Identity-Based Encryption Secure Against Selective Opening Chosen-Ciphertext Attack

Junzuo Lai[1], Robert H. Deng[2], Shengli Liu[3⋆],
Jian Weng[1], and Yunlei Zhao[4]

[1] Department of Computer Science, Jinan University, China
{laijunzuo,cryptjweng}@gmail.com
[2] School of Information Systems,
Singapore Management University, Singapore
robertdeng@smu.edu.sg
[3] Department of Computer Science and Engineering,
Shanghai Jiao Tong University, China
slliu@sjtu.edu.cn
[4] Software School, Fudan University,
SKLOIS (Beijing) and KLAISTC (Wuhan), China
yunleizhao@gmail.com

Abstract. Security against selective opening attack (SOA) requires that in a multi-user setting, even if an adversary has access to all ciphertexts from users, and adaptively corrupts some fraction of the users by exposing not only their messages but also the random coins, the remaining unopened messages retain their privacy. Recently, Bellare, Waters and Yilek considered SOA-security in the identity-based setting, and presented the first identity-based encryption (IBE) schemes that are proven secure against selective opening chosen plaintext attack (SO-CPA). However, how to achieve SO-CCA security for IBE is still open.
In this paper, we introduce a new primitive called extractable IBE and define its IND-ID-CCA security notion. We present a generic construction of SO-CCA secure IBE from an IND-ID-CCA secure extractable IBE with "One-Sided Public Openability"(1SPO), a collision-resistant hash function and a strengthened cross-authentication code. Finally, we propose two concrete constructions of extractable 1SPO-IBE schemes, resulting in the first simulation-based SO-CCA secure IBE schemes without random oracles.

Key words: identity-based encryption, chosen ciphertext security, selective opening security

1 Introduction

Security against chosen-plaintext attack (CPA) and security against chosen-ciphertext attack (CCA) are now well-accepted security notions for encryption. However, they may not suffice in some scenarios. For example,

⋆ Corresponding author

in a secure multi-party computation protocol, the communications among parties are encrypted, but an adversary may corrupt some parties to obtain not only their messages, but also the random coins used to encrypt the messages. This is the so-called "selective opening attack" (SOA). The traditional CPA (CCA) security does not imply SOA-security [1].

IND-SOA Security vs. SIM-SOA Security. There are two ways to formalize the SOA-security notion [2, 4, 18] for encryption, namely IND-SOA and SIM-SOA. IND-SOA security requires that no probabilistic polynomial-time (PPT) adversary can distinguish an unopened ciphertext from an encryption of a fresh message, which is distributed according to the conditional probability distribution (conditioned on the opened ciphertexts). Such a security notion requires that the joint plaintext distribution should be "efficiently conditionally re-samplable", which restricts SOA security to limited settings. To eliminate this restriction, the so-called full-IND-SOA security [5] was suggested. Unfortunately, there have been no known encryption schemes with full-IND-SOA security up to now. On the other hand, SIM-SOA security requires that anything that can be computed by a PPT adversary from all the ciphertexts and the opened messages together with the corresponding randomness can also be computed by a PPT simulator with only the opened messages. SIM-SOA security imposes no limitation on the message distribution, and it implies IND-SOA security.

The SOA-security (IND-SOA vs. SIM-SOA) is further classified into two notions, security against selective opening chosen-plaintext attacks (IND-SO-CPA vs. SIM-SO-CPA) and that against selective opening chosen-ciphertext attacks (IND-SO-CCA vs. SIM-SO-CCA), depending on whether the adversary has access to a decryption oracle or not.

SOA for PKE. The initial work about SOA security for encryption was done in the traditional public-key encryption (PKE) field. In [2], Bellare, Hofheinz and Yilek showed that any lossy encryption is able to achieve IND-SO-CPA security, and SIM-SOA security is achievable as well if the lossy encryption is "efficiently openable". This result suggests the existence of many IND-SO-CPA secure PKEs based on number-theoretic assumptions, such as the Decisional Diffie-Hellman (DDH), Decisional Composite Residuosity (DCR) and Quadratic Residuosity (QR), and lattices-related assumptions [25, 14, 16, 17, 6, 26, 22]. Later, Hemenway et al. [15] showed that both re-randomizable public-key encryption and statistically-hiding $\binom{2}{1}$-oblivious transfer imply lossy encryption.

In [15], Hemenway et al. also proposed a paradigm of constructing IND-SO-CCA secure PKE from selective-tag weakly secure and separable tag-based PKE with the help of chameleon hashing. Hofheinz [19] showed how to get SO-CCA secure PKE with compact ciphertexts. Fehr et al. [13] proved that sender-equivocable (NC-CCA) security implies SIM-SO-CCA security, and showed how to construct PKE schemes with NC-CCA security based on hash proof systems with explainable domains and L-cross-authentication codes (L-XAC, in short). Recently, Huang et al. [20, 21] showed that using the method proposed in [13] to construct SIM-SO-CCA secure PKE, L-XAC needs to be *strong*.

SOA for IBE. Compared with SOA security for PKE, SOA-secure IBE is lagged behind. The subtlety of proving security for IBE comes from the fact that a key generation oracle should be provided to an adversary to answer private key queries with respect to different identities, and the adversary is free to choose the target identity. It was not until 2011 that the question how to build SOA-secure IBE was answered by Bellare et al. in [3]. Bellare et al. [3] proposed a general paradigm to achieve SIM-SO-CPA security from IND-ID-CPA secure and "One-Sided Publicly Openable" (1SPO) IBE schemes. They also presented two 1SPO IND-ID-CPA IBE schemes without random oracles, one based on the Boyen-Waters anonymous IBE [8] and the other based on Water's dual-system approach [27], yielding two SIM-SO-CPA secure IBE schemes. The second SIM-SO-CPA secure IBE scheme proposed in [3] can be extended to construct the first SIM-SO-CPA secure hierarchical identity-based encryption (HIBE) scheme without random oracles. One may hope to obtain SIM-SO-CCA secure IBEs by applying the BCHK transform [7] to SIM-SO-CPA secure HIBEs. Unfortunately, as mentioned in [3], the BCHK transform [7] does not work in the SOA setting. Consequently, how to construct SIM-SO-CCA secure IBEs has been left as an open question.

Our contribution. We answer the open question of achieving SIM-SO-CCA secure IBE with a new primitive called extractable IBE with One-Sided Public Openability (extractable 1SPO-IBE, in short) and a *strengthened* cross authentication codes (XAC).

- We define a new primitive named extractable 1SPO-IBE and its IND-ID-CCA security notion.
- We define a new property of XAC: *semi-uniqueness*. If an XAC is strong and semi-unique, we say it is a *strengthened* XAC. We also show that the efficient construction of XAC proposed by Fehr et al. [13] is a strengthened XAC actually.

- We propose a paradigm of building SIM-SO-CCA secure IBE from IND-ID-CCA secure extractable 1SPO-IBE, collision-resistant hash function and strengthened XAC. Actually, we can define the notion of extractable 1SPO-PKE similarly, and use the same method to provide a paradigm of building SIM-SO-CCA secure PKE from IND-CCA secure extractable 1SPO-PKE, collision-resistant hash function and strengthened XAC, which is different from the paradigm proposed by Fehr et al. [13].
- We construct extractable 1SPO-IBE schemes without random oracles by adapting anonymous IBEs, including the anonymous extension of Lewko-Waters IBE scheme [23] by De Caro, Iovino and Persiano [11] and the Boyen-Waters anonymous IBE [8].

