by the difference lemma, $|\Pr[\mathsf{G}_4 = 1] - \Pr[\mathsf{G}_3 = 1]| \leq \Pr_4[\mathsf{Forge}]$.

To bound $\Pr_4[\mathsf{Forge}]$, we analyze the information about $\widetilde{\mathsf{sk}}$ that $\mathcal{A}$ may obtain in game G_4 before it finishes the $\mathcal{O}_{\mathrm{dec}}$ queries: $\mathcal{A}$ obtains $\widetilde{\mathsf{pk}} = \alpha(\widetilde{\mathsf{sk}})$ in pk and obtains $\{\widetilde{\pi}^*_\gamma = \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x^*_\gamma, \tau^*_\gamma)\}_{\gamma\in[k]}$ in $\{c^*_\gamma\}_{\gamma\in[k]}$; for $\mathcal{O}_{\mathrm{dec}}$ queries, the challenger will not output m unless $x \in \mathcal{L}$ (due to the new rejection rule added in G_4), thus $\mathcal{O}_{\mathrm{dec}}$ reveals nothing about $\widetilde{\mathsf{sk}}$ beyond $\widetilde{\mathsf{pk}} = \alpha(\widetilde{\mathsf{sk}})$.

Then by the $\mathrm{universal}_{k+1}$ property of tag-based $\widetilde{\mathsf{HPS}}$, for one $\mathcal{O}_{\mathrm{dec}}(c)$ query made by $\mathcal{A}$, it holds that $\tau \notin \{\tau^*_\gamma\}_{\gamma\in[k]}$, $\widetilde{\pi} = \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x, \tau)$ but $x \in \mathcal{X} \setminus \mathcal{L}$ with probability at most $\boldsymbol{\epsilon}^{\mathrm{univ}_{k+1}}_{\widetilde{\mathsf{HPS}},\mathcal{B}_3}(\lambda)$. By a union bound over at most Q_d number of $\mathcal{O}_{\mathrm{dec}}$ queries, we get that $\Pr_4[\mathsf{Forge}] \leq Q_d \cdot \boldsymbol{\epsilon}^{\mathrm{univ}_{k+1}}_{\widetilde{\mathsf{HPS}},\mathcal{B}_3}(\lambda)$. Thus, $|\Pr[\mathsf{G}_4 = 1] - \Pr[\mathsf{G}_3 = 1]| \leq Q_d \cdot \boldsymbol{\epsilon}^{\mathrm{univ}_{k+1}}_{\widetilde{\mathsf{HPS}},\mathcal{B}_3}(\lambda)$. For completeness, we provide a description of the reduction algorithm $\mathcal{B}_3$ in the full version [17].

Game G_5: It is the same as G_4, except that, for each $\gamma \in [k]$, when generating $c^*_\gamma = (x^*_\gamma, d^*_\gamma, \widetilde{\pi}^*_\gamma)$, the challenger samples $d^*_\gamma \leftarrow_{\$} \mathit{\Pi}$ uniformly (instead of $d^*_\gamma := \Lambda_{\mathsf{sk}}(x^*_\gamma) + m^*_\gamma$). Moreover, in the last step of this game, the challenger computes $e^*_\gamma := d^*_\gamma - m^*_\gamma \in \mathit{\Pi}$ and resamples $r_{e^*_\gamma} \leftarrow_{\$} \mathsf{ReSmp}_{\mathit{\Pi}}(e^*_\gamma)$ for each $\gamma \in [k]$, then invokes $\mathsf{sk}' \leftarrow_{\$} \mathsf{HOpen}_k(\mathsf{td}, \mathsf{pk}, \mathsf{sk}, (x^*_\gamma, r_{x^*_\gamma}, e^*_\gamma, r_{e^*_\gamma})_{\gamma\in[k]})$, and sends $(\mathsf{sk}', \widetilde{\mathsf{sk}})$ to $\mathcal{A}$. We have the following lemma whose proof is given in the full version [17].

Lemma 3. *There exists an unbounded $\mathcal{B}_4$ against the openable$_k$ property of HPS, s.t. $|\Pr[\mathsf{G}_5 = 1] - \Pr[\mathsf{G}_4 = 1]| \leq 2 \cdot \boldsymbol{\epsilon}^{\mathrm{open}_k}_{\mathsf{HPS},\mathcal{B}_4}(\lambda) + 2k \cdot \boldsymbol{\epsilon}^{\mathit{\Pi}\text{-resmp}}_{\mathsf{HPS}}(\lambda)$.*

Game G_6: It is the same as G_5, except that, for each $\gamma \in [k]$, when generating $c^*_\gamma = (x^*_\gamma, d^*_\gamma, \widetilde{\pi}^*_\gamma)$, the challenger samples $\widetilde{\pi}^*_\gamma \leftarrow_{\$} \widetilde{\mathit{\Pi}}$ uniformly with randomness $r_{\widetilde{\pi}^*_\gamma}$ (instead of $\widetilde{\pi}^*_\gamma := \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x^*_\gamma, \tau^*_\gamma)$). Moreover, in the last step of this game, the challenger computes $\widetilde{\mathsf{sk}}' \leftarrow_{\$} \widetilde{\mathsf{HOpen}}_k(\widetilde{\mathsf{td}}, \widetilde{\mathsf{pk}}, \widetilde{\mathsf{sk}}, (x^*_\gamma, r_{x^*_\gamma}, \widetilde{\pi}^*_\gamma, r_{\widetilde{\pi}^*_\gamma}, \tau^*_\gamma)_{\gamma\in[k]})$, and sends $(\mathsf{sk}', \widetilde{\mathsf{sk}}')$ to $\mathcal{A}$. We have the following lemma. The proof of this lemma is similar to that of Lemma 3, and is given in the full version [17].

Lemma 4. *There exists an unbounded $\mathcal{B}_5$ against the openable$_k$ property of tag-based $\widetilde{\mathsf{HPS}}$, s.t. $|\Pr[\mathsf{G}_6 = 1] - \Pr[\mathsf{G}_5 = 1]| \leq 2 \cdot \boldsymbol{\epsilon}^{\mathrm{open}_k}_{\widetilde{\mathsf{HPS}},\mathcal{B}_5}(\lambda)$.*

Game G_7: It is the same as G_6, except that, when answering decryption queries $\mathcal{O}_{\mathrm{dec}}(c)$ for $\mathcal{A}$ with $c = (x, d, \widetilde{\pi})$, the challenger removes the second new rejection rule added in G_4. In other words, it does not check whether $x \in \mathcal{L}$ or $x \in \mathcal{X} \setminus \mathcal{L}$ anymore. We note that the challenger in G_7 is now PPT again.

The change from G_6 to G_7 is symmetric to that from G_3 to G_4. By a similar argument, we get $|\Pr[\mathsf{G}_7 = 1] - \Pr[\mathsf{G}_6 = 1]| \leq Q_d \cdot \boldsymbol{\epsilon}^{\mathrm{univ}_{k+1}}_{\widetilde{\mathsf{HPS}},\mathcal{B}_3}(\lambda)$.

