Simulation-based Selective Opening CCA Security for PKE from Key Encapsulation Mechanisms

Shengli Liu[1] and Kenneth G. Paterson[2]

[1] Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200240, China
[2] Information Security Group, Royal Holloway, University of London
slliu@sjtu.edu.cn kenny.paterson@rhul.ac.uk

Abstract. We study simulation-based, selective opening security against chosen-ciphertext attacks (SIM-SO-CCA security) for public key encryption (PKE). In a selective opening, chosen-ciphertext attack (SO-CCA), an adversary has access to a decryption oracle, sees a vector of ciphertexts, adaptively chooses to open some of them, and obtains the corresponding plaintexts and random coins used in the creation of the ciphertexts. The SIM-SO-CCA notion captures the security of unopened ciphertexts with respect to probabilistic polynomial-time (ppt) SO-CCA adversaries in a semantic way: what a ppt SO-CCA adversary can compute can also be simulated by a ppt simulator with access only to the opened messages. Building on techniques used to achieve weak deniable encryption and non-committing encryption, Fehr *et al.* (Eurocrypt 2010) presented an approach to constructing SIM-SO-CCA secure PKE from extended hash proof systems (EHPSs), collision-resistant hash functions and an information-theoretic primitive called Cross Authentication Codes (XACs). We generalize their approach by introducing a special type of Key Encapsulation Mechanism (KEM) and using it to build SIM-SO-CCA secure PKE. We investigate what properties are needed from the KEM to achieve SIM-SO-CCA security. We also give three instantiations of our construction. The first uses hash proof systems, the second relies on the n-Linear assumption, and the third uses indistinguishability obfuscation ($i\mathcal{O}$) in combination with extracting, puncturable Pseudo-Random Functions in a similar way to Sahai and Waters (STOC 2014). Our results establish the existence of SIM-SO-CCA secure PKE assuming only the existence of one-way functions and $i\mathcal{O}$. This result further highlights the simplicity and power of $i\mathcal{O}$ in constructing different cryptographic primitives.

1 Introduction

Selective Opening Attacks (SOAs) concern a multi-user scenario, where an adversary adaptively corrupts a set of users to get their secret state information. In the case of public key encryption (PKE), we assume that several senders send ciphertexts encrypting possibly correlated messages to a receiver. The SOA adversary is able to (adaptively) corrupt some senders, exposing their messages and also the random coins used to generate their ciphertexts. Security against selective opening attacks (SOA security) considers whether the uncorrupted ciphertexts remain secure.

There are two ways of formalizing SOA security: indistinguishability-based (IND-SO) and simulation-based (SIM-SO). According to whether the adversary is able to access to a decryption oracle during its attack, SOA security is further classified into IND-SO-CPA, IND-SO-CCA, SIM-SO-CPA and SIM-SO-CCA. In the formalization of SOAs, we allow a probabilistic polynomial-time (ppt) adversary to get the public key, a vector of challenge ciphertexts, and to adaptively corrupt (open) some ciphertexts to obtain opened plaintexts and random coins (and also access to a decryption oracle in the case of SO-CCA). The IND-SO security notions require that the real messages (used to generate the challenge ciphertexts) and re-sampled messages conditioned on the opened messages are computationally indistinguishable to an SOA adversary. Here we have to assume that the joint message distributions are *efficiently conditionally re-samplable* after the opened messages are exposed. On the other hand, the SIM-SO security notions have no such limitations. They require that what a probabilistic polynomial-time (ppt) SOA adversary can compute from the information it has learned can be simulated by a ppt simulator only knowing the opened plaintexts. SIM-SO security seems to be stronger than IND-SO security and significantly harder to achieve. We note the existence of a stronger IND-SO security notion, namely full IND-SO security, which imposes no limitation on the joint message distributions. However, there is no PKE achieving full IND-SO-CPA security yet. The relations among SIM-SO security, IND-SO security, and traditional IND-CPA/CCA security were explored in [5, 17].

Lossy encryption [3] has shown itself to be a very useful tool in achieving IND-SO-CPA security. Different approaches to achieving IND-SO-CCA security include the use of lossy trapdoor functions [23], All-But-N [14], and All-But-Many lossy trapdoor functions [15]. The basic idea is to make sure that only challenge ciphertexts are lossy encryptions, while ciphertexts queried by the adversary are normal encryptions. If there exists an efficient opener which can open a lossy encryption to an encryption of an arbitrary message, then an IND-SO-CCA secure PKE can also been shown to be SIM-SO-CCA secure. However, it seems that, to date, only a single, DCR-based PKE scheme [15] is known to have this property.

In [12], Fehr *et al.* proposed a black-box PKE construction to achieve SIM-SO-CCA security based on an Extended Hash Proof System (EHPS) associated with a subset membership problem, a collision-resistant hash function and a new information-theoretic primitive called Cross-Authentication Code (XAC). As pointed in [18, 19], a stronger property of XACs is needed to make the security proof rigorous.

1.1 Our Contributions

We generalize the black-box PKE construction of Fehr *et al.* [12] by using a special kind of key encapsulation mechanism (KEM) in combination with a strengthened XAC. Essentially, the KEM replaces the EHPS component in [12], opening up a new set of construction possibilities. In more detail:

- We characterise the properties needed of a KEM for our PKE construction to be SIM-SO-CCA secure. At a high level, these properties are that the KEM should have efficiently samplable and explainable (ESE) ciphertext and key spaces; *tailored* decapsulation; and *tailored*, constrained chosen-ciphertext (tCCCA) security. Here tailored decapsulation roughly means that the valid ciphertexts output by the KEM are sparse in the ciphertext space, while tCCCA security is an extension of the CCCA security notion of [16]. If a KEM has all three properties, then we say that it is a *tailored KEM.*
- We show three constructions for tailored KEMs, including one based on hash proof systems (HPS) [8], a specific KEM from the n-Linear assumption [16] (but different from the HPS-based one) and one constructed from indistinguishability Obfuscation ($i\mathcal{O}$) in combination with an extracting puncturable Pseudo-Random Function (PRF) [24]. Consequently, we obtain PKEs of three different types, all enjoying SIM-SO-CCA security. Thus, by adopting the KEM viewpoint, we significantly enlarge the scope of Fehr *et al.*'s construction.
- Since our PKE construction does not rely on collision-resistant hash functions, we immediately obtain the following results:
  - PKE with SIM-SO-CCA security from HPS and strengthened XACs (as compared to the PKE construction of [12] using EPHS, a strong XAC, and a collision-resistant hash function).
  - PKE with SIM-SO-CCA security from the n-Linear assumption in a way that differs from our HPS-based construction.
  - PKE with SIM-SO-CCA security assuming only the existence of $i\mathcal{O}$ and one-way functions.

1.2 Ingredients of Our Main Construction

We follow the outline provided by the black-box PKE construction of Fehr *et al.* [12]. Observing that the EHPS used in [12] can actually be viewed as a KEM, our construction can be considered as a generalization of their result. We first outline the properties of KEMs and XACs needed for our result, before describing the construction and its security analysis at a high level.

The KEM component in our construction needs to be "tailored" with the following properties:

(1) Efficiently samplable and explainable (ESE) domains. The key space $\mathcal{K}$ and ciphertext space $\mathcal{C}$ of the KEM should both be ESE domains. (Meaning that, given a randomised sampling algorithm $\mathsf{SampleD}$ for $\mathcal{D}$, there exists an efficient algorithm, $\mathsf{SampleD}^{-1}(\mathcal{D},\cdot)$, with the property that, given element d from a domain $\mathcal{D}$ as input, $\mathsf{SampleD}^{-1}(\mathcal{D}, \cdot)$ outputs value R such that d can be "explained" as having been sampled using R, i.e., $d = \mathsf{SampleD}(\mathcal{D}; R)$.)

(2) Tailored decapsulation. The valid ciphertexts output by the encapsulation algorithm constitute only a (small) subset of ciphertext space $\mathcal{C}$. When the input is a ciphertext randomly chosen from $\mathcal{C}$, the decapsulation will either output $\perp$ with overwhelming probability or output a key that is almost uniformly distributed over $\mathcal{K}$.

(3) Tailored, constrained CCA (tCCCA) security. The output of the encapsulation algorithm is computationally indistinguishable from (K^R, ψ^R), a pair of key and ciphertext randomly chosen from $\mathcal{K} \times \mathcal{C}$, for any ppt adversary, even if the adversary has access to a constrained decryption oracle. The adversary is allowed to make queries of the form $(\psi, P(\cdot))$ to the constrained decryption oracle, where ψ is an element of $\mathcal{C}$ and $P(\cdot)$ is a ppt predicate, such that $P(\cdot) : \mathcal{K} \to \{0, 1\}$ evaluates to 1 only for a negligible fraction of keys. The constrained decryption oracle will provide the decapsulated K to the adversary if only if $P(K) = 1$.

We will also need a strengthened XAC definition. A strengthened ℓ-XAC is a collection of algorithms $\mathsf{XAC} = (\mathsf{XGen}, \mathsf{XAuth}, \mathsf{XVer})$ having the following properties:

Authentication and Verification. Algorithm XAuth computes a tag $T \leftarrow \mathsf{XAuth}(K_1, \ldots, K_\ell)$ from ℓ inputs (which will be random keys in our construction). Any K_i used in generating the tag T almost always satisfies $\mathsf{XVer}(K_i, T) = 1$.

Security against impersonation/substitution attacks. Security against impersonation attacks means that, given a tag T, a randomly chosen key K will almost always fail verification with this specific tag, i.e., $\mathsf{XVer}(K, T) = 0$. A substitution attack considers an (all-powerful) adversary who obtains a tag $T = \mathsf{XAuth}(K_1, \ldots, K_\ell)$ and tries to forge a tag $T' \neq T$ such that $\mathsf{XVer}(K_i, T') = 1$, where K_i is one of the keys used in computing T. Security against substitution attacks requires that, if K_i is randomly chosen, then any adversary succeeds in outputting T' with $T' \neq T$ and $\mathsf{XVer}(K_i, T') = 1$ with negligible probability, even if it is given T and all keys except K_i as input.

Strongness and semi-uniqueness. Strongness says that when K_i is randomly chosen, then K_i, given $(K_j)_{j \in [\ell], j \neq i}$ and the tag $T = \mathsf{XAuth}(K_1, \ldots, K_\ell)$, is re-samplable with the correct probability distribution. That is to say, there exists a ppt algorithm $\mathsf{ReSample}((K_j)_{j \in [\ell], j \neq i}, T)$ such that $\mathsf{ReSample}$ outputs a key $\hat{K}_i$ that is statistically indistinguishable from K_i, even given $(K_j)_{j \in [\ell], j \neq i}$ and $T = \mathsf{XAuth}(K_1, \ldots, K_\ell)$. Semi-uniqueness says that it is possible to parse a key K as $(K_x, K_y) \in \mathcal{K}_x \times \mathcal{K}_y$ for some sets $\mathcal{K}_x, \mathcal{K}_y$, and for every $K_x \in \mathcal{K}_x$ and a tag T, there is at most one $K_y \in \mathcal{K}_y$ such that (K_x, K_y) satisfies $\mathsf{XVer}((K_x, K_y), T) = 1$.

1.3 Overview of Our Main Construction

Given a tailored KEM KEM and a strengthened $(\ell+s)$-XAC XAC, our construction of a PKE scheme PKE is as follows. (See Figure 4 for full details.)