Extractable 1SPO-IBE. Extractable IBE combines one-bit IBE and identity-based key encapsulation mechanism (IB-KEM). The message space of extractable IBE is $\{0,1\}$. An encryption of 1 under identity ID also encapsulates a session key K, behaving like IB-KEM. More precisely, $(C,K) \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex},\mathsf{ID},1;R)$ and $C \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex},\mathsf{ID},0;R')$, where PK_{ex} is the public parameter and R,R' are the randomness used in encryption. If C is from the encryption of 1 under ID, the decryption algorithm, $(b,K) \leftarrow \mathsf{Decrypt}_{ex}(\mathsf{PK},\mathsf{SK}_{\mathsf{ID}},C)$, is able to use the private key $\mathsf{SK}_{\mathsf{ID}}$ to recover message $b=1$ as well as the encapsulated session key K. As for an encryption of 0, say $C=\mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex},\mathsf{ID},0;R')$, the decryption algorithm can recover message $b=0$ but generate a *uniformly random* key K as well.

The security of extractable IBE requires that given a challenge ciphertext C^* and a challenge key K^* under some identity ID^*, no PPT adversary can distinguish, except with negligible advantage, whether C^* is an encryption of 1 under identity ID^* and K^* is the encapsulated key of C^*, or C^* is an encryption of 0 under identity ID^* and K^* is a uniformly random key, even if the adversary has access to a key generation oracle for private key $\mathsf{SK}_{\mathsf{ID}}$ with $\mathsf{ID} \neq \mathsf{ID}^*$ and a decryption oracle to decrypt ciphertexts other than C^* under ID^*. Obviously, the security notion of extractable IBE inherits IND-ID-CCA security of one-bit IBE and IND-ID-CCA security of IB-KEM.

An extractable IBE is called *one-sided publicly openable* (1SPO), if there exists a PPT *public* algorithm POpen as follows: given $C=\mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex},\mathsf{ID},0;R)$, it outputs random coins R' which is uniformly distributed subject to $C=\mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex},\mathsf{ID},0;R')$. One-sided public openability [3] is an IBE-analogue of a weak form of deniable PKE [9] (which plays an essential role in the construction of NC-CPA/CCA secure PKE in [13],

consequently achieving SIM-SO-CPA/CCA secure PKE). In [3], Bellare et al. used one-bit 1SPO-IBE to construct SIM-SO-CPA secure IBE.

SIM-SO-CCA SECURE IBE FROM EXTRACTABLE 1SPO-IBE. We follow the line of [13], which achieves SIM-SO-CCA secure PKE from sender-equivocable or weak deniable encryption and XAC. We give a high-level description on how to construct a SIM-SO-CCA secure IBE scheme from an extractable 1SPO-IBE scheme characterized by $(\mathsf{Encrypt}_{ex}, \mathsf{Decrypt}_{ex})$, with the help of a collision-resistant hash function H and a strengthened $\ell+1$-cross-authentication code XAC.

First, we roughly recall the notion of cross-authentication code XAC, which was introduced in [13]. In an $\ell+1$-cross-authentication code XAC, an authentication tag T can be computed from a *list* of random keys $K_1, \ldots, K_{\ell+1}$ (without a designated message) using algorithm XAuth. The XVer algorithm is used to verify the correctness of the tag T with *any* single key K. If K is from the list, XVer will output 1. If K is uniformly randomly chosen, XVer will output 1 with negligible probability. If an XAC is *strong* and *semi-unique*, we say it is a strengthened XAC. Strongness of XAC means given $(K_i)_{1\le i\le \ell+1, i\neq j}$ and T, a new key $\hat{K}_j$ which is statistically indistinguishable to K_i, can be efficiently sampled. Semi-uniqueness of XAC requires that K can be parsed to (K_a, K_b) and for a fixed T and K_a, there is at most one K_b satisfying $\mathsf{XVer}((K_a, K_b), T) = 1$.

Our cryptosystem has message space $\{0,1\}^\ell$, and encryption of an ℓ-bit message $M = m_1 \| \cdots \| m_\ell$ for an identity ID is performed bitwise, with one ciphertext element per bit. For each bit m_i, the corresponding ciphertext element C_i is an encryption of m_i under ID, which is generated by the encryption algorithm of the extractable 1SPO-IBE scheme. As shown in [24], a scheme which encrypts long message bit-by-bit is vulnerable to *quoting attacks*. Hence, we use a collision-resistant hash function and a strengthened $\ell+1$-cross-authentication code XAC to bind $C_1, \ldots, C_\ell$ together to resist quoting attacks.

Specifically, let K_a be a public parameter, in our SIM-SO-CCA secure IBE scheme, encryption of an ℓ-bit message $M = m_1 \| \cdots \| m_\ell \in \{0,1\}^\ell$ for an identity ID is given by the ciphertext $CT = (C_1, \ldots, C_\ell, T)$, where

$$\begin{cases} (C_i, K_i) \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{ID}, 1) & \text{if } \ m_i = 1 \\ C_i \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{ID}, 0),\ K_i \leftarrow \mathcal{K} & \text{if } \ m_i = 0 \end{cases},$$

$$K_b = \mathsf{H}(\mathsf{ID}, C_1, \ldots, C_\ell),\ K_{\ell+1} = (K_a, K_b),\ T = \mathsf{XAuth}(K_1, \ldots, K_{\ell+1}).$$

Here C_i is from the extractable 1SPO-IBE encryption of bit m_i, and K_i is the encapsulated key or randomly chosen key depending on $m_i = 1$ or 0. Finally, XAC tag T glues all the C_is together. Given a ciphertext

$CT = (C_1, \ldots, C_\ell, T)$ for identity ID, the decryption algorithm first checks whether $\mathsf{XVer}(K'_{\ell+1}, T) = 1$ or not, where $K'_{\ell+1} = (K_a, \mathsf{H}(\mathsf{ID}, C_1, \ldots, C_\ell))$. If not, it outputs message $\overbrace{0 \cdots 0}^{\ell}$. Otherwise, it uses $\mathsf{Decrypt}_{ex}$ of the extractable 1SPO-IBE scheme to recover bit m'_i and a session key K'_i from each C_i. If $m'_i = 0$, set $m''_i = 0$, otherwise set $m''_i = \mathsf{XVer}(K'_i, T)$. Finally, it outputs $M'' = m''_1 \| \cdots \| m''_\ell$. We assume that the key space $\mathcal{XK}$ of the strengthened XAC and the session key space $\mathcal{K}$ of the extractable 1SPO-IBE are identical (i.e., $\mathcal{K}$=$\mathcal{XK}$), and $\mathcal{K}$ is efficiently samplable and explainable domain.

As for the $\mathsf{SIM\text{-}SO\text{-}CCA}$ security of the IBE scheme, the proving line is to show that encryptions of ℓ ones are "equivocable" ciphertexts, which can be opened to arbitrary messages, and the "equivocable" ciphertexts are computationally indistinguishable from real challenge ciphertexts in an SOA setting, i.e., even if the adversary is given access to a corruption oracle to get the opened messages and randomness, a decryption oracle to decrypt ciphertexts and a key generation oracle to obtain private keys. If so, a PPT SOA-simulator can be constructed to create "equivocable" ciphertexts (i.e., encryptions of ℓ ones) as challenge ciphertexts, then open them accordingly, and $\mathsf{SIM\text{-}SO\text{-}CCA}$ security follows.