Game G_8: It is the same as G_7, except that, when answering decryption queries $\mathcal{O}_{\mathrm{dec}}(c)$ for $\mathcal{A}$ with $c = (x, d, \widetilde{\pi})$, the challenger removes the first new rejection rule added in G_3. In other words, it does not check whether $\tau \in \{\tau^*_\gamma\}_{\gamma\in[k]}$ or not anymore.

The change from G_7 to G_8 is symmetric to the change from G_2 to G_3. Similarly, we have that $|\Pr[\mathsf{G}_8 = 1] - \Pr[\mathsf{G}_7 = 1]| \leq \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$.

Finally, we note that G_8 is exactly the $\mathbf{Exp}^{\text{kmnc-cca-sim}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda)$ experiment.

- For each $\gamma \in [k]$, $c^*_\gamma := (x^*_\gamma, d^*_\gamma, \widetilde{\pi}^*_\gamma)$, where $x^*_\gamma \leftarrow_\$ \mathcal{X}$ with sampling randomness $r_{x^*_\gamma}$, $d^*_\gamma \leftarrow_\$ \Pi$, and $\widetilde{\pi}^*_\gamma \leftarrow_\$ \widetilde{\Pi}$ with randomness $r_{\widetilde{\pi}^*_\gamma}$, the same as the c^*_γ generated by $\mathsf{Fake}(\mathsf{pp})$.
- $\mathcal{O}_{\mathrm{dec}}(c)$ queries are answered by $\mathsf{Dec}(\mathsf{pp}, sk, c)$ when $c \notin \{c^*_\gamma\}_{\gamma\in[k]}$.
- In the last step, $(\mathsf{sk}', \widetilde{\mathsf{sk}}')$ is generated by first computing $e^*_\gamma := d^*_\gamma - m^*_\gamma \in \Pi$ and resampling $r_{e^*_\gamma} \leftarrow_\$ \mathsf{ReSmp}_\Pi(e^*_\gamma)$ for each $\gamma \in [k]$, then invoking $\mathsf{sk}' \leftarrow_\$ \mathsf{HOpen}_k(\mathsf{td}, \mathsf{pk}, \mathsf{sk}, (x^*_\gamma, r_{x^*_\gamma}, e^*_\gamma, r_{e^*_\gamma})_{\gamma\in[k]})$ and $\widetilde{\mathsf{sk}}' \leftarrow_\$ \widetilde{\mathsf{HOpen}}_k(\widetilde{\mathsf{td}}, \widetilde{\mathsf{pk}}, \widetilde{\mathsf{sk}}, (x^*_\gamma, r_{x^*_\gamma}, \widetilde{\pi}^*_\gamma, r_{\widetilde{\pi}^*_\gamma}, \tau^*_\gamma)_{\gamma\in[k]})$ with $\tau^*_\gamma := H(x^*_\gamma, d^*_\gamma)$, the same as $\mathsf{Open}_k(\mathsf{pp}, tk, pk, sk, (c^*_\gamma, r_{c^*_\gamma}, m^*_\gamma)_{\gamma\in[k]})$ where $r_{c^*_\gamma} = (r_{x^*_\gamma}, r_{\widetilde{\pi}^*_\gamma})$.

Thus, $\Pr[\mathsf{G}_8 = 1] = \Pr[\mathbf{Exp}^{\text{kmnc-cca-sim}}_{\mathsf{KM\text{-}NCE},\mathcal{A},k}(\lambda) = 1]$.

Taking all things together, we obtain (2), thus Theorem 2 follows. ■

Finally, we show the robustness.

Theorem 3 (Robustness of KM-NCE). *The proposed* KM-NCE *in Fig. 7 is robust (cf. Definition 5) with* $\boldsymbol{\epsilon}^{\mathrm{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda) \leq 1/|\widetilde{\Pi}|$*, where* $\widetilde{\Pi}$ *is the hash value space of* $\widetilde{\mathsf{HPS}}$.

Proof of Theorem 3. For $\mathsf{pp} \leftarrow_\$ \mathsf{Setup}(1^\lambda)$, $(pk, sk, tk) \leftarrow_\$ \mathsf{Gen}(\mathsf{pp})$, $(c, td) \leftarrow_\$ \mathsf{Fake}(\mathsf{pp})$, we analyze the probability $\boldsymbol{\epsilon}^{\mathrm{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda) = \Pr[\mathsf{Dec}(\mathsf{pp}, sk, c) \neq \perp]$.

- For $(pk, sk, tk) \leftarrow_\$ \mathsf{Gen}(\mathsf{pp})$, we have $sk = (\mathsf{sk}, \widetilde{\mathsf{sk}})$ where $\widetilde{\mathsf{sk}} \leftarrow_\$ \widetilde{\mathcal{SK}}$.
- For $(c, td) \leftarrow_\$ \mathsf{Fake}(\mathsf{pp})$, we have $c = (x, d, \widetilde{\pi})$ where $x \leftarrow_\$ \mathcal{X}$, $d \leftarrow_\$ \Pi$ and $\widetilde{\pi} \leftarrow_\$ \widetilde{\Pi}$.
- Then in $\mathsf{Dec}(\mathsf{pp}, sk, c)$, it first checks whether or not $\widetilde{\pi} = \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x, \tau)$ holds, where $\tau := H(x, d)$, and returns $\perp$ if the check fails.

Since $\widetilde{\pi}$ is uniformly chosen from $\widetilde{\Pi}$ and independent of x, d and $\widetilde{\mathsf{sk}}$, so the check $\widetilde{\pi} = \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x, \tau)$ passes with probability $1/|\widetilde{\Pi}|$. Overall, we have $\boldsymbol{\epsilon}^{\mathrm{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda) = \Pr[\mathsf{Dec}(\mathsf{pp}, sk, c) \neq \perp] \leq \Pr[\widetilde{\pi} = \widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(x, \tau)] = 1/|\widetilde{\Pi}|$. ■

6 Concrete Instantiations

In this section, we show concrete instantiations of key-openable HPS based on the matrix decisional Diffie-Hellman (MDDH) assumption [10]. As a result, we can obtain concrete instantiations of KM-NCE, which in turn yields AC-RSO$_k$&C-CCA secure PKE schemes with compact ciphertexts. For certain instantiation, the resulting PKE can even achieve tight AC-RSO$_k$&C-CCA security.

6.1 Recall: Matrix Distribution

We recall the definition of matrix distribution defined in [10].