- The public key of PKE is the public key pk_{kem} of KEM, an injective function F with domain $\mathcal{C}^\ell$ and range $(\mathcal{K}_y)^s$, and a vector of values $(K_{x_1},\ldots,K_{x_s}) \in (\mathcal{K}_x)^s$. The secret key of PKE is sk_{kem}, the secret key of KEM.
- The encryption operates in a bitwise mode. Let the ℓ-bit message be $m_1||\ldots||m_\ell$.
  - When $m_i = 1$, we set $(K_i, \psi_i) \leftarrow \mathsf{KEM.Encap}(pk_{kem})$.
  - When $m_i = 0$, we choose (K_i, ψ_i) randomly from $\mathcal{K} \times \mathcal{C}$.
  - After encrypting ℓ bits, we compute $F(\psi_1,\ldots,\psi_\ell)$ to get $(K_{y_1},\ldots,K_{y_s})$, and construct s extra keys $K_{\ell+j} = (K_{x_j}, K_{y_j})$ for $j = 1,\ldots,s$. All $\ell+s$ keys are then used to compute a tag $T = \mathsf{XAuth}(K_1,\ldots,K_{\ell+s})$.
  - Finally, the PKE ciphertext is $C = (\psi_1,\ldots,\psi_\ell,T)$.
- The decryption also operates in a bitwise fashion. Omitting some crucial details, we first recompute $(K_{y_1},\ldots,K_{y_s})$ using F and $(\psi_1,\ldots,\psi_\ell)$, reconstruct $K_{\ell+j}$ for $j = 1,\ldots,s$, and then verify the correctness of T using each $K_{\ell+j}$ in turn. Assuming this step passes, for each i, we compute $K_i \leftarrow \mathsf{KEM.Decap}(sk_{kem},\psi_i)$, and set the recovered message bit as the output of $\mathsf{XVer}(K_i,T)$. (When $K_i = \perp$, we set $\mathsf{XVer}(K_i,T) = 0$).

Now, in the above decryption procedure, a KEM decapsulation error occurs whenever $m_i = 0$. However, ψ_i is random in this case, and the tailored decapsulation makes sure that the output of $\mathsf{KEM.Decap}(sk_{kem},\psi_i)$ is either $\perp$ or a random key K; in either case, $\mathsf{XVer}(K_i,T)$ is 0 except with negligible probability because of the security of XAC against impersonation attacks.

1.4 SIM-SO-CCA Security of Our Main Construction

We follow the techniques of non-committing and deniable encryption [7, 6, 10, 20] and try to create equivocable ciphertexts that not only can be opened arbitrarily but that are also computationally indistinguishable from real ciphertexts. In our construction, the equivocable ciphertexts are in fact encryptions of ones. Note that tCCCA security of KEM ensures that $(K,\psi) \approx_c (K^R,\psi^R)$, where (K,ψ) is the output of $\mathsf{KEM.Encap}(pk_{kem})$ and (K^R,ψ^R) is randomly chosen from $\mathcal{K}\times\mathcal{C}$. On the other hand, both $\mathcal{K}$ and $\mathcal{C}$ are ESE. Therefore, (K,ψ) encrypting 1 can always be explained as a random pair (K^R,ψ^R) encrypting 0 by exposing the randomness output from $\mathsf{SampleK}^{-1}(\mathcal{K},K)$ and $\mathsf{SampleC}^{-1}(\mathcal{C},\psi)$.

However, this is not sufficient in the SO-CCA setting since the adversary is able to query its decryption oracle and perform corruptions, and it might then be easy for the adversary to distinguish an encryption of ones and an encryption of a real message. For example, consider an adversary that is given a ciphertext $C = (\psi_1,\psi_2,\ldots,\psi_\ell,T)$, where C is either an encryption of ones but opened as zeros with re-explained randomness, or an encryption of zeros being opened honestly. In fact, opened randomness exposes all K_i's to the adversary. Then the adversary can generate a different ciphertext $C' = (\psi_1,\psi_2,\ldots,\psi_\ell,T')$ as follows.

A new tag T' ($T' \neq T$) is computed as $T' := \mathsf{XAuth}(K'_1, K_2, \ldots, K_{\ell+s})$, where K'_1 is randomly chosen and all other K_i's ($2 \leq i \leq \ell + s$) are the same as in T. The decryption of C' will be $(0, 1, \ldots, 1)$ if C is an encryption of ones but $(0, 0, \ldots, 0)$ if C is an encryption of zeros! The problem is that the opened randomness discloses K_i and that gives too much information to the adversary, especially when (K_i, ψ_i) encodes 0. To solve this problem, we have to use a different method to open K_i so that the adversary obtains no extra information about K_i when (K_i, ψ_i) encodes 0: first, we use algorithm $\mathsf{ReSample}$ of XAC to resample K_i to obtain a statistically indistinguishable $\hat{K}_i$; then we call $\mathsf{SampleK}^{-1}(\mathcal{K}, \hat{K}_i)$ and $\mathsf{SampleC}^{-1}(\mathcal{C}, \psi_i)$ to open $(\hat{K}_i, \psi_i)$ to an encryption of 0. Now an encryption of ones, say $C = (\psi_1, \psi_2, \ldots, \psi_\ell, T)$, is able to play the role of an equivocable ciphertext, due to the tCCCA security of KEM and the security of XAC.

Consequently, we can build a simulator $\mathcal{S}$ with respect to an adversary $\mathcal{A}$ to prove SIM-SO-CCA security: $\mathcal{S}$ simulates the real environment for $\mathcal{A}$ by generating public and private keys, and uses the private key to answer $\mathcal{A}$'s decryption queries; $\mathcal{S}$ creates n challenge ciphertexts all of which are encryptions of ones; when $\mathcal{A}$ makes a corruption query concerning a challenge ciphertext C, $\mathcal{S}$ can open C bit-by-bit according to the real message. If the bit m_i is 1, it opens (K_i, ψ_i) honestly, otherwise it opens (K_i, ψ_i) to 0 by using $\mathsf{ReSample}$, $\mathsf{SampleC}^{-1}$ and $\mathsf{SampleK}^{-1}$.

1.5 Related Work

The SOA security notion was first formally proposed by Dwork *et al.* [11]. SIM-SO-CPA and IND-SO-CPA notions were given by Bellare *et al.* [3]. The relations among SOA security notions and traditional IND-CPA security were investigated in [5, 17]. Bellare *et al.* [4] proposed the first SIM-SO-CPA secure Identity-Based Encryption (IBE), while also adopting the non-committing technique and weak deniable encryption. Lai *et al.* [21] proposed the first construction for SIM-SO-CCA secure IBE from a so-called extractable IBE, a collision-resistant hash function, and a strengthened XAC. Recently, Sahai and Waters [24] introduced the puncturable programming technique and employed puncturable PRFs and Indistinguishability Obfuscation ($i\mathcal{O}$) to obtain a variety of cryptographic primitives including deniable encryption with IND-CPA security, PKE with IND-CPA and IND-CCA security, KEM with IND-CCA security, injective trapdoor functions, etc. It should be noted that any IND-CPA secure deniable encryption with ESE ciphertext space implies a PKE with SIM-SO-CPA security. Therefore, the deniable encryption scheme in [24] that is based on a puncturable PRF and $i\mathcal{O}$ implicitly already gives us a SIM-SO-*CPA* secure PKE. Our result establishes that SIM-SO-*CCA* security is achievable from puncturable PRFs and $i\mathcal{O}$ as well, albeit via the combination of an IND-CCA secure KEM and a strengthened XAC.

2 Preliminaries

We use $s_1, \ldots, s_t \leftarrow S$ to denote picking elements $s_1, \ldots, s_t$ uniformly from set S. Let $|S|$ denote the size of set S. Let $[n]$ denote the set $\{1, \ldots, n\}$. Let $s_1 \| s_2 \| \ldots$

denotes the concatenation of strings. For a probabilistic polynomial-time (ppt) algorithm A, we denote $y \leftarrow A(x; R)$ the process of running A on input x with randomness R, and assigning y as the result. Let $\mathcal{R}_A$ denote the randomness space of A, and $y \leftarrow A(x)$ denote $y \leftarrow A(x; R)$ with R chosen from $\mathcal{R}_A$ uniformly at random. Let U_n denote the uniform distribution over $\{0,1\}^n$. A function $f(\kappa)$ is *negligible*, denoted by $neg(\kappa)$, if for every $c > 0$ there exists a κ_c such that $f(\kappa) < 1/\kappa^c$ for all $\kappa > \kappa_c$. Let $\approx_c$ (resp. $\approx_s$) denote computational (resp. statistical) indistinguishability between two ensembles of random variables.

We use boldface letters for vectors. For a vector $\mathbf{m}$ of finite dimension, let $|\mathbf{m}|$ denote the length of the vector. For a set $I = \{i_1, i_2, \ldots, i_{|I|}\} \subseteq [|\mathbf{m}|]$, we define $\mathbf{m}[I] := (\mathbf{m}[i_1], \mathbf{m}[i_2], \ldots, \mathbf{m}[i_{|I|}])$.

We refer to the full version of this paper [22] for the definition and an example of *Strengthened Cross Authentication Codes.*

2.1 Public Key Encryption

A public key encryption (PKE) scheme is made up of three ppt algorithms:

$\mathsf{KeyGen}(1^\kappa)$ takes as input the security parameter κ, and outputs a public key and a secret key (pk, sk).

$\mathsf{Enc}(pk, M)$ takes as input the public key pk and a message M and outputs a ciphertext C.

$\mathsf{Dec}(sk, C)$ takes as input the secret key sk and a ciphertext C and outputs either a message M or a failure symbol $\perp$.

The correctness of a PKE scheme is relaxed to allow a negligible decryption error $\epsilon(\kappa)$. That is, $\mathsf{Dec}(sk, \mathsf{Enc}(pk, M)) = M$ holds with probability at least $1 - \epsilon(\kappa)$ for all $(pk, sk) \leftarrow \mathsf{KeyGen}(1^\kappa)$, where the probability is taken over the coins used in encryption.

Let $\mathbf{m}$ and $\mathbf{r}$ be two vectors of dimension $n := n(\kappa)$. Define $\mathsf{Enc}(pk, \mathbf{m}; \mathbf{r}) := (\mathsf{Enc}(pk, \mathbf{m}[1]; \mathbf{r}[1]), \ldots, \mathsf{Enc}(pk, \mathbf{m}[n]; \mathbf{r}[n]))$. Here $\mathbf{r}[i]$ is the fresh randomness used for the encryption of $\mathbf{m}[i]$ for $i \in [n]$.

2.2 Simulation-based, Selective Opening CCA Security of PKE

We review the simulation-based definition of security for PKE against selective opening, chosen-ciphertext adversaries from [12].Let $\mathcal{M}$ denote an n-message sampler, which on input string $\alpha \in \{0,1\}^*$ outputs an n-vector $\mathbf{m} = (\mathbf{m}[1], \ldots, \mathbf{m}[n])$ of messages. Let R be any ppt algorithm outputting a single bit.