To prove a challenge ciphertext $CT = (C_1, \ldots, C_\ell, T)$ under ID, which encrypts $m_1 \| \cdots \| m_\ell$, is indistinguishable from encryption of ℓ ones in the SOA setting, we use hybrid argument. For each $m_i = 0$, we replace (C_i, K_i) (which is used to create CT under ID) with an extractable 1SPO-IBE encryption of 1. If this replacement is distinguishable to an adversary $\mathcal{A}$, then another PPT algorithm $\mathcal{B}$ can simulate SOA-environment for $\mathcal{A}$ by setting (C_i, K_i) to be its own challenge (C^*, K^*) under ID, and use $\mathcal{A}$ to break the $\mathsf{IND\text{-}ID\text{-}CCA}$ security of the extractable 1SPO-IBE. The subtlety lies in how $\mathcal{B}$ deals with $\mathcal{A}$'s decryption query $\widetilde{CT} = (\widetilde{C}_1, \ldots, \widetilde{C}_l, \widetilde{T})$ under ID with $\widetilde{C}_j = C^*$ for some $j \in [\ell]$. Recall that $\mathcal{B}$ is not allowed to issue a private key query $\langle \mathsf{ID} \rangle$ or a decryption query $\langle \mathsf{ID}, C^* \rangle$ to it's own challenger in the extractable 1SPO-IBE security game. In this case, $\mathcal{B}$ will resort to XAC to set $\widetilde{m}''_j = \mathsf{XVer}(K^*, \widetilde{T})$. Observe that, if $(C^*, K^*) = \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{ID}, 1)$, then $\widetilde{m}''_j = \mathsf{XVer}(K^*, \widetilde{T}) = 1$, which is exactly the same as the output of $\mathsf{Decrypt}$ algorithm. If $C^* = \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{ID}, 0)$ and K^* is random, then $\widetilde{m}''_j = \mathsf{XVer}(K^*, \widetilde{T}) = 0$ except with negligible probability, due to XAC's security against substitution attacks. This is also consistent with the output of the decryption algorithm, except with negligible probability. Hence, with overwhelming probability, $\mathcal{B}$ sim-

ulates SOA-environment for $\mathcal{A}$ properly. Note that to apply XAC's security against substitution attacks, we require:

1. $\widetilde{T} \neq T$, which is guaranteed by XAC's *semi-unique* property and *collision resistance* of hash function.
2. K^* should not be revealed to adversary $\mathcal{A}$. Therefore, in the corruption phase, if $\mathcal{B}$ is asked to open (C^*, K^*), it first resamples a $\hat{K}$, which is statistically indistinguishable from K^*. This is guaranteed by the *strongness* of XAC. Then, C will be opened to 0 with algorithm POpen, and $\hat{K}$ (instead of K^*) is opened with a suitable randomness.

Construction of Extractable 1SPO-IBE. In [3], Bellare et al. proposed two one-bit 1SPO-IBEs, one based on the anonymous extension of Lewko-Waters IBE scheme [23] by De Caro, Iovino and Persiano [11] and the other based on the Boyen-Waters anonymous IBE [8]. Both schemes rely on a pairing $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. The 1SPO property of the two one-bit IBE schemes is guaranteed by the fact that $\mathbb{G}$ is an *efficiently samplable and explainable domain*, which is characterized by two PPT algorithms Sample and Sample^{-1} for group $\mathbb{G}$. More precisely, Sample chooses an element g from $\mathbb{G}$ uniformly at random, and $\mathsf{Sample}^{-1}(\mathbb{G}, g)$ will output a uniformly distributed R subject to $g = \mathsf{Sample}(\mathbb{G}; R)$. Details of algorithms Sample and Sample^{-1} are given in [3].

Unfortunately, the one-bit 1SPO-IBE schemes in [3] are not extractable IBEs. No session keys can be extracted from encryptions of 1, and the schemes are vulnerable to chosen-ciphertext attacks. Therefore, we have to resort to new techniques for extractable 1SPO-IBE.

We start from anonymous IBE schemes in [11, 8]. Recall that an encryption of a message M for an identity ID in anonymous IBEs [11, 8] takes the form of $(c_0 = f_0(\mathsf{PK}, s, s_0),\ c_1 = f_1(\mathsf{PK}, \mathsf{ID}, s, s_1),\ c_2 = e(g, g)^{\alpha s} \cdot M)$, where PK denotes the system's public parameter, α is the master secret key, s, s_0, s_1 are the randomness used in the encryption algorithm, f_0, f_1 are two efficient functions and each of c_0, c_1 denotes one or several elements in $\mathbb{G}$. The private key $\mathsf{SK}_{\mathsf{ID}}$ is structured such that pairings with group elements of (c_1, c_2) result in $e(g, g)^{\alpha s}$, hence the message M can be recovered from c_2.

The idea of constructing extractable 1SPO-IBE is summerized as follows. Firstly, we generate ciphertexts of the form $(c'_0 = f'_0(\mathsf{PK}, s, s_0),\ c'_1 = f'_1(\mathsf{PK}, \mathsf{ID}, \mathsf{ID}', s, s_1))$, where $\mathsf{ID}' = \mathsf{H}(\mathsf{ID}, c'_0)$ and H is a collision-resistant hash function. The structure of (c'_0, c'_1) is characterized by the shared randomness s and this structure can be publicly verified. The master secret key is now (α, β). Correspondingly the private key $\mathsf{SK}_{\mathsf{ID}} = (\mathsf{SK}_{\mathsf{ID},1}, \mathsf{SK}_{\mathsf{ID},2})$,

and $\mathsf{SK}_{\mathsf{ID},i}(i = 1, 2)$ are generated by the master secret key α and β respectively, in a similar way as that in the anonymous IBEs [11, 8]. Consequently, $\mathsf{SK}_{\mathsf{ID},1}$ and $\mathsf{SK}_{\mathsf{ID},2}$ help generate $e(g,g)^{\alpha s}$ and $e(g,g)^{\beta s}$ from (c'_0, c'_1).

Next, we use $e(g,g)^{\alpha s}$ to blind (c'_0, c'_1) and obtain $(c''_0 = f''_1(\mathsf{PK}, s, s_0)$, $c''_1 = f''_1(\mathsf{PK}, \mathsf{ID}, \mathsf{ID}', s, s_1))$, which satisfies the following properties:

1. Without the private key $\mathsf{SK}_{\mathsf{ID}} = (\mathsf{SK}_{\mathsf{ID},1},\ \mathsf{SK}_{\mathsf{ID},2})$ for ID, the relationship between c''_0 and c''_1 (that they share the same s) is hidden from any PPT adversary.
2. With $\mathsf{SK}_{\mathsf{ID},1}$ and $\mathsf{SK}_{\mathsf{ID},2}$, it is still possible to generate $e(g,g)^{\alpha s}$ and $e(g,g)^{\beta s}$ from the blinded ciphertext (c''_0, c''_1).
3. Given the blinded factor $e(g,g)^{\alpha s}$, (c''_0, c''_1) can be efficiently changed back to (c'_0, c'_1).