In this section, we use bold uppercase letters to represent matrices and bold lowercase letters to represent (column) vectors. Let GGen be a PPT algorithm that on input 1^λ returns $\mathcal{G} = (\mathbb{G}, q, P)$, a description of an (additive) cyclic group $\mathbb{G}$ with a generator P of order q which is a λ-bit prime. For $a \in \mathbb{Z}_q$, define $[a] := aP \in \mathbb{G}$ as the *implicit representation* of a in $\mathbb{G}$. More generally, for a matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n\times m}$, we define $[\mathbf{A}]$ as the implicit representation of $\mathbf{A}$ in $\mathbb{G}$, i.e., $[\mathbf{A}] := (a_{ij}P) \in \mathbb{G}^{n\times m}$. Note that from $[a] \in \mathbb{G}$ it is generally hard to compute the value a (discrete logarithm problem is hard in $\mathbb{G}$). Obviously, given $[a], [b] \in \mathbb{G}$ and a scalar $x \in \mathbb{Z}$, one can efficiently compute $[ax] \in \mathbb{G}$ and $[a + b] \in \mathbb{G}$. Similarly, for $\mathbf{A} \in \mathbb{Z}_q^{m\times n}, \mathbf{B} \in \mathbb{Z}_q^{n\times t}, \mathbf{AB} \in \mathbb{Z}_q^{m\times t}$, given $[\mathbf{A}], \mathbf{B}$ one can efficiently compute $[\mathbf{A}]\mathbf{B} := [\mathbf{AB}] \in \mathbb{G}^{m\times t}$ and given $\mathbf{A}, [\mathbf{B}]$, one can efficiently compute $\mathbf{A}[\mathbf{B}] := [\mathbf{AB}] \in \mathbb{G}^{m\times t}$.

Definition 12 (Matrix Distribution). *Let $d, k \in \mathbb{N}^+$. $\mathcal{D}_{d+k,d}$ is called a* matrix distribution *if it outputs matrices in $\mathbb{Z}_q^{(d+k)\times d}$ of full rank d in polynomial time.*

As in [10], let $\mathcal{U}_{d+k,d}$ be the uniform distribution over $\mathbb{Z}_q^{(d+k)\times d}$. Without loss of generality, for $\mathbf{A} \leftarrow_\$ \mathcal{D}_{d+k,d}$, we assume that $\overline{\mathbf{A}}$ (the upper square submatrix of $\mathbf{A}$) is invertible.

Definition 13 (The $\mathcal{D}_{d+k,d}$-Matrix Decision Diffie-Hellman Assumption, $\mathcal{D}_{d+k,d}$-MDDH). *Let $\mathcal{D}_{d+k,d}$ be a matrix distribution. The $\mathcal{D}_{d+k,d}$-*Matrix Decision Diffie-Hellman ($\mathcal{D}_{d+k,d}$-MDDH) Assumption *holds relative to GGen if for each PPT adversary $\mathcal{A}$, the advantage*

$$\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{D}_{d+k,d},\mathsf{GGen},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}], [\mathbf{Aw}]) = 1] - \Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}], [\mathbf{u}]) = 1]|$$

is negligible, where the probability is taken over $\mathcal{G} \leftarrow_\$ \mathsf{GGen}(1^\lambda), \mathbf{A} \leftarrow_\$ \mathcal{D}_{d+k,d}$, $\mathbf{w} \leftarrow_\$ \mathbb{Z}_q^d$ and $\mathbf{u} \leftarrow_\$ \mathbb{Z}_q^{d+k}$.

As shown in [10], $\mathcal{D}_{d+k,d}$-MDDH assumption is a generalization of a large range of assumptions. By setting the matrix distribution $\mathcal{D}_{\ell,k}$ to specific distributions, $\mathcal{D}_{d+k,d}$-MDDH assumption can capture DDH assumption, k-Linear assumption, k-Cascade assumption and many other assumptions.

The MDDH assumption can be generalized into a multi-instance version. We recall the Q-fold MDDH assumption as defined in [10].

Definition 14 (Q-fold $\mathcal{D}_{d+k,d}$-Matrix Decision Diffie-Hellman Assumption). *Let Q be a positive integer and $\mathcal{D}_{d+k,d}$ be a matrix distribution. The* Q-fold $\mathcal{D}_{d+k,d}$-Matrix Decision Diffie-Hellman Assumption *holds relative to* GGen *if for each PPT adversary $\mathcal{A}$, the advantage*

$$\mathbf{Adv}^{\text{Q-mddh}}_{\mathcal{D}_{d+k,d},\mathsf{GGen},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(\mathcal{G},[\mathbf{A}],[\mathbf{AW}])=1]-\Pr[\mathcal{A}(\mathcal{G},[\mathbf{A}],[\mathbf{U}])=1]|$$

is negligible, where the probability is taken over $\mathcal{G}\leftarrow_{\$}\mathsf{GGen}(1^{\lambda}),\mathbf{A}\leftarrow_{\$}\mathcal{D}_{d+k,d}$, $\mathbf{W}\leftarrow_{\$}\mathbb{Z}_q^{d\times Q}$ and $\mathbf{U}\leftarrow_{\$}\mathbb{Z}_q^{(d+k)\times Q}$.

6.2 Openable$_k$ HPS Instantiation

In this subsection, we provide a key-openable HPS instantiation with openable$_k$ and efficient randomness resampling properties based on the MDDH assumption. This HPS can be seen as a generalization of the DDH-based HPS in [9]. Inspired by the technique in [12,15], we are able to make the hash value space of our HPS to be compact and efficient randomness resamplable. Meanwhile, this does not affect the openability of our HPS.

More precisely, fixing some group generation algorithm GGen, some positive integers d,k, some matrix distribution $\mathcal{D}_{d+k,d}$ and some polynomial $l=l(\lambda)$ (which can be set as the desired message length of the PKE scheme), consider $\mathsf{HPS}=(\mathsf{MPar},\mathsf{Par},\mathsf{Pub},\mathsf{Priv},\mathsf{HOpen}_k)$ in the following.