Definition 1 (SIM-SO-CCA Security) *A PKE scheme* PKE=(KeyGen, Enc, Dec) *is simulation-based, selective opening, chosen-ciphertext secure (SIM-SO-CCA secure) if for every ppt n-message sampler $\mathcal{M}$, every ppt relation R, every restricted, stateful ppt adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$, there is a stateful ppt simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$ such that $\mathsf{Adv}^{\mathsf{so\text{-}cca}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},n,\mathcal{M},R}(\kappa)$ is negligible, where*

$$\mathsf{Adv}^{\mathsf{so\text{-}cca}}_{\mathsf{PKE},\mathcal{A},\mathcal{S},n,\mathcal{M},R}(\kappa) = \left| \mathsf{Pr}\left[\mathsf{Exp}^{\text{so-cca-real}}_{\mathsf{PKE},\mathcal{A},n,\mathcal{M},R}(\kappa) = 1\right] - \mathsf{Pr}\left[\mathsf{Exp}^{\text{so-cca-ideal}}_{\mathsf{PKE},\mathcal{S},n,\mathcal{M},R}(\kappa) = 1\right] \right|$$

and experiments $\mathsf{Exp}^{\text{so-cca-real}}_{\mathsf{PKE},A,n,\mathcal{M},R}(\kappa)$ *and* $\mathsf{Exp}^{\text{so-cca-ideal}}_{\mathsf{PKE},\mathcal{S},n,\mathcal{M},R}(\kappa)$ *are defined in Figure 1. Here the restriction on* $\mathcal{A}$ *is that* $\mathcal{A}_2, \mathcal{A}_3$ *are not allowed to query the decryption oracle* $\mathsf{Dec}(\cdot)$ *with any challenge ciphertext* $\mathbf{c}[i] \in \mathbf{c}$.

```
$\mathsf{Exp}^{\text{so-cca-real}}_{\mathsf{PKE},A,n,\mathcal{M},R}(\kappa)$:
    $(pk, sk) \leftarrow \mathsf{KeyGen}(1^\kappa)$
    $(\alpha, a_1) \leftarrow \mathcal{A}_1^{\mathsf{Dec}(\cdot)}(pk)$
    $\mathbf{m} \leftarrow \mathcal{M}(\alpha)$, $\mathbf{r} \leftarrow \mathsf{coins}$
    $\mathbf{c} \leftarrow \mathsf{Enc}(pk, \mathbf{m}; \mathbf{r})$
    $(I, a_2) \leftarrow \mathcal{A}_2^{\mathsf{Dec}_{\notin \mathbf{c}}(\cdot)}(a_1, \mathbf{c})$
    $out_{\mathcal{A}} \leftarrow \mathcal{A}_3^{\mathsf{Dec}_{\notin \mathbf{c}}(\cdot)}(a_2, \mathbf{m}[I], \mathbf{r}[I])$
    return $R(\mathbf{m}, I, out_{\mathcal{A}})$

$\mathsf{Exp}^{\text{so-cca-ideal}}_{\mathsf{PKE},\mathcal{S},n,\mathcal{M},R}(\kappa)$:
    $(\alpha, s_1) \leftarrow \mathcal{S}_1(1^\kappa)$
    $\mathbf{m} \leftarrow \mathcal{M}(\alpha)$
    $(I, s_2) \leftarrow \mathcal{S}_2(s_1, (1^{|\mathbf{m}[i]|})_{i \in [n]})$
    $out_{\mathcal{S}} \leftarrow \mathcal{S}_3(s_2, \mathbf{m}[I])$
    return $R(\mathbf{m}, I, out_{\mathcal{S}})$
```

Fig. 1. Experiments used in the definition of SIM-SO-CCA security of PKE.

2.3 Key Encapsulation Mechanisms

A Key Encapsulation Mechanism (KEM) KEM consists of three ppt algorithms $(\mathsf{KEM.Kg}, \mathsf{KEM.Enc}, \mathsf{KEM.Dec})$. Let $\mathcal{K}$ be the key space associated with KEM.

$\mathsf{KEM.Kg}(1^\kappa)$ takes as input a security parameter κ and outputs public/secret key pair (pk, sk).

$\mathsf{KEM.Encap}(pk)$ takes as input the public key pk and outputs a key K and a ciphertext (or encapsulation) ψ.

$\mathsf{KEM.Decap}(sk, \psi)$ takes as input the secret key sk and a ciphertext ψ, and outputs either a key K or a failure symbol $\perp$.

The correctness condition on a KEM KEM is that $\mathsf{KEM.Decap}(sk, \psi) = K$ holds for all $\kappa \in \mathbb{N}$, all $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^\kappa)$, and all $(K, \psi) \leftarrow \mathsf{KEM.Encap}(pk)$.

2.4 Efficiently Samplable and Explainable (ESE) Domain

A domain $\mathcal{D}$ is said to be *efficiently samplable and explainable* (ESE) [12] if associated with $\mathcal{D}$ are the following two ppt algorithms:

$\mathsf{Sample}(\mathcal{D}; R)$: On input (a description of) domain $\mathcal{D}$ and random coins $R \leftarrow \mathcal{R}_{\mathsf{Sample}}$, this algorithm outputs an element that is uniformly distributed over $\mathcal{D}$.

$\mathsf{Sample}^{-1}(\mathcal{D}, x)$: On input (a description of) domain $\mathcal{D}$ and *any* $x \in \mathcal{D}$, this algorithm outputs R that is uniformly distributed over the set $\{R \in \mathcal{R}_{\mathsf{Sample}} \mid \mathsf{Sample}(\mathcal{D}; R) = x\}$.

Clearly $\mathcal{D} = \{0,1\}^\kappa$ is ESE with $R = \mathsf{Sample}(\mathcal{D}; R) = \mathsf{Sample}^{-1}(\mathcal{D}, R)$. It was shown by Damgård and Nielsen in [10] that any dense subset of an efficiently samplable domain is ESE as long as the dense subset admits an efficient membership test. Hence, for example, $\mathbb{Z}^*_{N^s}$ for a RSA modulus N is ESE.

```
$\underline{\mathsf{Exp}^{\text{VCI-}b}_{\mathsf{KEM},\mathcal{A}}(\kappa):}$
    $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^\kappa)$
    $\psi_0^* \leftarrow \mathcal{C}$, $(K^*, \psi_1^*) \leftarrow \mathsf{KEM.Encap}(pk)$
    $b' \leftarrow \mathcal{A}^{\widetilde{\mathsf{Decap}}_{\neq\psi_b^*}(\cdot)}(pk, \psi_b^*)$
    Return$(b')$
```

```
$\widetilde{\mathsf{Decap}}_{\neq\psi^*}(P, \psi)$
    If $\psi = \psi^*$ return $(\perp)$
    $K \leftarrow \mathsf{KEM.Decap}(sk, \psi)$
    If $P(K) = 0$ return $(\perp)$;
    Else return $(K)$
```

Fig. 2. Experiment for defining Valid Ciphertext Indistinguishability of KEMs. Here $\widetilde{\mathsf{Decap}}_{\neq\psi^*}(P, \psi)$ denotes a constrained decryption oracle, taking as input predicate $P(\cdot)$ and encapsulation ψ.

3 KEM Tailored for Construction of PKE with SIM-SO-CCA Security

We describe the properties that are required of a KEM to build SIM-SO-CCA secure PKE; the construction itself is given in the next section.

3.1 Valid Ciphertext Indistinguishability (VCI) of KEMs

Suppose $\mathsf{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Encap}, \mathsf{KEM.Decap})$ is associated with an efficiently recognizable ciphertext space $\mathcal{C}$. For fixed κ, let $\Psi \subset C$ denote the set of possible key encapsulations output by $\mathsf{KEM.Encap}$, so $\Psi = \{\psi : \psi \leftarrow \mathsf{KEM.Encap}(pk; r), (pk, sk) \leftarrow \mathsf{KEM.Kg}(1^\kappa), r \leftarrow \mathsf{Coins}\}$. The set Ψ is called the *valid ciphertext set* (for κ).

Definition 2 (Valid Ciphertext Indistinguishability) *Let KEM be a KEM with valid ciphertext set Ψ and ciphertext space $\mathcal{C}$. Define the advantage of an adversary $\mathcal{A}$ in the experiment depicted in Figure 2 to be*

$$\mathsf{Adv}^{\text{VCI}}_{\mathsf{KEM},\mathcal{A}}(\kappa) := \left|\Pr\left[\mathsf{Exp}^{\text{VCI-0}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1\right] - \Pr\left[\mathsf{Exp}^{\text{VCI-1}}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1\right]\right|.$$

Then KEM is said to be Valid Ciphertext Indistinguishable (VCI) *if for all ppt adversaries $\mathcal{A}$, $\mathsf{Adv}^{\text{VCI}}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ is negligible.*

3.2 Tailored KEMs

To be of service in our construction of SIM-SO-CCA secure PKE, we need a KEM that is tailored to have the following three properties, as explained in the introduction: (1) the key space $\mathcal{K}$ and ciphertext space $\mathcal{C}$ of the KEM should both be ESE domains; (2) the valid ciphertexts output by the encapsulation algorithm constitute only a small subset of ciphertext space $\mathcal{C}$, and the decryption of a random ciphertext results in failure or a random key; (3) the KEM has tailored, constrained CCA security. We define the last of these three properties next.

```
$\mathsf{Exp}^{tccca-b}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ :
    $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^\kappa)$
    $K_0^* \leftarrow \mathcal{K}$, $\psi_0^* \leftarrow \mathcal{C}$
    $(K_1^*, \psi_1^*) \leftarrow \mathsf{KEM.Encap}(pk)$
    $b' \leftarrow \mathcal{A}^{\widetilde{\mathsf{Decap}}_{\neq\psi^*}(\cdot)}(pk, K_b^*, \psi_b^*)$
    Return$(b')$
```

```
$\widetilde{\mathsf{Decap}}_{\neq\psi^*}(P, \psi)$
    If $\psi = \psi^*$ return $(\perp)$
    $K \leftarrow \mathsf{KEM.Decap}(sk, \psi)$
    If $P(K) = 0$ return $(\perp)$;
    Else return $(K)$
```

Fig. 3. Experiment for defining IND-tCCCA security of KEMs. Here $\widetilde{\mathsf{Decap}}_{\neq\psi^*}(P, \psi)$ denotes a constrained decryption oracle, taking as input predicate $P(\cdot)$ and encapsulation ψ. Predicate $P(\cdot)$ may vary in different queries.