Finally, we obtain the extractable 1SPO-IBE with the following features:

$$\mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{ID}, b) = \begin{cases} ((c''_0, c''_1), K) = \big((f''_1(\mathsf{PK}, s, s_0), f''_1(\mathsf{PK}, \mathsf{ID}, \mathsf{ID}', s, s_1)), e(g,g)^{\beta s}\big) & b = 1 \\ (c''_0, c''_1) \leftarrow \mathsf{Sample}(\mathbb{G}) & b = 0 \end{cases}.$$

- Given a ciphertext $C = (c''_0, c''_1)$ for ID, the decryption algorithm first uses $\mathsf{SK}_{\mathsf{ID},1}$ to compute a blinding factor from (c''_0, c''_1). Then, it uses the blinding factor to retrieve (c'_0, c'_1) from (c''_0, c''_1). Next, it checks whether (c'_0, c'_1) have a specific structure. If yes, it outputs message 1 and computes the encapsulated session key from (c''_0, c''_1) using $\mathsf{SK}_{\mathsf{ID},2}$; otherwise, it outputs message 0 and a uniformly random session key.
- Algorithm POpen for 1SPO can be implemented with Sample^{-1}.

We emphasize that the 2-hierarchical IBE structure (when encrypting 1) helps to answer decryption queries in the IND-ID-CCA security proof of the above extractable 1SPO-IBE. In the private key $\mathsf{SK}_{\mathsf{ID}} = (\mathsf{SK}_{\mathsf{ID},1}, \mathsf{SK}_{\mathsf{ID},2})$, $\mathsf{SK}_{\mathsf{ID},2}$ is used to generate the encapsulated key $e(g,g)^{\beta s}$ when encrypting 1, and $\mathsf{SK}_{\mathsf{ID},1}$ is used to generate a blind factor $e(g,g)^{\alpha s}$, which helps to convert the publicly verifiable structure of (c'_0, c'_1) to a privately verifiable structure, resulting in IND-ID-CCA secure extractable 1SPO-IBE.

Organization. The rest of the paper is organized as follows. Some preliminaries are given in Section 2. We introduce the notion and security model of extractable 1SPO-IBE in Section 3. The notion of strengthened XAC and its efficient construction are given in Section 4. We propose a

paradigm of building SIM-SO-CCA secure IBE from IND-ID-CCA secure extractable 1SPO-IBE, collision-resistant hash function and strengthened XAC in Section 5. We present two IND-ID-CCA secure extractable 1SPO-IBE schemes in Section 6.

2 Preliminaries

If S is a set, then $s_1, \ldots, s_t \leftarrow S$ denotes the operation of picking elements $s_1, \ldots, s_t$ uniformly at random from S. If $n \in \mathbb{N}$ then $[n]$ denotes the set $\{1, \ldots, n\}$. For $i \in \{0,1\}^*$, $|i|$ denotes the bit-length of i. If $x_1, x_2, \ldots$ are strings, then $x_1 \| x_2 \| \cdots$ denotes their concatenation. For a probabilistic algorithm A, we denote $y \leftarrow A(x; R)$ the process of running A on input x and with randomness R, and assigning y the result. Let $\mathcal{R}_A$ denote the randomness space of A, and we write $y \leftarrow A(x)$ for $y \leftarrow A(x; R)$ with R chosen from $\mathcal{R}_A$ uniformly at random. A function $f(\kappa)$ is *negligible*, if for every $c > 0$ there exists a κ_c such that $f(\kappa) < 1/\kappa^c$ for all $\kappa > \kappa_c$.

2.1 Key Derivation Functions

A family of *key derivation functions* [12] $\mathcal{KDF} = \{\mathsf{KDF}_i : \mathcal{X}_i \to \mathcal{K}_i\}$, indexed by $i \in \{0,1\}^*$, is *secure* if, for all PPT algorithms $\mathcal{A}$ and for sufficiently large i, the distinguishing advantage $Adv^{\mathcal{A}}_{\mathcal{KDF}}(i)$ is negligible (in $|i|$), where

$$Adv^{\mathcal{A}}_{\mathcal{KDF}}(i) = |\Pr[\mathcal{A}(\mathsf{KDF}_i, \mathsf{KDF}_i(x)) = 1 \,|\mathsf{KDF}_i \leftarrow \mathcal{KDF}, x \leftarrow \mathcal{X}_i] - \Pr[\mathcal{A}(\mathsf{KDF}_i, K) = 1 \,|\mathsf{KDF}_i \leftarrow \mathcal{KDF}, K \leftarrow \mathcal{K}_i]| \,.$$

The above definition is for presentation simplicity. In general, the index i should be generated by a PPT sampler algorithm on the security parameter κ. For notational convenience, we ignore the index i of a key derivation function.

2.2 Efficiently samplable and explainable domain

A domain $\mathcal{D}$ is *efficiently samplable and explainable* [13] iff there exist two PPT algorithms:

- $\mathsf{Sample}(\mathcal{D}; R)$: On input random coins $R \leftarrow \mathcal{R}_{\mathsf{Sample}}$ and a domain $\mathcal{D}$, it outputs an element uniformly distributed over $\mathcal{D}$.
- $\mathsf{Sample}^{-1}(\mathcal{D}, x)$: On input $\mathcal{D}$ and *any* $x \in \mathcal{D}$, this algorithm outputs R that is uniformly distributed over the set $\{R \in \mathcal{R}_{\mathsf{Sample}} \,|\mathsf{Sample}(\mathcal{D}; R) = x\}$.

3 Extractable IBE with One-Sided Public Openability (Extractable 1SPO-IBE)

Formally, an extractable identity-based encryption (extractable IBE) scheme consists of the following four algorithms:

$\mathsf{Setup}_{ex}(1^\kappa)$ takes as input a security parameter κ. It generates a public parameter PK and a master secret key MSK. The public parameter PK defines an identity space $\mathcal{ID}$, a ciphertext space $\mathcal{C}$ and a session key space $\mathcal{K}$.

$\mathsf{KeyGen}_{ex}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$ takes as input the public parameter PK, the master secret key MSK and an identity $\mathsf{ID} \in \mathcal{ID}$. It produces a private key $\mathsf{SK}_{\mathsf{ID}}$ for the identity ID.

$\mathsf{Encrypt}_{ex}(\mathsf{PK}, \mathsf{ID}, m)$ takes as input the public parameter PK, an identity $\mathsf{ID} \in \mathcal{ID}$ and a message $m \in \{0,1\}$. It outputs a ciphertext C if $m = 0$, and outputs a ciphertext and a session key (C, K) if $m = 1$. Here $K \in \mathcal{K}$.

$\mathsf{Decrypt}_{ex}(\mathsf{PK}, \mathsf{SK}_{\mathsf{ID}}, C)$ takes as input the public parameter PK, a private key $\mathsf{SK}_{\mathsf{ID}}$ and a ciphertext $C \in \mathcal{C}$. It outputs a message $m' \in \{0,1\}$ and a session key $K' \in \mathcal{K}$.