- $\mathsf{MPar}(1^{\lambda})$. The master parameter generation algorithm runs $\mathcal{G}=(\mathbb{G},q,P)\leftarrow_{\$}\mathsf{GGen}(1^{\lambda})$. Let $\mathcal{H}_{\mathsf{u}}=\{\mathsf{H}_{\mathsf{u}}:\mathbb{G}\rightarrow\{0,1\}\}$ be a family of universal hash functions based on group $\mathbb{G}$. The algorithm selects $\mathsf{H}_{\mathsf{u}}\leftarrow_{\$}\mathcal{H}_{\mathsf{u}}$ and returns $\mathsf{mpar}:=(\mathcal{G},d,k,l,\mathcal{D}_{d+k,d},\mathsf{H}_{\mathsf{u}})$ which implicitly defines the instance space $\mathcal{X}:=\mathbb{G}^{d+k}$ with randomness space $R_{\mathcal{X}}:=\mathbb{Z}_q^{d+k}$ and the hash value space $\Pi:=\{0,1\}^l$ with randomness space $R_{\Pi}:=\mathbb{Z}_q^l$. Given mpar, one can efficiently sample a uniform element x from $\mathcal{X}$ by selecting $r_x=\mathbf{x}\leftarrow_{\$}R_{\mathcal{X}}$ and setting $x:=[r_x]=[\mathbf{x}]$. For simplicity, we define an efficiently computable function $\mathsf{H}_{\mathsf{u},l}:\mathbb{G}^l\rightarrow\{0,1\}^l$ where $\mathsf{H}_{\mathsf{u},l}([\mathbf{a}]):=(\mathsf{H}_{\mathsf{u}}([a_1]),\cdots,\mathsf{H}_{\mathsf{u}}([a_l]))$ for all $[\mathbf{a}]=[a_1,\cdots,a_l]\in\mathbb{G}^l$. Then, one can also efficiently sample a uniform element π from Π by selecting $r_{\pi}=\boldsymbol{\pi}\leftarrow_{\$}R_{\Pi}$ and setting $\pi:=\mathsf{H}_{\mathsf{u},l}([\boldsymbol{\pi}])\in\Pi$.[6]
- $\mathsf{Par}(\mathsf{mpar})$. The (ordinary) parameter generation algorithm selects matrix $\mathbf{A}\in\mathbb{Z}_q^{(d+k)\times d}\leftarrow_{\$}\mathcal{D}_{d+k,d}$, then it returns $\mathsf{par}:=[\mathbf{A}]$ and $\mathsf{td}:=\mathbf{A}$.
  The public parameter par (together with mpar) implicitly defines the language as $\mathcal{L}:=[\mathsf{span}(\mathbf{A})]=\{[\mathbf{Aw}]\mid\mathbf{w}\in\mathbb{Z}_q^d\}$. The hashing key space $\mathcal{SK}:=\mathbb{Z}_q^{(d+k)\times l}$ and the projection key space $\mathcal{PK}:=\mathbb{G}^{d\times l}$. The projection function α maps $\mathsf{sk}=\mathbf{S}\in\mathcal{SK}$ to $\mathsf{pk}=[\mathbf{P}]\in\mathcal{PK}$ where $[\mathbf{P}]=[\mathbf{A}^{\top}]\mathbf{S}$ and α is efficiently computable given par and sk. For $\mathsf{sk}=\mathbf{S}\in\mathcal{SK}$, the hash

[6] Actually, π is only statistical close to uniform. According to the leftover hash lemma together with the union bound, the statistically distance between π and uniform distribution over Π is bounded by $\frac{l}{2}\sqrt{\frac{2}{q}}$, which is exponentially small for polynomially bounded l. Therefore, we omit this statistical distance here.

$\mathsf{ReSmp}_{\Pi}(\mathbf{b}=(b_1,\cdots,b_l)\in\{0,1\}^l)$:	$\mathsf{OnebitReSmp}(\mathsf{H}_\mathsf{u}, b_i\in\{0,1\})$:
//Implicit input: $\mathsf{H}_\mathsf{u}\in\mathsf{mpar}$	For $j\in\{1,\cdots,\lambda\}$:
For $i\in\{1,\cdots,l\}$:	$r_j\leftarrow\$\ \mathbb{Z}_q$
$r_i\leftarrow\$\ \mathsf{OnebitReSmp}(\mathsf{H}_\mathsf{u}, b_i)$	If $\mathsf{H}_\mathsf{u}([r_j])=b_i$: Return r_j
Return $\mathbf{r}:=(r_1,\cdots,r_l)$	Return $\perp$

Fig. 8 Randomness resample algorithm ReSmp_{Π} for hash value space $\Pi=\{0,1\}^l$ of the hash proof system HPS. The algorithm $\mathsf{OnebitReSmp}$ will return $\perp$ and terminate after λ iterations, which makes it a polynomial-time algorithm.

function $\Lambda_{\mathsf{sk}}(\cdot)$ maps an element $x=[\mathbf{x}]\in\mathcal{X}$ to $\mathsf{H}_{\mathsf{u},l}(\mathbf{S}^\top[\mathbf{x}])\in\Pi$ and it is efficiently computable given sk and x.
Given par, one can efficiently sample a uniform element x from language $\mathcal{L}$ together with a witness w by choosing $w=\mathbf{w}\leftarrow\$\ \mathbb{Z}_q^d$ and computing $x=[\mathbf{x}]=[\mathbf{A}]\mathbf{w}$.

- $\mathsf{Pub}(\mathsf{pk},x,w)$. Given public key $\mathsf{pk}=[\mathbf{P}]\in\mathcal{PK}$, an instance $x=[\mathbf{x}]=[\mathbf{A}\mathbf{w}]\in\mathcal{L}$, and its witness $w=\mathbf{w}$, the public evaluation algorithm outputs $\pi=\mathsf{H}_{\mathsf{u},l}([\mathbf{P}^\top]\mathbf{w})\in\Pi$.
- $\mathsf{Priv}(\mathsf{sk},x)$. Given secret key $\mathsf{sk}=\mathbf{S}\in\mathcal{SK}$ and $x=[\mathbf{x}]\in\mathcal{X}$, the private evaluation algorithm outputs $\pi=\mathsf{H}_{\mathsf{u},l}(\mathbf{S}^\top[\mathbf{x}])\in\Pi$.
- $\mathsf{HOpen}_k(\mathsf{td},\mathsf{pk},\mathsf{sk},(x_\gamma,r_{x_\gamma},\pi_\gamma,r_{\pi_\gamma})_{\gamma\in\{1,\cdots,k\}})$. Given $\mathsf{td}=\mathbf{A},\mathsf{pk}=[\mathbf{P}],\mathsf{sk}=\mathbf{S},x_\gamma=[\mathbf{x}_\gamma],r_{x_\gamma}=\mathbf{x}_\gamma,\pi_\gamma=\mathsf{H}_{\mathsf{u},l}([\boldsymbol{\pi}_\gamma])$ and $r_{\pi_\gamma}=\boldsymbol{\pi}_\gamma\in\mathbb{Z}_q^l$ for all $\gamma\in\{1,\cdots,k\}$, the open algorithm computes $\mathsf{sk}'=\mathbf{S}'\in\mathbb{Z}_q^{(d+k)\times l}$ by solving the following system of linear equations,

$$\mathbf{S}'^\top(\mathbf{A}\mid\mathbf{x}_1\mid\cdots\mid\mathbf{x}_k)=(\mathbf{S}^\top\mathbf{A}\mid\boldsymbol{\pi}_1\mid\cdots\mid\boldsymbol{\pi}_k)\bmod q. \tag{3}$$

Note that, given $\mathsf{td}=\mathbf{A}$ and the randomnesses $(r_{x_\gamma}=\mathbf{x}_\gamma)_{\gamma\in\{1,\cdots,k\}}$, one can easily compute the square matrix $\mathbf{M}=(\mathbf{A}\mid\mathbf{x}_1\mid\cdots\mid\mathbf{x}_k)\in\mathbb{Z}_q^{(d+k)\times(d+k)}$. If $\mathbf{M}$ is invertible, one can easily compute and output $\mathbf{S}'^\top=(\mathbf{S}^\top\mathbf{A}\mid\boldsymbol{\pi}_1\mid\cdots\mid\boldsymbol{\pi}_k)\cdot\mathbf{M}^{-1}\bmod q$. If $\mathbf{M}$ is not invertible, algorithm HOpen_k outputs $\perp$.