Definition 3 (IND-tCCCA Security for KEMs) *Let* KEM *be a KEM with ciphertext space* $\mathcal{C}$ *and valid ciphertext set* Ψ*, let* $\mathcal{A}$ *be a ppt adversary, and consider the experiment* $\mathsf{Exp}^{tccca-b}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ *defined in Figure 3. Define the advantage* $\mathsf{Adv}^{tccca}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ *of* $\mathcal{A}$ *by:*

$$\mathsf{Adv}^{tccca}_{\mathsf{KEM},\mathcal{A}}(\kappa) := \left|\Pr\left[\mathsf{Exp}^{tccca-0}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1\right] - \Pr\left[\mathsf{Exp}^{tccca-1}_{\mathsf{KEM},\mathcal{A}}(\kappa) = 1\right]\right|.$$

Then KEM *is said to be* secure against tailored, constrained chosen ciphertext attacks (IND-tCCCA secure) *if for all ppt adversaries* $\mathcal{A}$ *with negligible uncertainty* $uncert_{\mathcal{A}}(\kappa)$ *(in* κ*), the advantage* $\mathsf{Adv}^{tccca}_{\mathsf{KEM},\mathcal{A}}(\kappa)$ *is also negligible in* κ*. Here, the* uncertainty *of* $\mathcal{A}$ *is defined as* $uncert_{\mathcal{A}}(\kappa) := \frac{1}{q_d}\sum_{i=1}^{q_d} \Pr[P_i(K) = 1]$, *which measures the average fraction of keys for which the evaluation of predicate* $P_i(\cdot)$ *is equal to 1 in the tCCCA experiment, where* P_i *denotes the predicate used in the i-th query by* $\mathcal{A}$*, and* q_d *the number of decapsulation queries made by* $\mathcal{A}$*.*

Constrained CCA (CCCA) security for PKE was introduced in [16] as a strictly weaker notion than IND-CCA security. The main difference between IND-CCCA security and our newly defined IND-tCCCA security is that, in the IND-CCCA definition, the adversary is given a pair (K_b^*, ψ^*) where ψ^* is always a correct encapsulation of K_1^*, while in the IND-tCCCA definition, the adversary is given a pair (K_b^*, ψ_b^*) where, when $b = 0$, ψ_b^* is just a random element of $\mathcal{C}$ and, when $b = 1$, ψ_b^* is a correct encapsulation of K_b^*. However, IND-CCCA security and VCI together imply IND-tCCCA security for KEMs:

Lemma 1. *Suppose that* KEM *is a KEM having an efficiently recognizable ciphertext space* $\mathcal{C}$*. If* KEM *is both IND-CCCA secure and VCI then it is also IND-tCCCA secure.*

Proof. Recall that the VCI and CCCA experiments are almost the same except for the construction of the adversary's challenge. Let $(K^{(R)}, \psi^{(R)})$ be chosen from $\mathcal{C}\times\mathcal{K}$ uniformly at random. Let (K, ψ) be the output of $\mathsf{KEM.Encap}$ in the CCCA experiment. IND-CCCA security implies $(K, \psi) \approx_c (K^{(R)}, \psi)$. The VCI property implies that $\psi \approx_c \psi^{(R)}$, hence $(K^{(R)}, \psi) \approx_c (K^{(R)}, \psi^{(R)})$ when $K^{(R)}$ is chosen uniformly and independently of everything else. Finally, $(K, \psi) \approx_c (K^{(R)}, \psi^{(R)})$ follows from transitivity. □

Tailored Decapsulation. We also tailor the functionality of our KEMs' decapsulation algorithms to suit our PKE construction.

Definition 4 (Tailored Decapsulation) *Suppose* $\mathsf{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Encap}, \mathsf{KEM.Decap})$ *is a KEM. Then* KEM *is said to have* tailored decapsulation *if there exists a negligible function* $\eta(\kappa)$ *such that for all* (pk, sk) *output by* $\mathsf{KEM.Kg}(1^\kappa)$*, one or the other of the following two cases pertains:*

- $\mathsf{KEM.Decap}$ *rejects a random* $\psi' \in \mathcal{C}$*, except with negligible probability, i.e.,*

$$\Pr\left[\mathsf{KEM.Decap}(sk_{kem}, \psi') \neq \perp \mid \psi' \leftarrow \mathcal{C}\right] \leq \eta(\kappa).$$

- $\mathsf{KEM.Decap}$ *outputs* $\eta(\kappa)$*-uniform keys on input a random element from* $\mathcal{C}$*. That is, the statistical distance between the output and a uniform distribution on* $\mathcal{K}$ *is bounded by* $\eta(\kappa)$*:*

$$\frac{1}{2}\sum_{k\in\mathcal{K}}\left|\Pr\left[\mathsf{KEM.Decap}(sk_{kem}, \psi') = k \mid \psi' \leftarrow \mathcal{C}\right] - \frac{1}{|\mathcal{K}|}\right| \leq \eta(\kappa).$$

Remark. The former case implies that valid ciphertexts are sparse in the whole ciphertext space, i.e., $|\mathcal{V}|/|\mathcal{C}|$ is negligible. In the latter case, VCI (when VCI holds for all $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^\kappa)$) alone might imply IND-tCCCA security of KEM, since the decapsulated key is uniquely determined by the secret key and the ciphertext (be it valid or invalid).

4 Construction of PKE with SIM-SO-CCA Security from Tailored KEMs

Let $\mathsf{KEM} = (\mathsf{KEM.Kg}, \mathsf{KEM.Encap}, \mathsf{KEM.Decap})$ be a KEM with valid ciphertext set Ψ, efficiently recognizable ciphertext space $\mathcal{C}$, and key space $\mathcal{K} = \mathcal{K}_x \times \mathcal{K}_y$. We further assume that:

(1) $\mathsf{KEM.Decap}$ has tailored functionality as per Definition 4 (this will be used for the correctness of our PKE construction);

(2) KEM is IND-tCCCA secure (this will be used in the SIM-SO-CCA security proof of the PKE construction).

(3) Both the key space $\mathcal{K}$ and the ciphertext space $\mathcal{C}$ of KEM are efficiently samplable and explainable domains, with algorithms $(\mathsf{SampleK}, \mathsf{SampleK}^{-1})$ and $(\mathsf{SampleC}, \mathsf{SampleC}^{-1})$ (these algorithms are also used in the security analysis).

We refer to a KEM possessing all three properties above as being a *tailored* KEM.

Let $F : \mathcal{C}^\ell \rightarrow (\mathcal{K}_y)^s$ be an injective function (such functions are easily constructed using, for example, encodings from $\mathcal{C}$ to bit-strings and from bit-strings to $\mathcal{K}_y$, provided s is sufficiently large). Let $\mathsf{XAC} = (\mathsf{XGen}, \mathsf{XAuth}, \mathsf{XVer})$ be a $\delta(\kappa)$-strong and semi-unique $(\ell+s)$-XAC with tag space $\mathcal{XT}$ and key space $\mathcal{XK}$;

```
$\mathsf{KeyGen}(1^\kappa)$ :
  $(pk_{kem}, sk_{kem}) \leftarrow \mathsf{KEM.Kg}(1^\kappa)$
  $K_{x_1}, \ldots, K_{x_s} \leftarrow \mathcal{K}_x$
  $pk = (pk_{kem}, (K_{x_j})_{j\in[s]}, F)$
  $sk = (sk_{kem}, pk)$.
  Return$(pk, sk)$

$\mathsf{Enc}(pk, m_1||\ldots||m_\ell)$ :
  Parse $pk$ as $(pk_{kem}, (K_{x_j})_{j\in[s]}, F)$
  For $i = 1$ to $\ell$
    If $m_i = 1$
      $(K_i, \psi_i) \leftarrow \mathsf{KEM.Encap}(pk_{kem})$
    Else $\psi_i \leftarrow \mathcal{C}; K_i \leftarrow \mathcal{K}$
  $(K_{y_1}, \ldots, K_{y_s}) \leftarrow F(\psi_1, \ldots, \psi_\ell)$
  For $j = 1$ to $s$
    $K_{\ell+j} \leftarrow (K_{x_j}, K_{y_j})$
  $T \leftarrow \mathsf{XAuth}(K_1, \ldots, K_{\ell+s})$
  Return $(\psi_1, \ldots, \psi_\ell, T)$
```

```
$\mathsf{Dec}(sk, C)$ :
  Parse $C$ as $(\psi_1, \ldots, \psi_\ell, T)$
  For $i = 1$ to $\ell$
    $m'_i \leftarrow 0$
  $(K'_{y_1}, \ldots, K'_{y_s}) \leftarrow F(\psi_1, \ldots, \psi_\ell)$
  For $j = 1$ to $s$
    $K'_{\ell+j} \leftarrow (K_{x_j}, K'_{y_j})$
  If $\bigwedge_{j=1}^{s} \mathsf{XVer}(K'_{\ell+j}, T) = 1$
    For $i = 1$ to $\ell$
      $K'_i \leftarrow \mathsf{KEM.Decap}(sk_{kem}, \psi_i)$
      If $K'_i = \perp$, then $m'_i \leftarrow 0$
      Else $m'_i \leftarrow \mathsf{XVer}(K'_i, T)$
  Return$(m'_1||m'_2||\ldots, m'_\ell)$
```

Fig. 4. Construction of PKE scheme PKE from tailored KEM and $(\ell + s)$-XAC.

suppose also that $\mathcal{XK} = \mathcal{K} = \mathcal{K}_x \times \mathcal{K}_y$. Our main construction of PKE scheme $\mathsf{PKE} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ with message space $\{0, 1\}^\ell$ is shown in Figure 4.

Note that in the decryption, if $\mathsf{XVer}(K'_{\ell+j}, T) = 1$ for all $j \in [s]$, then the recovered bit m'_i equals 0 if and only if the decapsulated key K'_i equals $\perp$ or $\mathsf{XVer}(K'_i, T) = 0$.

Correctness. Encryption and decryption are performed in bitwise fashion. Suppose $m_i = 1$. Then (K_i, ψ_i) are the encapsulated key and corresponding valid encapsulation; by the correctness of KEM and XAC, the decryption algorithm outputs $m'_i = 1$, except with negligible probability $\mathsf{fail}_{\mathsf{XAC}}$. Suppose $m_i = 0$. Then K_i and ψ_i are chosen independently and uniformly at random from $\mathcal{K}$ and $\mathcal{C}$, respectively. It follows that the tag T is independent of ψ_i. Now, during the decryption of the i-th bit, according to the tailored property of $\mathsf{KEM.Decap}$, K'_i is either $\perp$ (and thus $m'_i = 0$) with probability at least $1-\eta(\kappa)$, or K'_i is $\eta(\kappa)$-close to being uniformly distributed on $\mathcal{K}$. In the latter case, it holds that $m'_i = 0$ except with probability $\eta(\kappa) + \mathsf{Adv}^{\mathsf{imp}}_{\mathsf{XAC}}(\kappa)$ due to the $\eta(\kappa)$-uniformity of the key and the security of XAC against impersonation attack. Consequently, decryption correctly undoes encryption except with probability at most $\ell \cdot \max\{\mathsf{fail}_{\mathsf{XAC}}(\kappa), \mathsf{Adv}^{\mathsf{imp}}_{\mathsf{XAC}}(\kappa) + \eta(\kappa)\}$, which is negligible.

Lemma 2. *PKE scheme PKE in Figure 4 has the property that, if two distinct ciphertexts $C, \hat{C}$ both pass the verification step $\bigwedge_{j=1}^{s} \mathsf{XVer}(K_{\ell+j}, T) = 1$ during decryption, then they must have different tags $T \neq \hat{T}$.*

Proof. The proof is by contradiction and relies on the injectivity of F. Let $C = (\psi_1, \ldots, \psi_\ell, T)$ and $\hat{C} = (\hat{\psi}_1, \ldots, \hat{\psi}_\ell, \hat{T})$ be two different ciphertexts. Let

```
KeyGen'($1^\kappa$) :
    $(pk_{kem}, sk_{kem})$ ←KEM.Kg($1^\kappa$)
    $K_x \leftarrow \mathcal{K}_x$, $H \leftarrow$ HGen($1^\kappa$).
    $pk = (pk_{kem}, K_x, H)$
    $sk = (sk_{kem}, pk)$
    Return$(pk, sk)$
Enc'($pk, m_1|| \dots ||m_\ell$) :
    For $i = 1$ to $\ell$
      If $m_i = 1$
        $(K_i, \psi_i) \leftarrow$ KEM.Encap($pk_{kem}$)
      Else $\psi_i \leftarrow \mathcal{C}; K_i \leftarrow \mathcal{K}$
    $K_y \leftarrow H(\psi_1, \dots, \psi_\ell)$
    $K_{\ell+1} \leftarrow (K_x, K_y)$
    $T =$ XAuth($K_1, \dots, K_{\ell+1}$)
    Return $(\psi_1, \dots, \psi_\ell, T)$
```

```
Dec'($sk, C$) :
    $C = (\psi_1, \dots, \psi_\ell, T)$
    For $i = 1$ to $\ell$   $m'_i \leftarrow 0$
    $K'_y \leftarrow H(\psi_1, \dots, \psi_\ell)$
    $K'_{\ell+1} \leftarrow (K_x, K'_y)$
    If XVer($K'_{\ell+1}, T$) $= 1$
      For $i = 1$ to $\ell$
        $K'_i \leftarrow$ KEM.Decap($sk_{kem}, \psi_i$)
        If $K'_i = \perp$, then $m'_i \leftarrow 0$
        Else $m'_i \leftarrow$ XVer($K'_i, T$)}
    Return$(m'_1||m'_2|| \dots, m'_\ell)$
```

Fig. 5. Construction of PKE scheme PKE' from tailored KEM, $(\ell + 1)$-XAC and CR hash function.