Correctness. An extractable IBE scheme has completeness error ϵ, if for all κ, $\mathsf{ID} \in \mathcal{ID}$, $m \in \{0,1\}$, $(\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}_{ex}(1^\kappa)$, $C/(C,K) \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}, \mathsf{ID}, m)$, $\mathsf{SK}_{\mathsf{ID}} \leftarrow \mathsf{KeyGen}_{ex}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID})$ and $(m', K') \leftarrow \mathsf{Decrypt}_{ex}(\mathsf{PK}, \mathsf{SK}_{\mathsf{ID}}, C)$:

- The probability that $m' = m$ is at least $1 - \epsilon$, where the probability is taken over the coins used in encryption.
- If $m = 1$ then $m' = m$ and $K' = K$. If $m' = 0$, K' is uniformly distributed in $\mathcal{K}$.

Security. The IND-ID-CCA security of extractable IBE is twisted from IND-ID-CCA security of one-bit IBE and IND-ID-CCA security of identity-based key encapsulation mechanism (IB-KEM). The security notion is defined using the following game between a PPT adversary $\mathcal{A}$ and a challenger.

Setup The challenger runs $\mathsf{Setup}_{ex}(1^\kappa)$ to obtain a public parameter PK and a master secret key MSK. It gives the public parameter PK to the adversary.

Query phase 1 The adversary $\mathcal{A}$ adaptively issues the following queries:

- Key generation query $\langle \mathsf{ID} \rangle$: the challenger runs KeyGen_{ex} on ID to generate the corresponding private key $\mathsf{SK}_{\mathsf{ID}}$, which is returned to $\mathcal{A}$.
- Decryption query $\langle \mathsf{ID}, C \rangle$: the challenger runs KeyGen_{ex} on ID to get the private key, then use the key to decrypt C with $\mathsf{Decrypt}_{ex}$ algorithm. The result is sent back to $\mathcal{A}$.

Challenge The adversary $\mathcal{A}$ submits a challenge identity ID^*. The only restriction is that, $\mathcal{A}$ did not issue a private key query for ID^* in Query phase 1. The challenger first selects a random bit $\delta \in \{0, 1\}$. If $\delta = 1$, the challenger computes $(C^*, K^*) \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}, \mathsf{ID}^*, 1)$. Otherwise (i.e., $\delta = 0$), the challenger computes $C^* \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}, \mathsf{ID}^*, 0)$ and chooses $K^* \leftarrow \mathcal{K}$. Then, the challenge ciphertext and session key (C^*, K^*) are sent to the adversary by the challenger.

Query phase 2 This is identical to Query phase 1, except that the adversary does not request a private key for ID^* or the decryption of $\langle \mathsf{ID}^*, C^* \rangle$.

Guess The adversary $\mathcal{A}$ outputs its guess $\delta' \in \{0, 1\}$ for δ and wins the game if $\delta = \delta'$.

The advantage of the adversary in this game is defined as $\mathsf{Adv}^{\mathsf{cca}}_{\mathsf{ex\text{-}IBE},\mathcal{A}}(\kappa) = |\mathsf{Pr}[\delta' = 1|\delta = 1] - \mathsf{Pr}[\delta' = 1|\delta = 0]|$, where the probability is taken over the random bits used by the challenger and the adversary.

Definition 1 *An extractable IBE scheme is IND-ID-CCA secure, if the advantage in the above security game is negligible for all PPT adversaries.*

We say that an extractable IBE scheme is IND-sID-CCA secure if we add an **Init** stage before setup in the above security game where the adversary commits to the challenge identity ID^*.

Definition 2 (Extractable 1SPO-IBE) *An extractable IBE scheme is* One-Sided Publicly Openable *if it is associated with a PPT public algorithm* POpen *such that for all* PK *generated by* $(\mathsf{PK}, \mathsf{MSK}) \leftarrow \mathsf{Setup}_{ex}(1^\kappa)$*, for all* $\mathsf{ID} \in \mathcal{ID}$ *and any* $C \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}, \mathsf{ID}, 0)$*, it holds that: the output of* $\mathsf{POpen}(\mathsf{PK}, \mathsf{ID}, C)$ *distributes uniformly at random over* $\mathsf{Coins}(\mathsf{PK}, \mathsf{ID}, C, 0)$*, where* $\mathsf{Coins}(\mathsf{PK}, \mathsf{ID}, C, 0)$ *denotes the set of random coins* $\{\tilde{R} \mid C = \mathsf{Encrypt}_{ex}(\mathsf{PK}, \mathsf{ID}, 0; \tilde{R})\}$.

4 Strengthened Cross-authentication Codes

In this section, we first review the notion and security requirements of cross-authentication codes introduced in [13]. Then we define a new property of cross-authentication codes: *semi-unique*. If a cross-authentication

code is *strong* and *semi-unique*, we say it is a *strengthened* cross-authentication code, which will play an important role in our construction of SIM-SO-CCA secure IBE. Finally, we will show that the efficient construction of cross-authentication code proposed by Fehr et al. [13] is actually a strengthened cross-authentication code.

Definition 3 (L-Cross-authentication code.) *For $L \in \mathbb{N}$, an L-cross-authentication code XAC is associated with a key space $\mathcal{XK}$ and a tag space $\mathcal{XT}$, and consists of three PPT algorithms XGen, XAuth and XVer. $\mathsf{XGen}(1^\kappa)$ produces a uniformly random key $K \in \mathcal{XK}$, deterministic algorithm $\mathsf{XAuth}(K_1, \ldots, K_L)$ outputs a tag $T \in \mathcal{XT}$, and deterministic algorithm $\mathsf{XVer}(K, T)$ outputs a decision bit[5]. The following is required:*

Correctness. *For all $i \in [L]$, the probability*

$$\mathsf{fail}_{\mathsf{XAC}}(\kappa) := \Pr[\mathsf{XVer}(K_i, \mathsf{XAuth}(K_1, \ldots, K_L)) \neq 1],$$

is negligible, where $K_1, \ldots, K_L \leftarrow \mathsf{XGen}(1^\kappa)$ in the probability.

Security against impersonation and substitution attacks. *$\mathsf{Adv}^{\mathsf{imp}}_{\mathsf{XAC}}(\kappa)$ and $\mathsf{Adv}^{\mathsf{sub}}_{\mathsf{XAC}}(\kappa)$ as defined below are both negligible:*

$$\mathsf{Adv}^{\mathsf{imp}}_{\mathsf{XAC}}(\kappa) := \max_{T'} \Pr[\mathsf{XVer}(K, T') = 1 | K \leftarrow \mathsf{XGen}(1^\kappa)],$$

where the max *is over all $T' \in \mathcal{XT}$, and*

$$\mathsf{Adv}^{\mathsf{sub}}_{\mathsf{XAC}}(\kappa) := \max_{i, K_{\neq i}, F} \Pr\left[\begin{array}{c} T' \neq T \wedge \\ \mathsf{XVer}(K_i, T') = 1 \end{array} \middle| \begin{array}{c} K_i \leftarrow \mathsf{XGen}(1^\kappa), \\ T = \mathsf{XAuth}(K_1, \ldots, K_L), \\ T' \leftarrow F(T) \end{array} \right]$$

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

Definition 4 (Strengthened XAC.) *An L-cross-authentication code XAC is a* strengthened *XAC, if it enjoys the following additional properties.*