Note that the hash value space $\Pi=\{0,1\}^l$ is an additive group with group operation $\oplus$ (string xor). We define its randomness resample algorithm ReSmp_{Π} in Fig. 8.

Theorem 4. *The above instantiation* HPS *(1) is a key-openable HPS; (2) has a hard multi-fold SMP under the multi-fold* $\mathcal{D}_{d+k,d}$-MDDH *assumption (i.e., for any PPT adversary* $\mathcal{A}$*, there exists a PPT adversary* $\mathcal{B}$ *such that* $\mathbf{Adv}^{k\text{-msmp}}_{\mathsf{HPS},\mathcal{A}}(\lambda)\le\mathbf{Adv}^{k\text{-mddh}}_{\mathcal{D}_{d+k,d},\mathsf{GGen},\mathcal{B}}(\lambda)$*); (3) is openable*$_k$ *and (4) supports efficient randomness resampling on* Π *with algorithm* ReSmp_{Π}*.*

We put the proof of Theorem 4 in the full version [17].

6.3 Openable$_k$ and Universal$_{k+1}$ Tag-based HPS Instantiation

In this subsection, we provide a tag-based key-openable HPS instantiation with both openable$_k$ and universal$_{k+1}$ properties based on the MDDH assumption.

This tag-based HPS can be seen as a generalization of the tag-based HPS from the DDH assumption in [9]. More precisely, fixing some group generation algorithm GGen, some positive integers d, k and some matrix distribution $\mathcal{D}_{d+k,d}$, consider instantiation $\widetilde{\mathsf{HPS}} = (\widetilde{\mathsf{MPar}}, \widetilde{\mathsf{Par}}, \widetilde{\mathsf{Pub}}, \widetilde{\mathsf{Priv}}, \widetilde{\mathsf{HOpen}}_k)$ in the following.

- $\widetilde{\mathsf{MPar}}(1^\lambda)$. The master parameter generation algorithm runs $\mathcal{G} = (\mathbb{G}, q, P) \leftarrow_\$ \mathsf{GGen}(1^\lambda)$ and returns $\widetilde{\mathsf{mpar}} := (\mathcal{G}, d, k, \mathcal{D}_{d+k,d})$ which implicitly defines the instance space $\mathcal{X} := \mathbb{G}^{d+k}$ with randomness space $R_{\mathcal{X}} := \mathbb{Z}_q^{d+k}$ and the hash value space $\widetilde{\Pi} := \mathbb{G}$ with randomness space $R_{\widetilde{\Pi}} := \mathbb{Z}_q$.[7] Given mpar, one can efficiently sample a uniform element x from $\mathcal{X}$ by selecting $r_x = \mathbf{x} \leftarrow_\$ R_{\mathcal{X}}$ and set $x = [r_x] = [\mathbf{x}]$. One can also efficiently sample a uniform element $\widetilde{\pi}$ from $\widetilde{\Pi}$ by selecting $r_{\widetilde{\pi}} \leftarrow_\$ R_{\widetilde{\Pi}}$ and set $\widetilde{\pi} = [r_{\widetilde{\pi}}]$.
- $\widetilde{\mathsf{Par}}(\widetilde{\mathsf{mpar}})$. The (ordinary) parameter generation algorithm selects matrix $\mathbf{A} \in \mathbb{Z}_q^{(d+k)\times d} \leftarrow_\$ \mathcal{D}_{d+k,d}$, then it returns $\widetilde{\mathsf{par}} := [\mathbf{A}]$ and $\widetilde{\mathsf{td}} := \mathbf{A}$.
  The public parameter $\widetilde{\mathsf{par}}$ (together with $\widetilde{\mathsf{mpar}}$) implicitly defines the language as $\mathcal{L} := [\mathsf{span}(\mathbf{A})] = \{[\mathbf{Aw}] \mid \mathbf{w} \in \mathbb{Z}_q^d\}$.[8] The hashing key space $\widetilde{\mathcal{SK}} := \mathbb{Z}_q^{2d+2k}$ and the projection key space $\widetilde{\mathcal{PK}} := \mathbb{G}^{2d}$. The projection function $\widetilde{\alpha}$ maps $\widetilde{\mathsf{sk}} = \mathbf{s} = \begin{pmatrix}\mathbf{s}_1\\ \mathbf{s}_2\end{pmatrix} \in \widetilde{\mathcal{SK}}$ (where $\mathbf{s}_1, \mathbf{s}_2 \in \mathbb{Z}_q^{d+k}$) to $\widetilde{\mathsf{pk}} = [\mathbf{p}] = \begin{bmatrix}\mathbf{p}_1\\ \mathbf{p}_2\end{bmatrix} = \begin{bmatrix}\mathbf{A}^\top & \\ & \mathbf{A}^\top\end{bmatrix}\mathbf{s} \in \widetilde{\mathcal{PK}}$ (where $[\mathbf{p}_i] = \left[\mathbf{A}^\top \mathbf{s}_i\right] \in \mathbb{G}^d$ for $i \in \{1, 2\}$) and $\widetilde{\alpha}$ is efficiently computable given $\widetilde{\mathsf{par}}$ and $\widetilde{\mathsf{sk}}$. The tag space is $\mathcal{T} := \mathbb{Z}_q$. For $\widetilde{\mathsf{sk}} = \mathbf{s} \in \widetilde{\mathcal{SK}}$, the hash function $\widetilde{\Lambda}_{\widetilde{\mathsf{sk}}}(\cdot,\cdot)$ maps an element $x = [\mathbf{x}] \in \mathcal{X}$ together with a tag $\tau \in \mathcal{T}$ to $\widetilde{\pi} = \mathbf{s}^\top \begin{bmatrix}\mathbf{x}\\ \tau\mathbf{x}\end{bmatrix} = \left[\mathbf{s}_1^\top \mathbf{x} + \tau \mathbf{s}_2^\top \mathbf{x}\right] \in \widetilde{\Pi}$ and it is efficiently computable given $\widetilde{\mathsf{sk}}, x$ and τ.
  Given $\widetilde{\mathsf{par}}$, one can efficiently sample a uniform element x from language $\mathcal{L}$ together with a witness w by choosing $w = \mathbf{w} \leftarrow_\$ \mathbb{Z}_q^d$ and computing $x = [\mathbf{x}] = [\mathbf{Aw}]$.
- $\widetilde{\mathsf{Pub}}(\widetilde{\mathsf{pk}}, x, w, \tau)$. Given public key $\widetilde{\mathsf{pk}} = [\mathbf{p}]$, witness $w = \mathbf{w}$ of instance $x = [\mathbf{Aw}]$ and tag τ, the public evaluation algorithm outputs the hash value $\widetilde{\pi} = \left[\mathbf{p}^\top\right]\begin{pmatrix}\mathbf{w}\\ \tau\mathbf{w}\end{pmatrix}$.
- $\widetilde{\mathsf{Priv}}(\widetilde{\mathsf{sk}}, x, \tau)$. Given secret key $\widetilde{\mathsf{sk}} = \mathbf{s}$, $x = [\mathbf{x}]$ and tag τ, the private evaluation algorithm outputs $\widetilde{\pi} = \mathbf{s}^\top \begin{bmatrix}\mathbf{x}\\ \tau\mathbf{x}\end{bmatrix}$.
- $\widetilde{\mathsf{HOpen}}_k(\widetilde{\mathsf{td}}, \widetilde{\mathsf{pk}}, \widetilde{\mathsf{sk}}, (x_\gamma, r_{x_\gamma}, \widetilde{\pi}_\gamma, r_{\widetilde{\pi}_\gamma}, \tau_\gamma)_{\gamma\in\{1,\cdots,k\}})$. Given trapdoor $\widetilde{\mathsf{td}} = \mathbf{A}$, public key $\widetilde{\mathsf{pk}} = [\mathbf{p}]$, secret key $\widetilde{\mathsf{sk}} = \mathbf{s}$, instance $x_\gamma = [\mathbf{x}_\gamma]$ with random-