$(K_{y_1}, \dots, K_{y_s}) = F(\psi_1, \dots, \psi_\ell)$ and $(\hat{K}_{y_1}, \dots, \hat{K}_{y_s}) = F(\hat{\psi}_1, \dots, \hat{\psi}_\ell)$. Suppose $\bigwedge_{j=1}^{s} \mathsf{XVer}((K_{x_j}, K_{y_j}), T) = \bigwedge_{j=1}^{s} \mathsf{XVer}((\hat{K}_{x_j}, \hat{K}_{y_j}), \hat{T}) = 1$. If $T = \hat{T}$, then $C \neq \hat{C}$ implies $(\psi_1, \dots, \psi_\ell) \neq (\hat{\psi}_1, \dots, \hat{\psi}_\ell)$, which further implies $K_{y_j} \neq \hat{K}_{y_j}$ for some $j \in [s]$, by the injectivity of F. On the other hand, we know that $\mathsf{XVer}((K_{x_j}, K_{y_j}), T) = 1$ and $\mathsf{XVer}((K_{x_j}, \hat{K}_{y_j}), \hat{T} = T) = 1$; the semi-unique property of XAC now implies that $K_{y_j} = \hat{K}_{y_j}$, a contradiction. □

The SIM-SO-CCA security of PKE will rely on Lemma 2, which in turn relies on the injectivity of F. The size of F's domain is closely related to parameter s: generally the parameter s will be linear in ℓ. Since we need a $(\ell + s)$-XAC in the construction, the size of public key will be linear in ℓ. The size of tag T in the ciphertext will also grow linearly in s and therefore in ℓ. To further decrease the size of public key and tags in our PKE construction, we can employ a collision-resistant (CR) hash function $\mathsf{H} = (\mathsf{HGen}, \mathsf{HEval})$ mapping $\mathcal{C}^\ell$ to $\mathcal{K}_y$ instead of the injective function F (see the full paper [22] for definitions). Then an $(\ell+1)$-XAC is sufficient for the construction, and this results in more compact public keys and tags, but requires an additional cryptographic assumption. The construction using CR hash functions is given in Figure 5.

Theorem 1 *Suppose KEM is a tailored KEM, and the $(\ell+s)$-cross-authentication code XAC is $\delta(\kappa)$-strong, semi-unique, and secure against impersonation and substitution attacks. Then the PKE scheme PKE constructed in Figure 4 is SIM-SO-CCA secure. More precisely, for every ppt adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ against PKE in the SIM-SO-CCA real experiment that makes at most q_d decryption queries, for every ppt n-message sampler $\mathcal{M}$, and every ppt relation R, we can construct a stateful ppt simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$ for the ideal experiment, and* *a ppt adversary $\mathcal{B}$ against the IND-tCCCA security of* KEM*, such that:*

$$\mathit{Adv}^{\mathit{so\text{-}cca}}_{\mathit{PKE},\mathcal{A},\mathcal{S},n,\mathcal{M},R}(\kappa) \leq n\ell \cdot \mathit{Adv}^{\mathit{tccca}}_{\mathit{KEM},\mathcal{B}}(\kappa) + n\ell^2 q_d \cdot \left(\mathit{Adv}^{\mathit{sub}}_{\mathit{XAC}}(\kappa) + \mathit{Adv}^{\mathit{imp}}_{\mathit{XAC}}(\kappa) + \eta(\kappa)\right) + n\ell \cdot \delta(\kappa).$$

The proof of this theorem, our main result, can be found in the full paper [22]. Here we only give a high level overview. We construct a ppt simulator $\mathcal{S}$ as follows.

- $\mathcal{S}$ generates a public/private key pair and provides the public key to $\mathcal{A}$.
- $\mathcal{S}$ answers $\mathcal{A}$'s decryption queries using the private key.
- $\mathcal{S}$ prepares for $\mathcal{A}$ a vector of n challenge ciphertexts, each ciphertext encrypting ℓ ones.
- When $\mathcal{A}$ decides to corrupt a subset of the challenge ciphertexts, $\mathcal{S}$ obtains the messages corresponding to the corrupted ciphertexts and opens the corrupted ciphertexts bit-by-bit according to the messages. If bit m_i should be opened to 1, $\mathcal{S}$ reveals to $\mathcal{A}$ the original randomness used by $\mathsf{KEM.Encap}$ to generate (K_i, ψ_i). If bit m_i should be opened to 0, $\mathcal{S}$ first explains ψ_i with randomness output by $\mathsf{SampleC}^{-1}(\mathcal{C}, \psi_i)$ (as if ψ_i were randomly chosen). Then $\mathcal{S}$ uses algorithm $\mathsf{ReSample}$ of XAC to resample K_i to get $\hat{K}_i$, and explains $\hat{K}_i$ with randomness output by $\mathsf{SampleC}^{-1}(\mathcal{K}, \hat{K}_i)$ (as if $\hat{K}_i$ was randomly chosen).
- $\mathcal{S}$ finally outputs whatever $\mathcal{A}$ outputs.

The essence of the SIM-SO-CCA security proof is then to show that encryptions of 1's are computationally indistinguishable from encryptions of real messages, even if the adversary can see the opened (real) messages and the randomness of a corrupted subset of the challenge ciphertexts of his/her choice, and have access to the decryption oracle. This is done with a hybrid argument running from Game 0 to Game $n\ell$. In Game k the first k bits of messages are 1's and are opened as $\mathcal{S}$ does while the last $n\ell - k$ bits come from the real messages and are opened honestly. The proof shows that Games k and $k-1$ are indistinguishable using the tCCCA security of the tailored KEM and the security properties of the strengthened XAC.

If the k-th bit of the messages is 1, Games k and $k-1$ are identical. Otherwise, a tailored KEM adversary $\mathcal{B}$ can be constructed to simulate Game k or $k+1$ for adversary $\mathcal{A}$. $\mathcal{B}$ is provided with a public key pk_{kem}, a challenge (K^*, ψ^*) and a constrained decryption oracle, and is going to tell whether (K^*, ψ^*) is an output of $\mathsf{KEM.Encap}(pk_{kem})$ or a random pair. $\mathcal{B}$ can generate a public key for $\mathcal{A}$. When preparing the vector of challenge ciphertexts, $\mathcal{B}$ will encrypt the first $k-1$ bits from the real messages, use (K^*, ψ^*) as the encryption of the k-th bit, and encrypt $n\ell - k$ ones for the remaining bits. If (K^*, ψ^*) is an output of $\mathsf{KEM.Encap}(pk_{kem})$, the challenge vector of ciphertexts is just that in Game k, otherwise it is just that in Game $k-1$. Finally, to answer $\mathcal{A}$'s decryption query $C = (\psi_1, \ldots, \psi_\ell, T)$, $\mathcal{B}$ can query $(\psi_i, \mathsf{XVer}(\cdot, T))$ (note that $\mathsf{XVer}(\cdot, T)$ is a predicate) to his own constrained decryption oracle if $\psi^* \neq \psi_i$; $\mathcal{B}$ then replies to $\mathcal{A}$ with decrypted bit 0 iff $\mathcal{B}$ gets $\perp$ from its own oracle. The decryption is correct because $\mathcal{B}$'s oracle outputs $\perp$ iff the decapsulated key is $K_i = \perp$ or $\mathsf{XVer}(K_i, T) = 0$. If $\psi^* = \psi_i$, $\mathcal{B}$ is not allowed to query his own oracle, but can instead respond to $\mathcal{A}$ with the output of $\mathsf{XVer}(K^*, T)$ as the decrypted bit. This decryption is also correct with overwhelming probability for the following reasons: (1) If K^* is the encapsulated key of ψ^*, then $\mathsf{XVer}(K^*, T) = 1$ and decryption is correct. (2) If (K^*, ψ^*) is a random pair, then all the information leaked about K^* is just the very tag T^* that is computed by K^* during the generation of some challenge ciphertext. The semi-uniqueness of XAC guarantees that $T \neq T^*$, and the adversary's corruption only reveals information about a re-sampled $\hat{K}^*$. The security of XAC against substitution attacks shows that even if $\mathcal{A}$ knows T^* and all keys other than K^*, then $\mathcal{A}$ forges a different tag T such that $\mathsf{XVer}(K^*, T) = 1$ with negligible probability. Therefore, $\mathcal{B}$ will almost always respond to $\mathcal{A}$ with bit 0, which is the correct answer.

The security of our modified construction using CR hash functions is stated in the following theorem, whose proof is similar to that of Theorem 1.

Theorem 2 *Suppose KEM is a tailored KEM, the $(\ell+1)$-cross-authentication code XAC is $\delta(\kappa)$-strong, semi-unique, and secure against impersonation and substitution attacks, and H is collision-resistant. Then the PKE scheme PKE' constructed in Figure 5 is SIM-SO-CCA secure. More precisely, for every ppt adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3)$ against PKE' in the SIM-SO-CCA real experiment that makes at most q_d decryption queries, for every ppt n-message sampler $\mathcal{M}$, and every ppt relation R, we can construct a stateful ppt simulator $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2, \mathcal{S}_3)$ for the ideal experiment, a ppt adversary $\mathcal{B}$ against the IND-tCCCA security of KEM, and a ppt algorithm $\mathcal{F}$ against the collision-resistance of H such that:*

$$\mathsf{Adv}^{\textsf{so-cca}}_{\mathsf{PKE'},\mathcal{A},\mathcal{S},n,\mathcal{M},R}(\kappa) \leq n\ell \cdot \mathsf{Adv}^{tccca}_{\mathsf{KEM},\mathcal{B}}(\kappa) + n\ell^2 q_d \cdot \Big(\mathsf{Adv}^{\textsf{sub}}_{\mathsf{XAC}}(\kappa) + \mathsf{Adv}^{\textsf{imp}}_{\mathsf{XAC}}(\kappa) + \eta(\kappa)\Big)$$
$$+ n\ell \cdot \delta(\kappa) + \mathsf{Adv}^{\mathrm{cr}}_{H,\mathcal{F}}(\kappa).$$

5 Instantiations

In this section, we explore three different constructions of tailored KEMs, each suitable for the application of Theorems 1 and 2. The first is based on any Strongly Universal$_2$ hash proof system, the second is a direct construction relying on the n-Linear Assumption and a target collision-resistant hash function, while the third uses indistinguishability obfuscation.

5.1 Strongly Universal$_2$ Hash Proof Systems

We use hash proof systems [8] to build tailored KEMs suitable for application in our main theorem.