Strongness [20]: *There exists another PPT public algorithm ReSamp, which takes as input i, $(K_j)_{j \neq i}$ and T, with $K_1, \ldots, K_L \leftarrow \mathsf{XGen}(1^\kappa)$ and $T \leftarrow \mathsf{XAuth}(K_1, \ldots, K_L)$, outputs $\hat{K}_i$ (i.e., $\hat{K}_i \leftarrow \mathsf{ReSamp}(K_{\neq i}, T)$),*

[5] In Fehr et al.'s original definition [13], algorithm XVer includes an additional input parameter: index i. Let $K_1, \ldots, K_L \leftarrow \mathsf{XGen}(1^\kappa)$ and $T \leftarrow \mathsf{XAuth}(K_1, \ldots, K_L)$. Since $\mathsf{XVer}(K_i, i, T) = \mathsf{XVer}(K_i, j, T)$ in their efficient construction, we only take a key and a tag as input of algorithm XVer for notational convenience.

such that $\hat{K}_i$ *is statistically indistinguishable with* K_i*, i.e., the statistical distance*

$$Dist(\kappa) := \frac{1}{2} \cdot \sum_{K \in \mathcal{XK}} \left| \Pr[\hat{K}_i = K \,|(K_{\neq i}, T)] - \Pr[K_i = K \,|(K_{\neq i}, T)] \right|$$

is negligible.

Semi-Uniqueness: *The key space* $\mathcal{XK} = \mathcal{K}_a \times \mathcal{K}_b$*. Given an authentication tag* T *and* $K_a \in \mathcal{K}_a$*, there exists at most* one $K_b \in \mathcal{K}_b$ *such that* $\mathsf{XVer}((K_a, K_b), T) = 1$.

Next, we review the efficient construction of L-cross-authentication code secure against impersonation and substitution attacks proposed by Fehr et al. [13], and show that it is *strong* and *semi-unique* as well, i.e. it is a *strengthened* XAC.

- $\mathcal{XK} = \mathcal{K}_a \times \mathcal{K}_b = \mathbb{F}_q^2$ and $\mathcal{XT} = \mathbb{F}_q^L \cup \{\perp\}$.
- XGen outputs (a, b), which is chosen from $\mathbb{F}_q^2$ uniformly at random.
- $T \leftarrow \mathsf{XAuth}((a_1, b_1), \ldots, (a_L, b_L))$. Let $\mathbf{A} \in \mathbb{F}_q^{L \times L}$ be a matrix with its i-th row $(1, a_i, a_i^2, \ldots, a_i^{L-1})$ for $i \in [L]$. Let $b_1, \ldots, b_L \in \mathbb{F}_q^L$ constitute the column vector $\mathbf{B}$. If $\mathbf{A}T = \mathbf{B}$ has no solution or more than one solution, set $T = \perp$. Otherwise $\mathbf{A}$ is a Vandermonde matrix, and the tag $T = (T_0, \ldots, T_{L-1})$ can be computed efficiently by solving the linear equation system $\mathbf{A}T = \mathbf{B}$.
- Define $poly_T(x) = T_0 + T_1 x + \cdots + T_{L-1} x^{L-1} \in \mathbb{F}_q[x]$ with $T = (T_0, \ldots, T_{L-1})$. $\mathsf{XVer}((a, b), T)$ outputs 1 if and only if $T \neq \perp$ and $poly_T(a) = b$.
- $(a, b) \leftarrow \mathsf{ReSamp}((a_j, b_j)_{j \neq i}, T)$. Choose $a \leftarrow \mathbb{F}_q$ such that $a \neq a_j$ $(1 \leq j \leq \ell, j \neq i)$ and compute $b = poly_T(a)$. Conditioned on $T = \mathsf{XAuth}((a_1, b_1), \ldots, (a_L, b_L))$ $(T \neq \perp)$ and $(a_j, b_j)_{j \neq i}$, both of (a, b) and (a_i, b_i) are uniformly distributed over the same support.
- Fixing $a \in \mathbb{F}_q$ results in a unique $b = poly_T(a)$ such that $\mathsf{XVer}((a, b), T) = 1$, if $T \neq \perp$.

5 Proposed SIM-SO-CCA Secure IBE Scheme

Let $(\mathsf{Setup}_{ex}, \mathsf{KeyGen}_{ex}, \mathsf{Encrypt}_{ex}, \mathsf{Decrypt}_{ex})$ be an extractable 1SPO-IBE scheme with identity space $\mathcal{ID}$, ciphertext space $\mathcal{C}$ and session key space $\mathcal{K} = \mathcal{K}_a \times \mathcal{K}_b$, and $(\mathsf{XGen}, \mathsf{XAuth}, \mathsf{XVer})$ be a strengthened $\ell + 1$-cross-authentication code XAC with key space $\mathcal{XK} = \mathcal{K} = \mathcal{K}_a \times \mathcal{K}_b$ and tag space $\mathcal{XT}$. We require that key space $\mathcal{K}$ is also an *efficiently samplable and*

explainable domain[6] associated with algorithms Sample' and Sample'^{-1}. Our cryptosystem has message space $\{0,1\}^\ell$.

Our scheme consists of the following algorithms:

$\mathsf{Setup}(1^\kappa)$: The setup algorithm first chooses $K_a \leftarrow \mathcal{K}_a$ and a collision-resistant hash function $\mathsf{H} : \mathcal{ID} \times \overbrace{\mathcal{C} \times \cdots \times \mathcal{C}}^{\ell} \rightarrow \mathcal{K}_b$, and calls Setup_{ex} to obtain $(\mathsf{PK}_{ex}, \mathsf{MSK}_{ex}) \leftarrow \mathsf{Setup}_{ex}(1^\kappa)$. It sets the public parameter $\mathsf{PK} = (\mathsf{PK}_{ex}, \mathsf{H}, K_a)$ and the master secret key $\mathsf{MSK} = \mathsf{MSK}_{ex}$.

$\mathsf{KeyGen}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID} \in \mathcal{ID})$: The key generation algorithm takes as input the public parameter $\mathsf{PK} = (\mathsf{PK}_{ex}, \mathsf{H}, K_a)$, the master secret key $\mathsf{MSK} = \mathsf{MSK}_{ex}$ and an identity ID. It calls KeyGen_{ex} to get $\mathsf{SK}_{\mathsf{ID}} \leftarrow \mathsf{KeyGen}_{ex}(\mathsf{PK}_{ex}, \mathsf{MSK}_{ex}, \mathsf{ID})$, and outputs the private key $\mathsf{SK}_{\mathsf{ID}}$.

$\mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID} \in \mathcal{ID}, M)$: The encryption algorithm takes as input the public parameter $\mathsf{PK} = (\mathsf{PK}_{ex}, \mathsf{H}, K_a)$, an identity ID and a message $M = m_1 \| \cdots \| m_\ell \in \{0,1\}^\ell$. For $i \in [\ell]$, it computes

$$\begin{cases} (C_i, K_i) \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{ID}, 1) & \text{if } \ m_i = 1 \\ C_i \leftarrow \mathsf{Encrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{ID}, 0),\ K_i \leftarrow \mathsf{Sample}'(\mathcal{K}; R_i^K) & \text{if } \ m_i = 0 \end{cases},$$

where $R_i^K \leftarrow \mathcal{R}_{\mathsf{Sample}'}$. Then, it sets $K_{\ell+1} = (K_a, K_b)$ where $K_b = \mathsf{H}(\mathsf{ID}, C_1, \ldots, C_\ell)$, and computes the tag $T = \mathsf{XAuth}(K_1, \ldots, K_{\ell+1})$. Finally, it outputs the ciphertext $CT = (C_1, \ldots, C_\ell, T)$.