[7] To get an instantiation $\widetilde{\mathsf{HPS}}$ which satisfies the conditions of Theorem 2, $\widetilde{\mathsf{HPS}}$ needs to share the same universe set $\mathcal{X}$ with HPS. In that way, we can set $(\mathcal{G}, d, k, \mathcal{D}_{d+k,d})$ in $\widetilde{\mathsf{mpar}}$ to be exactly the same with the ones in mpar.

[8] Similarly, we set $\widetilde{\mathsf{par}} := \mathsf{par}$ and $\widetilde{\mathsf{td}} := \mathsf{td}$ to make sure $\widetilde{\mathsf{HPS}}$ shares the same language $\mathcal{L}$ with HPS.

ness $r_{x_\gamma} = \mathbf{x}_\gamma$, hash value $\widetilde{\pi}_\gamma = [r_{\widetilde{\pi}_\gamma}]$ with randomness $r_{\widetilde{\pi}_\gamma}$ and tag τ_γ for all $\gamma \in \{1, \cdots, k\}$, the open algorithm computes $\widetilde{\mathsf{sk}}' = \mathbf{s}' \in \mathbb{Z}_q^{2d+2k}$ by solving the following system of linear equations.

$$\mathbf{s}'^{\top}\mathbf{E} = (\mathbf{s}_1^{\top}\mathbf{A},\ \mathbf{s}_2^{\top}\mathbf{A},\ r_{\widetilde{\pi}_1}, \cdots,\ r_{\widetilde{\pi}_k}) \bmod q,\ \mathbf{E} = \begin{pmatrix} \mathbf{A} & \mathbf{x}_1 & \cdots & \mathbf{x}_k \\ & \mathbf{A} & \tau_1\mathbf{x}_1 & \cdots \tau_k\mathbf{x}_k \end{pmatrix}. \tag{4}$$

Matrix $\mathbf{E}$ has $2d + 2k$ rows and $2d + k$ columns.

- If matrix $(\mathbf{A} \mid \mathbf{x}_1 \mid \cdots \mid \mathbf{x}_k)$ has full column rank $d + k$, then matrix $\mathbf{E}$ has full column rank $2d + k$ and there are q^k possible solutions for $\mathbf{s}'$ to make Equation (4) hold. Algorithm $\widetilde{\mathsf{HOpen}}_k$ selects and outputs a uniformly random solution.
- Otherwise, algorithm $\widetilde{\mathsf{HOpen}}_k$ outputs $\perp$.

Note that given $\widetilde{\mathsf{td}} = \mathbf{A}$, tags $(\tau_\gamma)_{\gamma\in\{1,\cdots,k\}}$ and the randomnesses $(r_{x_\gamma} = \mathbf{x}_\gamma)_{\gamma\in\{1,\cdots,k\}}$, one can easily compute the matrix $\mathbf{E}$. The right hand side of Equation (4) is also efficiently computable given $\widetilde{\mathsf{sk}} = \begin{pmatrix} \mathbf{s}_1 \\ \mathbf{s}_2 \end{pmatrix}$ and randomnesses $(r_{\widetilde{\pi}_\gamma})_{\gamma\in\{1,\cdots,k\}}$.

Theorem 5. *The above instantiation $\widetilde{\mathsf{HPS}}$ (1) is a tag-based key-openable HPS; (2) is universal$_{k+1}$ and (3) is openable$_k$.*

We put the proof of Theorem 5 in the full version [17].

6.4 Concrete AC-RSO$_k$&C-CCA secure PKE Instantiation

We instantiate our PKE scheme by plugging the instantiations, HPS in Section 6.2 and $\widetilde{\mathsf{HPS}}$ in Section 6.3, into the generic KM-NCE construction in Fig. 7. By Theorem 1, we immediately get a PKE instantiation that can achieve AC-RSO$_k$&C-CCA security in the standard model with *compact* ciphertexts. If we set the matrix distribution $\mathcal{D}_{d+k,d}$ (i.e., the matrix distribution used to sample matrix $\mathbf{A}$ by the key generation algorithm Gen) to be uniform matrix distribution $\mathcal{U}_{d+k,d}$, the resulting PKE can achieve *tight* AC-RSO$_k$&C-CCA security.

Fixing some group generation algorithm GGen, some positive integers d, k, some matrix distribution $\mathcal{D}_{d+k,d}$ and some polynomial $l = l(\lambda)$, the instantiation $\mathsf{PKE} = (\mathsf{Setup}, \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\{0,1\}^l$ is shown in Fig. 9. This scheme can be viewed as a generalization of the DDH-based scheme in [12, Fig. 3] and both schemes are variants of the Cramer-Shoup encryption scheme [9].

We can see that, for the PKE scheme in Fig. 9, the ciphertext length is $(d + k + 1) \times |\mathbb{G}| + l$ for messages of length l and the ciphertext overhead is the size of a constant number of group elements (since d and k are both fixed constants), which is also independent of the message length. This suggests that the PKE instantiation in Fig. 9 has compact ciphertexts [15,12].