Let $\Psi \subset \mathcal{C}$ be a language. The hardness of the *subset membership problem* for Ψ with respect to $\mathcal{C}$ requires that a random element from Ψ is indistinguishable from a random element from $\mathcal{C}$. Let $\mathcal{K}$ be a set and $\Lambda_{sk} : \mathcal{C} \to \mathcal{K}$ be a hash function indexed with $sk \in \mathcal{SK}$. Then Λ_{sk} is said to be *projective* if there exists a map $\mu : \mathcal{SK} \to \mathcal{PK}$ such that $\mu(sk) \in \mathcal{PK}$ defines the action of Λ_{sk} on the subset Ψ; μ is then said to be a *projection* on subset Ψ.

A hash proof system (HPS) HPS consists of three algorithms ($\mathsf{HPS.param}$, $\mathsf{HPS.pub}$, $\mathsf{HPS.priv}$). The randomized algorithm $\mathsf{HPS.param}(1^\kappa)$ outputs $\mathsf{params} = (\mathbb{G}, \mathcal{C}, \Psi, \mathcal{PK}, \mathcal{SK}, \Lambda, \mu)$, where $\mathbb{G}$ is a group. The secret key sk is randomly chosen from $\mathcal{SK}$, and the public key is computed as $pk = \mu(sk)$ where μ is a projection on Ψ. Algorithm $\mathsf{HPS.Pub}(pk, \psi, w)$ is given the public key pk, an element $\psi \in \Psi$ and its witness w, and outputs an encapsulated key $K = \mathsf{HPS.Pub}(pk, \psi, w)$ such that $K = \Lambda_{sk}(\psi)$. Algorithm $\mathsf{HPS.Priv}(sk, \psi)$ recovers $K = \Lambda_{sk}(\psi)$ using sk.

The *Strongly Universal*$_2$ *(SU*$_2$*)* property of an HPS characterizes the unpredictability of $\Lambda_{sk}(\psi)$ for $\psi \in \mathcal{C} \setminus \Psi$.

Definition 5 *Let $\mathsf{HPS} = (\mathsf{HPS.param}, \mathsf{HPS.pub}, \mathsf{HPS.priv})$ be a hash proof system. Then HPS is said to be SU$_2$ if*

$$\Pr\left[\Lambda_{sk}(\psi) = K \mid pk = \mu(sk), \psi', K' = \Lambda_{sk}(\psi')\right] = 1/|\mathcal{K}|,$$

for all $pk \in \mathcal{PK}$, all $\psi, \psi' \in \mathcal{C} \setminus \Psi$ with $\psi' \neq \psi$ and all $K, K' \in \mathcal{K}$, where the probability is taken over $sk \leftarrow \mathcal{SK}$.

Given that HPS is an SU$_2$ HPS, a KEM KEM can be constructed as shown in Figure 6. The output params of $\mathsf{HPS.param}$ is used as a set of public parameters implicitly used as input in the algorithms of KEM. Notice that the valid ciphertext set for KEM is Ψ.

$\underline{\mathsf{KEM.Kg}(1^\kappa)}$:	$\underline{\mathsf{KEM.Encap}(pk)}$:	$\underline{\mathsf{KEM.Decap}(sk, \psi)}$:
$sk \leftarrow \mathcal{SK}$	$\psi \leftarrow \Psi$ with witness w	
$pk = \mu(sk)$.	$K \leftarrow \mathsf{HPS.Pub}(pk, \psi, w)$	$K \leftarrow \mathsf{HPS.Priv}(sk, \psi)$
Return (pk, sk)	Return(K, ψ)	Return(K)

Fig. 6. Construction of a KEM from an SU$_2$ hash proof system.

Theorem 3 *Let HPS be an SU$_2$ HPS with $\mathsf{params} = (\mathbb{G}, \mathcal{C}, \Psi, \mathcal{PK}, \mathcal{SK}, \Lambda, \mu)$. Suppose the subset membership problem is hard for Ψ with respect to $\mathcal{C}$. Then the KEM KEM constructed from HPS as shown in Figure 6 is IND-tCCCA secure. Furthermore, if Ψ is sparse in $\mathcal{C}$, and both $\mathcal{C}$ and $\mathcal{K}$ are efficiently samplable and explainable, then KEM is a tailored KEM.*

Proof. It was already proved in [16] that the SU$_2$ property and the hardness of the subset membership problem for Ψ with respect to $\mathcal{C}$ implies the IND-CCCA security of KEM. On the other hand, public and secret key pairs can be generated independently from $\mathcal{C}$ and Ψ and the subset membership problem holds even if the secret key is known to the adversary. More precisely, when an adversary $\mathcal{B}$ is given ψ and tries to distinguish whether ψ is randomly chosen from Ψ or $\mathcal{C}$, it can establish a VCI experiment for a VCI adversary $\mathcal{A}$ as follows: first call $(pk, sk) \leftarrow \mathsf{KEM.Kg}(1^\kappa)$ and use sk to answer decryption queries. $\mathcal{B}$ gives pk to $\mathcal{A}$ and gives ψ as the challenge ciphertext. Finally $\mathcal{B}$ outputs whatever $\mathcal{A}$ returns. It is clear that $\mathcal{B}$ has the same advantage as $\mathcal{A}$. This implies that the VCI property holds for KEM under the hardness of the subset membership problem. Then IND-tCCCA security follows from Lemma 1.

The SU_2 property of HPS implies that

$$\Pr\left[\mathsf{KEM.Decap}(sk, \psi) = K\right] = \Pr\left[\mathsf{HPS.Priv}(sk, \psi) = K\right] = \frac{1}{|\mathcal{K}|}$$

for all invalid ciphertexts $\psi \in \mathcal{C} \setminus \Psi$, all $K \in \mathcal{K}$, and all $pk = \mu(sk)$, where the probability is taken over $sk \leftarrow \mathcal{SK}$. Then

$$\Pr\left[\mathsf{KEM.Decap}(sk, \psi) = K \mid \psi \leftarrow \mathcal{C}\right] = \Pr\left[\mathsf{KEM.Decap}(sk, \psi) = K \mid \psi \in \Psi\right] \cdot \frac{|\Psi|}{|\mathcal{C}|}$$

$$+ \Pr\left[\mathsf{KEM.Decap}(sk, \psi) = K \mid \psi \in \mathcal{C} \setminus \Psi\right] \cdot \left(1 - \frac{|\Psi|}{|\mathcal{C}|}\right)$$

$$= \Pr\left[\mathsf{KEM.Decap}(sk, \psi) = K \mid \psi \in \Psi\right] \cdot \frac{|\Psi|}{|\mathcal{C}|} + \frac{1}{|\mathcal{K}|} \cdot \left(1 - \frac{|\Psi|}{|\mathcal{C}|}\right) \leq \frac{|\Psi|}{|\mathcal{C}|} + \frac{1}{|\mathcal{K}|}.$$

Noting that $\Pr\left[\mathsf{KEM.Decap}(sk, \psi) = K \mid \psi \in \Psi\right]$ lies between 0 and 1, it follows that the statistical distance between $\mathsf{KEM.Decap}(sk, \psi)$ (when ψ is uniformly selected from $\mathcal{C}$) and the uniform distribution is at most $|\Psi|/|\mathcal{C}|$, which is negligible due to the sparseness of Ψ. This establishes that $\mathsf{KEM.Decap}$ has tailored functionality.

Finally, KEM is a tailored KEM because it has samplable and explainable domains $\mathcal{C}$ and $\mathcal{K}$, it has IND-tCCCA security, and $\mathsf{KEM.Decap}$ has tailored functionality. □

Remark 1. . As pointed out in [12], both DDH-based and DCR-based HPS could have samplable and explainable platform groups. For example, we can choose the subgroup of order q in $\mathbb{Z}_p^*$ (with $p = 2q + 1$) as the DDH group, and choose $\mathbb{Z}_{N^2}^*$ as the DCR group.

5.2 Tailored KEM Based on n-Linear Assumption

Let $\mathcal{G}(1^\kappa)$ be a group generator, that is, a ppt algorithm which outputs $(\mathbb{G}, g, p)$ where $\mathbb{G}$ is a group of prime order p (having κ bits) and g a generator of $\mathbb{G}$.

Definition 6 *The n-Linear Assumption for $\mathcal{G}(1^\kappa)$ states that for all ppt adversaries $\mathcal{B}$, the advantage of $\mathcal{B}$ defined below is negligible.*

$$\mathsf{Adv}_{\mathcal{B}}^{n\text{-}lin}(\kappa) := \Big| \Pr\left[\mathcal{B}(g_1, \ldots, g_n, g_1^{r_1}, \ldots, g_n^{r_n}, h, h^{\sum_{i=1}^{n} r_i}) = 1\right]$$

$$- \Pr\left[\mathcal{B}(g_1, \ldots, g_n, g_1^{r_1}, \ldots, g_n^{r_n}, h, h^{z}) = 1\right] \Big|,$$

```
$\mathsf{KEM.Kg}(1^\kappa)$:
    $b \leftarrow \mathbb{Z}_p$; $h \leftarrow g^b$
    For $i = 1$ to $n$
        $a_i, \alpha_i, \beta_i \leftarrow \mathbb{Z}_p$
        $g_i \leftarrow g^{a_i}$; $\omega_i = a_i^{-1} b$
        $u_i \leftarrow g_i^{\alpha_i}$; $v_i \leftarrow g_i^{\beta_i}$
    $pk = (h, (g_i, u_i, v_i)_{i \in [n]})$
    $sk \leftarrow \big((\alpha_i, \beta_i, \omega_i)_{i \in [n]}, pk\big)$
    Return $(pk, sk)$

$\mathsf{KEM.Encap}(pk)$:
    For $i = 1$ to $n$
        $r_i \leftarrow \mathbb{Z}_p$; $c_i \leftarrow g_i^{r_i}$
    $t = \mathsf{TCR}(c_1, \ldots, c_n)$
    $\pi \leftarrow \prod_{i=1}^{n} (u_i^t v_i)^{r_i}$
    $K \leftarrow h^{r_1 + \cdots + r_n}$
    $\psi \leftarrow (c_1, \ldots, c_n, \pi)$
    Return$(K, \psi)$

$\mathsf{KEM.Decap}(sk, \psi)$:
    For $i = 1$ to $n$
        Check if $c_i \in \mathbb{G}$
    $t = \mathsf{TCR}(c_1, \ldots, c_m)$
    If $\prod_{i=1}^{n} c_i^{\alpha_i t + \beta_i} \neq \pi$
        Return $(\perp)$
    $K \leftarrow \prod_{i=1}^{n} c_i^{\omega_i}$
    Return$(K)$
```

Fig. 7. KEM from n-Linear Assumption [16].

where $(\mathbb{G}, g, p) \leftarrow \mathcal{G}(1^\kappa)$*,* $(g_i)_{i \in [n]}, h \leftarrow \mathbb{G}$ *and* $(r_i)_{i \in [n]}, z \leftarrow \mathbb{Z}_p$*.*

In [16], Hofheiz and Kiltz presented a KEM based on the n-Linear Assumption for a group generator $\mathcal{G}(1^\kappa)$ and a target collision-resistant hash function, and proved its IND-CCCA security. We replicate the algorithms of this KEM in Figure 7. Note that this construction does not fall into the category of HPS-based KEMs.