$\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_{\mathsf{ID}}, CT)$: The decryption algorithm takes as input the public parameter $\mathsf{PK} = (\mathsf{PK}_{ex}, \mathsf{H}, K_a)$, a private key $\mathsf{SK}_{\mathsf{ID}}$ for identity ID and a ciphertext $CT = (C_1, \ldots, C_\ell, T)$. This algorithm first computes $K'_b = \mathsf{H}(\mathsf{ID}, C_1, \ldots, C_\ell)$ and checks whether $\mathsf{XVer}(K'_{\ell+1}, T) = 1$ with $K'_{\ell+1} = (K_a, K'_b)$. If not, it outputs $M'' = \overbrace{0 \cdots 0}^{\ell}$. Otherwise, for $i \in [\ell]$, it computes $(m'_i, K'_i) \leftarrow \mathsf{Decrypt}_{ex}(\mathsf{PK}_{ex}, \mathsf{SK}_{\mathsf{ID}}, C_i)$ and sets

$$m''_i = \begin{cases} \mathsf{XVer}(K'_i, T) & \text{if } \ m'_i = 1 \\ 0 & \text{if } \ m'_i = 0 \end{cases}.$$

Then, it outputs the message $M'' = m''_1 \| \cdots \| m''_\ell$.

[6] As mentioned in [13], the *efficiently samplable and explainable* key space $\mathcal{K}$ can be assumed without loss of generality, because $\mathcal{K}$ can always be efficiently mapped into $\mathcal{K}' = \{0,1\}^l$ by means of a suitable (almost) balanced function, such that uniform distribution in $\mathcal{K}$ induces (almost) uniform distribution in $\mathcal{K}'$, and where l is linear in $\log(|\mathcal{K}|)$.

Correctness. If $m_i = 1$, then $(m'_i, K'_i) = (m_i, K_i)$ by correctness of extractable 1SPO-IBE scheme, so $\mathsf{XVer}(K'_i, T) = 1$ (hence $m''_i = 1$) except with probability $\mathsf{fail}_{\mathsf{XAC}}$ by correctness of XAC. On the other hand, if $m_i = 0$, the ϵ-completeness of the extractable 1SPO-IBE guarantees $m'_i = 0$ (hence $m''_i = 0$) with probability at least $1 - \epsilon$. Consequently, for any $CT \leftarrow \mathsf{Encrypt}(\mathsf{PK}, \mathsf{ID}, M)$, we have $\mathsf{Decrypt}(\mathsf{PK}, \mathsf{SK}_{\mathsf{ID}}, CT) = M$ except with probability at most $\ell \cdot \max\{\mathsf{fail}_{\mathsf{XAC}}, \epsilon\}$.

Theorem 1 *If the extractable 1SPO-IBE scheme is IND-ID-CCA secure, the hash function H is collision-resistant and the strengthened $\ell+1$-cross-authentication code XAC is secure against substitution attacks, then our proposed IBE scheme is SIM-SO-CCA secure.*

Proof. See the full version of this paper.

6 Proposed IND-ID-CCA Secure Extractable 1SPO-IBE Scheme

In this section, we propose a concrete construction of extractable 1SPO-IBE from the anonymous IBE [11] in a composite order bilinear group. (In the full version of this paper, we show how to construct an extractable 1SPO-IBE from Boyen-Waters anonymous HIBE [8], which is based on a prime order bilinear group.) The design principle has already been described in the introduction.

The proposed scheme consists of the following algorithms:

$\mathsf{Setup}_{ex}(1^\kappa)$: Run an N-order group generator $\mathcal{G}(\kappa)$ to obtain a group description $(p_1, p_2, p_3, p_4, \mathbb{G}, \mathbb{G}_T, e)$, where $\mathbb{G} = \mathbb{G}_{p_1} \times \mathbb{G}_{p_2} \times \mathbb{G}_{p_3} \times \mathbb{G}_{p_4}$, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerate bilinear map, $\mathbb{G}$ and $\mathbb{G}_T$ are cyclic groups of order $N = p_1p_2p_3p_4$. Next choose $g, u, v, h \leftarrow \mathbb{G}_{p_1}$, $g_3 \leftarrow \mathbb{G}_{p_3}$, $g_4, W_4 \leftarrow \mathbb{G}_{p_4}$ and $\alpha, \beta \leftarrow \mathbb{Z}_N$. Then choose a collision-resistant hash function $\mathsf{H} : \mathbb{Z}_N \times \mathbb{G} \to \mathbb{Z}_N$, and a key derivation function $\mathsf{KDF} : \mathbb{G}_T \to \mathbb{Z}_N$. The public parameter is $\mathsf{PK} = ((\mathbb{G}, \mathbb{G}_T, e, N),\ u, v, h, W_{14} = gW_4,\ g_4,\ e(g,g)^\alpha,\ e(g,g)^\beta,\ \mathsf{H}, \mathsf{KDF})$. The master secret key is $\mathsf{MSK} = (g, g_3, \alpha, \beta)$. We require the group $\mathbb{G}$ be an *efficiently samplable and explainable domain* associated with algorithms Sample and Sample^{-1}. Details on how to instantiate such groups are given in [3].

$\mathsf{KeyGen}_{ex}(\mathsf{PK}, \mathsf{MSK}, \mathsf{ID} \in \mathbb{Z}_N)$: Choose $r, \bar{r} \leftarrow \mathbb{Z}_N$ and $R_3, R'_3, R''_3, \bar{R}_3, \bar{R}'_3, \bar{R}''_3 \leftarrow \mathbb{G}_{p_3}$ (this is done by raising g_3 to a random power). Output the private key $\mathsf{SK}_{\mathsf{ID}} = (\mathsf{ID}, D_0, D_1, D_2, \bar{D}_0, \bar{D}_1, \bar{D}_2)$, where $D_0 = g^\alpha (u^{\mathsf{ID}} h)^r R_3$, $D_1 = v^r R'_3$, $D_2 = g^r R''_3$, $\bar{D}_0 = g^\beta (u^{\mathsf{ID}} h)^{\bar{r}} \bar{R}_3$, $\bar{D}_1 = v^{\bar{r}} \bar{R}'_3$, $\bar{D}_2 = g^{\bar{r}} \bar{R}''_3$.

$\mathsf{Encrypt}_{ex}(\mathsf{PK}, \mathsf{ID} \in \mathbb{Z}_N, m \in \{0,1\})$: If $m = 1$, choose $s, t_4 \leftarrow \mathbb{Z}_N$ and compute $c_0 = W_{14}^s g_4^{t_4}$, $c_1 = (u^{\mathsf{ID}} v^{\mathsf{ID}'} h)^s g_4^{\mathsf{KDF}(e(g,g)^{\alpha s})}$, $K = e(g,g)^{\beta s}$, where $\mathsf{ID}' = \mathsf{H}(\mathsf{ID}, c_0)$, then output the ciphertext and the session key $(C, K) = ((c_0, c_1), K)$; otherwise (i.e., $m = 0$), choose $c_0, c_1 \leftarrow \mathsf{Sample}(\mathbb{G})$, and output the ciphertext $C = (c_0, c_1)$.