We note that our PKE can achieve *tight* AC-RSO$_k$&C-CCA security for certain instantiation. Taking a closer look at the AC-RSO$_k$&C-CCA security of our

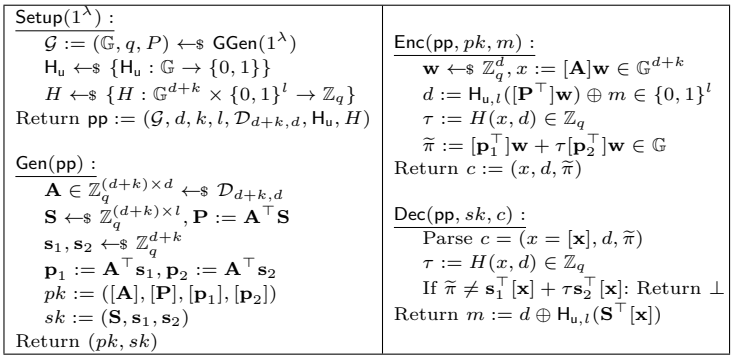

Fig. 9 Concrete AC-RSO$_k$&C-CCA secure PKE instantiation.

MDDH-based PKE instantiation, we obtain the following inequality by combining Eq. (1) in Theorem 1, Eq. (2) in Theorem 2 and Theorem 4 together.

$$\begin{aligned}
&\mathbf{Adv}^{\text{ac-rso\&c-cca}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},\mathcal{D},n,t,k}(\lambda) \leq n \cdot \mathbf{Adv}^{\text{kmnc-cca}}_{\mathsf{KM\text{-}NCE},\mathcal{B}',k}(\lambda) + n \cdot t \cdot k \cdot \boldsymbol{\epsilon}^{\text{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda) \\
&\leq n \cdot \mathbf{Adv}^{k\text{-mddh}}_{\mathcal{D}_{d+k,d},\mathsf{GGen},\mathcal{B}_1}(\lambda) + 2n \cdot \mathbf{Adv}^{\text{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda) + 2Q_d n \cdot \boldsymbol{\epsilon}^{\text{univ}_{k+1}}_{\widetilde{\mathsf{HPS}},\mathcal{B}_3}(\lambda) + \ 2n \cdot \boldsymbol{\epsilon}^{\text{open}_k}_{\mathsf{HPS},\mathcal{B}_4}(\lambda) \\
&\quad + 2n \cdot \boldsymbol{\epsilon}^{\text{open}_k}_{\widetilde{\mathsf{HPS}},\mathcal{B}_5}(\lambda) + 2kn \cdot \boldsymbol{\epsilon}^{\Pi\text{-resmp}}_{\mathsf{HPS}}(\lambda) + n \cdot t \cdot k \cdot \boldsymbol{\epsilon}^{\text{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda). \qquad (5)
\end{aligned}$$

The $2Q_d n \cdot \boldsymbol{\epsilon}^{\text{univ}_{k+1}}_{\widetilde{\mathsf{HPS}},\mathcal{B}_3}(\lambda) + \ 2n \cdot \boldsymbol{\epsilon}^{\text{open}_k}_{\mathsf{HPS},\mathcal{B}_4}(\lambda) + 2n \cdot \boldsymbol{\epsilon}^{\text{open}_k}_{\widetilde{\mathsf{HPS}},\mathcal{B}_5}(\lambda) + 2kn \cdot \boldsymbol{\epsilon}^{\Pi\text{-resmp}}_{\mathsf{HPS}}(\lambda) + n \cdot t \cdot k \cdot \boldsymbol{\epsilon}^{\text{rob}}_{\mathsf{KM\text{-}NCE}}(\lambda)$ part in equation (5) does not affect tightness of the reduction since it is statistically small. Only reductions to computational properties matter to tightness of the reduction, i.e., the term $n \cdot \mathbf{Adv}^{k\text{-mddh}}_{\mathcal{D}_{d+k,d},\mathsf{GGen},\mathcal{B}_1}(\lambda) + 2n \cdot \mathbf{Adv}^{\text{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$. This security loss n and $2n$ are introduced because 1) in the proof of Theorem 1 (KMNC$_k$-CCA + robustness $\Rightarrow$ AC-RSO$_k$&C-CCA), we handle one user at a time with n game transitions (cf. Lemma 1), and in each transition, a term $\mathbf{Adv}^{\text{kmnc-cca}}_{\mathsf{KM\text{-}NCE},\mathcal{B}'_1,k}(\lambda)$ is incurred; 2) according to Theorem 2, the term $\mathbf{Adv}^{\text{kmnc-cca}}_{\mathsf{KM\text{-}NCE},\mathcal{B}'_1,k}(\lambda)$ contains $\mathbf{Adv}^{k\text{-msmp}}_{\mathsf{HPS},\mathcal{B}''_1}(\lambda) + 2 \cdot \mathbf{Adv}^{\text{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$; and 3) according to Theorem 4, $\mathbf{Adv}^{k\text{-msmp}}_{\mathsf{HPS},\mathcal{B}''_1}(\lambda) \leq \mathbf{Adv}^{k\text{-mddh}}_{\mathcal{D}_{d+k,d},\mathsf{GGen},\mathcal{B}_1}(\lambda)$.

Alternatively, if we set the matrix distribution to be uniform matrix distribution (i.e., $\mathcal{D}_{d+k,d} := \mathcal{U}_{d+k,d}$), we can avoid such security loss by integrating the proofs of Theorem 1, Theorem 2 and Theorem 4. We can handle the n reductions to the k-fold $\mathcal{U}_{d+k,d}$-MDDH assumption (i.e., $n \cdot \mathbf{Adv}^{k\text{-mddh}}_{\mathcal{U}_{d+k,d},\mathsf{GGen},\mathcal{B}_1}(\lambda)$) and the $2n$ reductions to the collision-resistance of $\mathcal{H}$ (i.e., $2n \cdot \mathbf{Adv}^{\text{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$) *for all n users at one time* (while keeping the reductions to other statistical properties unchanged, namely one user at a time). Specifically,

- we can change all the kn ciphertexts (of all n users) at one time, corresponding to the game transition G_1 to G_2 in the proof of Theorem 2, and the indistinguishability can be reduced to the $\mathcal{U}_{d+k,d}$-MDDH assumption using Lemma 5 in below;

– we can handle collisions of all users at one time, corresponding to the game transitions G_2 to G_3 and G_7 to G_8 in the proof of Theorem 2.

With this strategy, we obtain a tight reduction with $\mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{U}_{d+k,d},\mathsf{GGen},\mathcal{B}_1}(\lambda) + 2 \cdot \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$, instead of $n \cdot \mathbf{Adv}^{k\text{-mddh}}_{\mathcal{U}_{d+k,d},\mathsf{GGen},\mathcal{B}_1}(\lambda) + 2n \cdot \mathbf{Adv}^{\mathrm{cr}}_{\mathcal{H},\mathcal{B}_2}(\lambda)$, to the computational properties. Thus, the PKE scheme enjoys tight security reduction.