Lemma 3. *If the n-Linear Assumption holds for $\mathcal{G}(1^\kappa)$, and TCR is target collision-resistant, then the Hofheinz-Kiltz KEM in Figure 7 is IND-tCCCA secure.*

Proof. In view of the results of [16] and Lemma 1, we need only prove that the KEM in Figure 7 has the VCI property.

Given an adversary $\mathcal{A}$ winning the VCI experiment with non-negligible probability, we can construct a ppt algorithm $\mathcal{B}$ solving the n-Linear problem with help of $\mathcal{A}$ with non-negligible probability. Let $(g_1, \ldots, g_n, g_1^{r_1}, \ldots, g_n^{r_n}, h, K^*)$ be a challenge instance from the n-Linear problem, where $K^* = h^{\sum_{i=1}^{n} r_i}$ or K^* is a random element from $\mathbb{G}$. Here, $\mathcal{B}$ simulates the VCI experiment for $\mathcal{A}$ using its input $(g_1^{r_1}, \ldots, g_n^{r_n}, h, K^*)$.

- $\mathcal{B}$ chooses $(x_i, y_i)_{i \in [n]}, z, z' \leftarrow \mathbb{Z}_p^*$, and computes $u_i = g_i^{x_i} h^z$ and $v_i = g_i^{y_i} h^{z'}$ for $i \in [n]$. $\mathcal{B}$ sets $pk = \big((g_i, u_i, v_i)_{i \in [n]}, h\big)$. All the elements in pk is randomly distributed, as in the real VCI experiment. Here $\mathcal{B}$ implicitly sets $sk = \big((\alpha_i, \beta_i, \omega_i)_{i \in [n]}, pk\big)$ with $\alpha_i = x_i + \omega_i z, \beta_i = y_i + \omega_i z'$ and $\omega_i = \log_{g_i} h$.
- $\mathcal{B}$ computes the challenge ciphertext $\psi^* = (c_1^*, \ldots, c_n^*, \pi^*)$ for $\mathcal{A}$, where $c_i^* := g_i^{r_i}$ for $i \in [n]$, $t^* = \mathsf{TCR}(c_1^*, \ldots, c_n^*)$ and $\pi^* = (K^*)^{zt^* + z'} \prod_{i=1}^{n} (c_i^*)^{x_i t^* + y_i}$.
    - If $K^* = h^{\sum_{i=1}^{n} r_i^*}$, we have $\pi^* = \prod_{i=1}^{n} \big(u_i^{t^*} v_i\big)^{r_i}$. Hence ψ^* is just a valid ciphertext output by the KEM's encapsulation algorithm with randomness $(r_i)_{i \in [n]}$.
    - If K^* is random, then π^* is also random, so that ψ^* is uniformly distributed in $\mathcal{C} = \mathbb{G}^n$.
- $\mathcal{B}$ uses $\big((x_i, y_i)_{i \in [n]}, z, z'\big)$ to answer $\mathcal{A}$'s constrained decryption queries (P, ψ). Let $\psi = (c_1, \ldots, c_n, \pi)$. We have that $t = \mathsf{TCR}(c_1, \ldots, c_n) \neq t^*$ due to the

target-collision resistance of TCR. $\mathcal{B}$ computes $K = \left(\frac{\pi}{\prod_{i=1}^{n} c_i^{x_i t+y_i}}\right)^{1/(zt+z')}$. If $P(K) = 1$ then $\mathcal{B}$ returns K; otherwise $\mathcal{B}$ returns $\perp$.

- If ψ is consistent, i.e., ψ satisfies $\prod_{i=1}^{n} c_i^{\alpha_i t+\beta_i} = \pi$, then $\pi = h^{(zt+z')\sum_{i=1}^{n} r_i'} \cdot \prod_{i=1}^{n} c_i^{x_i t+y_i}$, where $t = \mathsf{TCR}(c_1, \ldots, c_n)$ and $r_i' = \log_{g_i} c_i$. Then $K = h^{\sum_{i=1}^{n} r_i'}$ is exactly the encapsulated key. Thus the correct K is returned to $\mathcal{A}$ when $P(K) = 1$.
- If ψ is NOT consistent, then $\pi \neq \prod_{i=1}^{n} c_i^{\alpha_i t+\beta_i}$. Let $\beta = \log_g \pi$, $\omega = \log_g h$, $a_i = \log_g g_i$, and $r_i' = \log_{g_i} c_i$. Then $\gamma := \beta - \sum_{i=1}^{n} a_i r_i'(\alpha_i t+\beta_i) \neq 0$. Consequently, $\log_g K = \gamma/(zt+z') + \omega \sum_{i=1}^{n} r_i'$. The following $2n+2$ equations in $2n+2$ unknowns $((x_i, y_i)_{i\in[n]}, z, z')$ are linearly independent, as long as $t \neq t^*$, which is guaranteed by the target-collision resistance of TCR:

$$\log_g u_i = a_i x_i + \omega z \quad i = 1, 2, \ldots, n$$
$$\log_g v_i = a_i y_i + \omega z' \quad i = 1, 2, \ldots, n$$
$$\log_g \pi^* = \sum_{i=1}^{n} a_i r_i (t^* x_i + y_i) + (\log_g K^*) \cdot (t^* z + z')$$
$$\gamma \left(\log_g K - \omega \sum_{i=1}^{n} r_i'\right)^{-1} = zt + z'.$$

  This establishes that $zt + z'$ is uniformly distributed over $\mathbb{Z}_p$. Therefore, $\log_g K$ is uniformly distributed over $\mathbb{Z}_p$ and the predicate P satisfies $P(K) = 0$ except with negligible probability. As a result, ψ will be correctly rejected (due to the failed predicate) except with negligible probability.

Hence, $\mathcal{B}$ provides an almost perfect decryption oracle to $\mathcal{A}$ as long as $t \neq t^*$, for all queried encapsulations $\psi \neq \psi^*$.

- Eventually, $\mathcal{B}$ returns what $\mathcal{A}$ returns.

Finally, $\mathcal{A}$'s non-negligible advantage in the VCI game is converted into $\mathcal{B}$'s non-negligible advantage in breaking the n-Linear Assumption. □

Theorem 4. *Suppose that the n-Linear Assumption holds for $\mathcal{G}(1^\kappa)$, and TCR is target collision-resistant. If groups $\mathbb{G}$ output by $\mathcal{G}(1^\kappa)$ are samplable and explainable, then the KEM in Figure 7 is a tailored KEM.*

Proof. We note that the ciphertext space $\mathcal{C}$ equals $\mathbb{G}^{n+1}$ and the encapsulated key space $\mathcal{K}$ equals $\mathbb{G}$. If group $\mathbb{G}$ is samplable and explainable, so are $\mathcal{C}$ and $\mathcal{K}$.

Next, we have $|\mathcal{C}| = p^{n+1}$. For a valid ciphertext $\psi = (c_1, \ldots, c_n, \pi)$, we note that π is uniquely determined by $c_1, \ldots, c_n$ and pk. Therefore, the valid ciphertext set $|\Psi|$ has size p^n. Consequently, a random ciphertext from $\mathbb{G}^{n+1}$ passes the verification test $\pi = \prod_{i=1}^{n} c_i^{\alpha_i t+\beta_i}$ in the decapsulation algorithm with negligible probability $1/p$. Therefore, the decapsulation algorithm has tailored functionality.

```
$\mathsf{KEM.Kg}(1^\kappa)$:
    $k \leftarrow \mathsf{PGen}(1^\kappa)$
    $pk \leftarrow i\mathcal{O}(\mathsf{Encap}(k, \cdot))$
    $sk \leftarrow k$
    Return $(pk, sk)$

$\mathsf{KEM.Encap}(pk)$:
    $r \leftarrow \{0,1\}^\kappa$
    $(K, \psi) \leftarrow i\mathcal{O}(\mathsf{Encap}(k, r))$
    Return$(K, \psi)$
$\mathsf{Encap}(k, r)$:
    $\psi \leftarrow \mathsf{PRG}(r)$
    $K \leftarrow \mathsf{PEval}(k, \psi)$
    Return$(K, \psi)$

$\mathsf{KEM.Decap}(sk, \psi)$:
    $k \leftarrow sk$
    $K \leftarrow \mathsf{PEval}(k, \psi)$
    Return$(K)$
```

Fig. 8. Sahai-Waters KEM from $i\mathcal{O}$ and Puncturable PRF [24].

Together with Lemma 3, it follows that the KEM in Figure 7 is a tailored, and therefore suitable for the application of Theorem 1.

5.3 Tailored KEM Based on Indistinguishability Obfuscation and Puncturable PRF

Background definitions for this construction can be found in [24] and the full paper [22].

Sahai and Waters [24] gave a KEM construction from an indistinguishability obfuscator ($i\mathcal{O}$) and a puncturable PRF, as shown in Figure 8. Their construction makes use of a Pseudo-Random Generator (PRG) $\mathsf{PRG} : \{0,1\}^\kappa \to \{0,1\}^{2\kappa}$ and a puncturable PRF family $\mathsf{PRF} = (\mathsf{PGen}, \mathsf{PEval}, \mathsf{Punc})$ whose functions map $\{0,1\}^{2\kappa}$ to $\{0,1\}^\kappa$. We assume that (descriptions of) PRG and PRF are implicitly part of the inputs to $\mathsf{KEM.Kg}$, Encap, and $\mathsf{KEM.Decap}$ in Figure 8.

The ciphertext space of the KEM is $\mathcal{C} = \{0,1\}^{2\kappa}$, the valid ciphertext set is $\Psi = \{\psi \mid \psi = \mathsf{PRG}(r); r \in \{0,1\}^\kappa\}$, and the key space is $\mathcal{K} = \{0,1\}^\kappa$. Obviously, both of $\mathcal{C}$ and $\mathcal{K}$ are efficiently samplable and explainable with $\mathsf{SampleC}^{-1}(\mathcal{C}, \psi) := \psi$ and $\mathsf{SampleK}^{-1}(\mathcal{K}, K) := K$.

Lemma 5 *If $i\mathcal{O}(\cdot)$ is an indistinguishability obfuscator for P/poly, PRG is a secure PRG, and PRF is a puncturable PRF, then the Sahai-Waters KEM in Figure 8 is IND-tCCCA secure.*

Proof. In [24], the Sahai-Waters KEM was proved to be IND-CCA secure, so it is obviously IND-CCCA secure.

Next we prove the VCI property, based on the security of PRG. If there is a ppt adversary $\mathcal{A}$ that can distinguish a random ciphertext from a random valid ciphertext with non-negligible probability, then we can construct a ppt algorithm $\mathcal{B}$ that breaks the security of PRG. Suppose $\mathcal{B}$ is given an element ψ^* and tries to decide whether ψ^* is the output of PRG or a randomly chosen element from $\mathcal{C}$. $\mathcal{B}$ will simulate a VCI experiment for $\mathcal{A}$. It first chooses a puncturable PRF PRF and calls $\mathsf{KEM.Kg}(1^\kappa)$ to generate (pk, sk). The public key pk is given to $\mathcal{A}$. Then $\mathcal{B}$ gives ψ^* as the challenge encapsulation to $\mathcal{A}$. Using the secret key sk and algorithm PEval, $\mathcal{B}$ is able to provide a (constrained) decryption oracle for $\mathcal{A}$. Finally, $\mathcal{B}$ outputs whatever $\mathcal{A}$ outputs. Then it is easy to see that $\mathcal{A}$'s non-negligible advantage in the VCI security game results in a non-negligible advantage for $\mathcal{B}$ in breaking the security of PRG.