Lemma 5. *For any adversary $\mathcal{A}$, any positive integer d, k, n, any matrix distribution $\mathcal{D}_{d+k,d}$ and any group generation algorithm GGen, we define the advantage $\mathbf{Adv}^{(n,k)\text{-mddh}}_{\mathcal{D}_{d+k,d},\mathsf{GGen},\mathcal{A}}(\lambda) := |\Pr[\mathcal{A}(\mathcal{G}, ([\mathbf{A}_i], [\mathbf{X}_i])_{i=1}^n) = 1] - \Pr[\mathcal{A}(\mathcal{G}, ([\mathbf{A}_i], [\mathbf{X}'_i])_{i=1}^n) = 1]|$ where $\mathcal{G} \leftarrow_{\$} \mathsf{GGen}(1^\lambda), \mathbf{A}_i \leftarrow_{\$} \mathcal{D}_{d+k,d}, \mathbf{W}_i \leftarrow_{\$} \mathbb{Z}_q^{d\times k}, \mathbf{X}_i := \mathbf{A}_i\mathbf{W}_i$ and $\mathbf{X}'_i \leftarrow_{\$} \mathbb{Z}_q^{(d+k)\times k}$ for all $i \in \{1, \cdots, n\}$. Then, for any PPT adversary $\mathcal{A}$ and uniform matrix distribution $\mathcal{U}_{d+k,d}$, there exists a PPT adversary $\mathcal{B}$ such that*

$$\mathbf{Adv}^{(n,k)\text{-mddh}}_{\mathcal{U}_{d+k,d},\mathsf{GGen},\mathcal{A}}(\lambda) \leq \mathbf{Adv}^{\mathrm{mddh}}_{\mathcal{U}_{d+k,d},\mathsf{GGen},\mathcal{B}}(\lambda) + \frac{k+1}{q-1}.$$

We put the proof of Lemma 5 in the full version [17].

Acknowledgment. We appreciate the anonymous reviewers for their valuable comments. This work was supported by National Natural Science Foundation of China (Grant Nos. 61922036, U2001205, 62002223, 61825203), Major Program of Guangdong Basic and Applied Research Project (Grant No. 2019B030302008), National Joint Engineering Research Center of Network Security Detection and Protection Technology, Guangdong Key Laboratory of Data Security and Privacy Preserving, Guangdong Provincial Science and Technology Project (Grant No. 2021A0505030033), Shanghai Sailing Program (20YF1421100), Young Elite Scientists Sponsorship Program by China Association for Science and Technology (YESS20200185), and the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (Grant agreement 802823).

References

1. Michel Abdalla, Mihir Bellare, and Gregory Neven. Robust encryption. In *TCC 2010*, pages 480–497. Springer, 2010.
2. Mihir Bellare, Alexandra Boldyreva, Anand Desai, and David Pointcheval. Key-privacy in public-key encryption. In *ASIACRYPT 2001*, pages 566–582. Springer, 2001.
3. Mihir Bellare, Rafael Dowsley, Brent Waters, and Scott Yilek. Standard security does not imply security against selective-opening. In *EUROCRYPT 2012*, pages 645–662. Springer, 2012.
4. Mihir Bellare and Igors Stepanovs. Security under message-derived keys: Signcryption in imessage. In *EUROCRYPT 2020*, pages 507–537, Cham, 2020. Springer.
5. Fabrice Benhamouda, Craig Gentry, Sergey Gorbunov, Shai Halevi, Hugo Krawczyk, Chengyu Lin, Tal Rabin, and Leonid Reyzin. Can a public blockchain keep a secret? In *TCC 2020*, pages 260–290. Springer, 2020.

6. Florian Böhl, Dennis Hofheinz, and Daniel Kraschewski. On definitions of selective opening security. In *PKC 2012*, pages 522–539. Springer, 2012.
7. Ran Canetti, Uri Feige, Oded Goldreich, and Moni Naor. Adaptively secure multi-party computation. In *STOC 1996*, pages 639–648, 1996.
8. Ran Canetti, Shai Halevi, and Jonathan Katz. Adaptively-secure, non-interactive public-key encryption. In *TCC 2005*, pages 150–168. Springer, 2005.
9. Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In *EUROCRYPT 2002*, pages 45–64, 2002.
10. Alex Escala, Gottfried Herold, Eike Kiltz, Carla Ràfols, and Jorge Villar. An algebraic framework for Diffie-Hellman assumptions. In *CRYPTO 2013*, pages 129–147. Springer, 2013.
11. Shuai Han, Shengli Liu, Lin Lyu, and Dawu Gu. Tight leakage-resilient CCA-security from quasi-adaptive hash proof system. In *CRYPTO 2019*, pages 417–447. Springer, 2019.
12. Keisuke Hara, Fuyuki Kitagawa, Takahiro Matsuda, Goichiro Hanaoka, and Keisuke Tanaka. Simulation-based receiver selective opening CCA secure PKE from standard computational assumptions. In *SCN 2018*, pages 140–159. Springer, 2018.
13. Ryotaro Hayashi and Keisuke Tanaka. The sampling twice technique for the RSA-based cryptosystems with anonymity. In *PKC 2005*, pages 216–233. Springer, 2005.
14. Carmit Hazay, Arpita Patra, and Bogdan Warinschi. Selective opening security for receivers. In *ASIACRYPT 2015*, pages 443–469. Springer, 2015.
15. Dennis Hofheinz, Tibor Jager, and Andy Rupp. Public-key encryption with simulation-based selective-opening security and compact ciphertexts. In *TCC 2016*, pages 146–168. Springer, 2016.
16. 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.
17. Zhengan Huang, Junzuo Lai, Shuai Han, Lin Lyu, and Jian Weng. Anonymous public key encryption under corruptions. Cryptology ePrint Archive, Paper 2022/1176.
18. Dingding Jia, Xianhui Lu, and Bao Li. Receiver selective opening security from indistinguishability obfuscation. In *INDOCRYPT 2016*, pages 393–410. Springer, 2016.
19. Dingding Jia, Xianhui Lu, and Bao Li. Constructions secure against receiver selective opening and chosen ciphertext attacks. In *CT-RSA 2017*, pages 417–431. Springer, 2017.
20. Youngkyung Lee, Dong Hoon Lee, and Jong Hwan Park. Tightly CCA-secure encryption scheme in a multi-user setting with corruptions. *Designs, Codes and Cryptography*, 88(11):2433–2452, 2020.
21. Payman Mohassel. A closer look at anonymity and robustness in encryption schemes. In *ASIACRYPT 2010*, pages 501–518. Springer, 2010.
22. Baodong Qin, Shengli Liu, and Kefei Chen. Efficient chosen-ciphertext secure public-key encryption scheme with high leakage-resilience. *IET Information Security*, 9(1):32–42, 2015.
23. 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 2020*, pages 191–220. Springer, 2020.