The IND-CCCA security and VCI property in combination with Lemma 1 establish that the Sahai-Waters KEM in Figure 8 has IND-tCCCA security. □

Extracting puncturable PRFs are a strengthening of puncturable PRFs introduced in [24]; essentially, an extracting puncturable PRF acts as a strong extractor on its inputs.

Definition 7 (Extracting puncturable PRF) *Let $\epsilon(\cdot)$ and $\mathsf{h}_{min}(\cdot)$ be functions. A puncturable PRF family PRF=(PGen, PEval, Punc) mapping $\{0,1\}^{\ell_1(\kappa)}$ to $\{0,1\}^{\ell_2(\kappa)}$ is said to be* extracting with error $\epsilon(\kappa)$ for min-entropy function $\mathsf{h}_{min}(\kappa)$ *if for all $\kappa \in \mathbb{N}$ and for all random variables X on $\{0,1\}^{\ell_1(\kappa)}$ with min-entropy greater than $\mathsf{h}_{min}(\kappa)$, the statistical distance between $(k, \mathsf{PEval}(k, X))$ and $(k, U_{\ell_2(\kappa)})$ is at most $\epsilon(\kappa)$, where $k \leftarrow \mathsf{PGen}(1^\kappa)$ and $U_{\ell_2(\kappa)}$ denotes the uniform distribution over $\{0,1\}^{\ell_2(\kappa)}$. The family PRF is said to be* extracting puncturable *if the error $\epsilon(\kappa)$ is negligible (for some choice of function h_{min}).*

The existence of extracting puncturable PRFs is implied by the existence of one-way functions, as was proved in [24]:

Lemma 4. *[24] Assume that one-way functions exist. Then for all efficiently computable functions $\ell_1(\kappa)$, $\ell_2(\kappa)$, $e(\kappa)$ and $\mathsf{h}_{min}(\kappa)$ such that $\ell_1(\kappa) \geq \mathsf{h}_{min}(\kappa) \geq \ell_2(\kappa) + 2e(\kappa) + 2$, there exists an extracting puncturable PRF family $\mathsf{PRF} = (\mathsf{PGen}, \mathsf{PEval}, \mathsf{Punc})$ mapping $\{0,1\}^{\ell_1(\kappa)}$ to $\{0,1\}^{\ell_2(\kappa)}$ with error function $\epsilon(\kappa) = 2^{-e(\kappa)}$ and min-entropy function $\mathsf{h}_{min}(\kappa)$.*

Lemma 6 *If PRF is an extracting puncturable PRF obtained from Lemma 4, then the decapsulation algorithm KEM.Decap of the Sahai-Waters KEM in Figure 8 has tailored functionality.*

Proof. We show that the output of $\mathsf{PRF}(sk, \psi)$ is statistically close to the uniform distribution on $\{0,1\}^\kappa$ so long as ψ is chosen from $\mathcal{C}$ uniformly at random, and the puncturable PRF satisfies the bounds in Lemma 4.

Recall that PRF maps 2κ bits to κ bits. When ψ is randomly chosen from $\{0,1\}^{2\kappa}$, the min-entropy of ψ is 2κ. According to Lemma 4, the statistical distance between $(k, \mathsf{PEval}(k, \psi))$ and (k, U_κ) is upper-bounded by $2^{-(\kappa/2-1)}$, where $k \leftarrow \mathsf{PGen}(1^\kappa)$ and U_κ is the uniform distribution over $\{0,1\}^\kappa$. Hence, $\mathsf{KEM.Decap}$ has $2^{-(\kappa/2-1)}$-tailored functionality. □

Theorem 7. *If $i\mathcal{O}(\cdot)$ is an indistinguishability obfuscator for P/poly, PRG is a secure PRG, and PRF is an extracting puncturable PRF, then the Sahai-Waters KEM in Figure 8 is a tailored KEM.*

Proof. The fact that the KEM in Figure 8 is a tailored KEM follows immediately from Lemma 5, Lemma 6 and the fact that $\mathcal{C} = \{0,1\}^{2\kappa}$ and $\mathcal{K} = \{0,1\}^\kappa$ are efficiently samplable and explainable.

The existence of one-way functions implies the existence of PRGs and extracting puncturable PRFs. Hence the existence of one-way functions and $i\mathcal{O}$ implies the existence of a tailored KEM by the above theorem. Such a tailored KEM can further be used to build a PKE scheme encrypting ℓ bits at a time with the help of an information-theoretically secure $(\ell + s)$-XAC (for suitable parameter s), by following the construction in Figure 4; the SIM-SO-CCA security of the PKE scheme follows from Theorem 1. Thus we obtain the following corollary:

Corollary 8 *Suppose one-way functions and indistinguishability obfuscation for P/poly exist. Then there exists a PKE scheme with SIM-SO-CCA security.*

Acknowledgements

This work was done while Shengli Liu visited Prof. Kenneth G. Paterson's research group at Royal Holloway, University of London. The first author was supported by the National Natural Science Foundation of China (NSFC Grant No. 61170229 and 61373153), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No. 20110073110016), and the Scientific innovation projects of Shanghai Education Committee (Grant No. 12ZZ021). The second author was supported by EPSRC Leadership Fellowship EP/H005455/1 and by EPSRC Grant EP/L018543/1.

References

1. Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S.P., Yang, K.: On the (im)possibility of obfuscating programs. In: Kilian, J. (ed.) Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings. LNCS, vol. 2139, pp. 1–18. Springer (2001), http://dx.doi.org/10.1007/3-540-44647-8_1
2. Barak, B., Goldreich, O., Impagliazzo, R., Rudich, S., Sahai, A., Vadhan, S.P., Yang, K.: On the (im)possibility of obfuscating programs. J. ACM 59(2), 6 (2012), http://doi.acm.org/10.1145/2160158.2160159
3. Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer (2009)
4. Bellare, M., Waters, B., Yilek, S.: Identity-based encryption secure against selective opening attack. In: Ishai, Y. (ed.) Theory of Cryptography - 8th Theory of Cryptography Conference, TCC 2011, Providence, RI, USA, March 28-30, 2011. Proceedings. LNCS, vol. 6597, pp. 235–252. Springer (2011), http://dx.doi.org/10.1007/978-3-642-19571-6_15
5. Böhl, F., Hofheinz, D., Kraschewski, D.: On definitions of selective opening security. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings. LNCS, vol. 7293, pp. 522–539. Springer (2012), http://dx.doi.org/10.1007/978-3-642-30057-8_31

6. Canetti, R., Dwork, C., Naor, M., Ostrovsky, R.: Deniable encryption. In: Jr., B.S.K. (ed.) Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings. LNCS, vol. 1294, pp. 90–104. Springer (1997), http://dx.doi.org/10.1007/BFb0052229
7. Canetti, R., Feige, U., Goldreich, O., Naor, M.: Adaptively secure multi-party computation. In: Miller, G.L. (ed.) Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996. pp. 639–648. ACM (1996), http://doi.acm.org/10.1145/237814.238015
8. Cramer, R., Shoup, V.: Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 45–64. Springer (2002)
9. Cramer, R., Shoup, V.: Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. SIAM J. Comput. 33(1), 167–226 (Jan 2004), http://dx.doi.org/10.1137/S0097539702403773
10. Damgård, I., Nielsen, J.B.: Improved non-committing encryption schemes based on a general complexity assumption. In: Bellare, M. (ed.) Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings. LNCS, vol. 1880, pp. 432–450. Springer (2000), http://dx.doi.org/10.1007/3-540-44598-6_27
11. Dwork, C., Naor, M., Reingold, O., Stockmeyer, L.J.: Magic functions. J. ACM 50(6), 852–921 (2003), http://doi.acm.org/10.1145/950620.950623
12. Fehr, S., Hofheinz, D., Kiltz, E., Wee, H.: Encryption schemes secure against chosen-ciphertext selective opening attacks. In: Gilbert, H. (ed.) Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings. LNCS, vol. 6110, pp. 381–402. Springer (2010), http://dx.doi.org/10.1007/978-3-642-13190-5_20
13. Garg, S., Gentry, C., Halevi, S., Raykova, M., Sahai, A., Waters, B.: Candidate indistinguishability obfuscation and functional encryption for all circuits. In: 54th Annual IEEE Symposium on Foundations of Computer Science, FOCS 2013, 26-29 October, 2013, Berkeley, CA, USA. pp. 40–49. IEEE Computer Society (2013), http://doi.ieeecomputersociety.org/10.1109/FOCS.2013.13
14. Hemenway, B., Libert, B., Ostrovsky, R., Vergnaud, D.: Lossy encryption: Constructions from general assumptions and efficient selective opening chosen ciphertext security. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 70–88. Springer (2011)
15. Hofheinz, D.: All-but-many lossy trapdoor functions. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 209–227. Springer (2012)
16. Hofheinz, D., Kiltz, E.: Secure hybrid encryption from weakened key encapsulation. In: Menezes, A. (ed.) CRYPTO 2007. LNCS, vol. 4622, pp. 553–571. Springer (2007)
17. Hofheinz, D., Rupp, A.: Standard versus selective opening security: Separation and equivalence results. In: Lindell, Y. (ed.) Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014, San Diego, CA, USA, February 24-26, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8349, pp. 591–615. Springer (2014), http://dx.doi.org/10.1007/978-3-642-54242-8_25
18. Huang, Z., Liu, S., Qin, B.: Sender-equivocable encryption schemes secure against chosen-ciphertext attacks revisited. In: Kurosawa, K., Hanaoka, G. (eds.) Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and

Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings. Lecture Notes in Computer Science, vol. 7778, pp. 369–385. Springer (2013), http://dx.doi.org/10.1007/978-3-642-36362-7_23

19. Huang, Z., Liu, S., Qin, B., Chen, K.: Fixing the sender-equivocable encryption scheme in eurocrypt 2010. In: 2013 5th International Conference on Intelligent Networking and Collaborative Systems, Xi'an city, Shaanxi province, China, September 9-11, 2013. pp. 366–372. IEEE (2013), http://dx.doi.org/10.1109/INCoS.2013.69
20. Katz, J., Ostrovsky, R.: Round-optimal secure two-party computation. In: Franklin, M.K. (ed.) Advances in Cryptology - CRYPTO 2004, 24th Annual International CryptologyConference, Santa Barbara, California, USA, August 15-19, 2004, Proceedings. LNCS, vol. 3152, pp. 335–354. Springer (2004), http://dx.doi.org/10.1007/978-3-540-28628-8_21
21. Lai, J., Deng, R.H., Liu, S., Weng, J., Zhao, Y.: Identity-based encryption secure against selective opening chosen-ciphertext attack. In: Nguyen, P.Q., Oswald, E. (eds.) Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings. Lecture Notes in Computer Science, vol. 8441, pp. 77–92. Springer (2014), http://dx.doi.org/10.1007/978-3-642-55220-5_5
22. Liu, S., Paterson, K.G.: Simulation-based selective opening cca security for pke from key encapsulation mechanisms. Cryptology ePrint Archive, Report 2015/010 (2015), http://eprint.iacr.org/
23. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: Dwork, C. (ed.) STOC 2008. pp. 187–196. ACM (2008)
24. Sahai, A., Waters, B.: How to use indistinguishability obfuscation: deniable encryption, and more. In: Shmoys, D.B. (ed.) Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014. pp. 475–484. ACM (2014), http://doi.acm.org/10.1145/2591796.2591825