$\mathsf{Decrypt}_{ex}(\mathsf{PK}, \mathsf{SK}_{\mathsf{ID}} = (\mathsf{ID}, D_0, D_1, D_2, \bar{D}_0, \bar{D}_1, \bar{D}_2), C = (c_0, c_1))$: Compute $\mathsf{ID}' = \mathsf{H}(\mathsf{ID}, c_0)$ and $X = e(D_0 D_1^{\mathsf{ID}'}, c_0)/e(D_2, c_1)$. (One can view $(D_0 D_1^{\mathsf{ID}'}, D_2)$ as a private key associated to the 2-level identity $\widetilde{\mathsf{ID}} = (\mathsf{ID}, \mathsf{ID}')$.) Then, check whether $e(c_1/g_4^{\mathsf{KDF}(X)}, W_{14}) = e(c_0,\ u^{\mathsf{ID}} v^{\mathsf{ID}'} h)$. If not, set $m = 0$ and choose a session key $K \leftarrow \mathbb{G}_T$. Otherwise, set $m = 1$ and compute $K = e(\bar{D}_0 \bar{D}_1^{\mathsf{ID}'}, c_0)/e(\bar{D}_2, c_1)$. Output (m, K).

Correctness. Note that, if $C = (c_0, c_1)$ is an encryption of 1 under identity ID, then

$$\begin{aligned}
X &= e(D_0 D_1^{\mathsf{ID}'}, c_0)/e(D_2, c_1) \\
&= e(g^{\alpha}(u^{\mathsf{ID}} v^{\mathsf{ID}'} h)^r,\ g^s)/e(g^r,\ (u^{\mathsf{ID}} v^{\mathsf{ID}'} h)^s) = e(g,g)^{\alpha s}, \\
e(c_1/g_4^{\mathsf{KDF}(X)}, W_{14}) &= e((u^{\mathsf{ID}} v^{\mathsf{ID}'} h)^s, W_{14}) \\
&= e(u^{\mathsf{ID}} v^{\mathsf{ID}'} h, W_{14}^s) = e(c_0,\ u^{\mathsf{ID}} v^{\mathsf{ID}'} h), \\
K &= e(\bar{D}_0 \bar{D}_1^{\mathsf{ID}'}, c_0)/e(\bar{D}_2, c_1) \\
&= e(g^{\beta}(u^{\mathsf{ID}} v^{\mathsf{ID}'} h)^{\bar{r}},\ g^s)/e(g^{\bar{r}},\ (u^{\mathsf{ID}} v^{\mathsf{ID}'} h)^s) = e(g,g)^{\beta s},
\end{aligned}$$

so decryption always succeeds. On the other hand, if $C = (c_0, c_1)$ is an encryption of 0 under identity ID, then $c_0, c_1 \in \mathbb{G}$ are chosen uniformly at random, thus $\mathsf{Pr}[e(c_1/g_4^{\mathsf{KDF}(X)}, W_{14}) = e(c_0, u^{\mathsf{ID}} v^{\mathsf{ID}'} h)] \leq \frac{1}{2^{2\kappa}}$ where κ is the security parameter. So the completeness error is $\frac{1}{2^{2\kappa}}$.

One-Sided Public Openability (1SPO). If $C = (c_0, c_1)$ is an encryption of 0 under identity ID, then c_0 and c_1 are both randomly distributed in $\mathbb{G}$. Since the group $\mathbb{G}$ is an efficiently samplable and explainable domain associated with Sample and Sample^{-1}, $\mathsf{POpen}(\mathsf{PK}, \mathsf{ID}, C = (c_0, c_1))$ can employ Sample^{-1} to open (c_0, c_1). More precisely, $(R_0, R_1) \leftarrow \mathsf{POpen}(\mathsf{PK}, \mathsf{ID}, (c_0, c_1))$, where $R_0 \leftarrow \mathsf{Sample}^{-1}(\mathbb{G}, c_0)$ and $R_1 \leftarrow \mathsf{Sample}^{-1}(\mathbb{G}, c_1)$.

Security. We now state the security theorem of our proposed extractable IBE scheme.

Theorem 2 *The above extractable 1SPO-IBE scheme is IND-ID-CCA secure.*

Proof. See the full version of this paper.

Acknowledgement

We are grateful to the anonymous reviewers for their helpful comments. The work of Junzuo Lai was supported by the National Natural Science Foundation of China (Nos. 61300226, 61272534, 61272453), the Research Fund for the Doctoral Program of Higher Education of China (No. 20134401120017), the Guangdong Provincial Natural Science Foundation (No. S2013040014826), and the Fundamental Research Funds for the Central Universities. The work of Shengli Liu was supported by the National Natural Science Foundation of China (No. 61170229, 61373153), the Specialized Research Fund for the Doctoral Program of Higher Education (No. 20110073110016), and the Scientic innovation projects of Shanghai Education Committee (No. 12ZZ021). The work of Jian Weng was supported by the National Science Foundation of China (Nos. 61272413, 61373158, 61133014, 61272415), the Fok Ying Tung Education Foundation (No. 131066), the Program for New Century Excellent Talents in University (No. NCET-12-0680), and the Research Fund for the Doctoral Program of Higher Education of China (No. 20134401110011). The work of Yunlei Zhao was supported by the National Basic Research Program of China (973 Program) (No. 2014CB340600), the National Natural Science Foundation of China (Nos. 61070248, 61332019, 61272012), and the Innovation Project of Shanghai Municipal Education Commission (No.12ZZ013).

References

1. M. Bellare, R. Dowsley, B. Waters, and S. Yilek. Standard security does not imply security against selective-opening. In *EUROCRYPT*, pages 645–662, 2012.
2. M. Bellare, D. Hofheinz, and S. Yilek. Possibility and impossibility results for encryption and commitment secure under selective opening. In *EUROCRYPT*, pages 1–35, 2009.
3. M. Bellare, B. Waters, and S. Yilek. Identity-based encryption secure against selective opening attack. In *TCC*, pages 235–252, 2011.
4. M. Bellare and S. Yilek. Encryption schemes secure under selective opening attack. *IACR Cryptology ePrint Archive*, 2009:101, 2009.
5. F. Böhl, D. Hofheinz, and D. Kraschewski. On definitions of selective opening security. In *Public Key Cryptography*, pages 522–539, 2012.
6. A. Boldyreva, S. Fehr, and A. O'Neill. On notions of security for deterministic encryption, and efficient constructions without random oracles. In *CRYPTO*, pages 335–359, 2008.
7. D. Boneh, R. Canetti, S. Halevi, and J. Katz. Chosen-ciphertext security from identity-based encryption. *SIAM J. Comput.*, 36(5):1301–1328, 2007.
8. X. Boyen and B. Waters. Anonymous hierarchical identity-based encryption (without random oracles). In *CRYPTO*, pages 290–307, 2006.

9. R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky. Deniable encryption. In *CRYPTO*, pages 90–104, 1997.
10. R. Canetti, U. Feige, O. Goldreich, and M. Naor. Adaptively secure multi-party computation. In *STOC*, pages 639–648, 1996.
11. A. D. Caro, V. Iovino, and G. Persiano. Fully secure anonymous HIBE and secret-key anonymous IBE with short ciphertexts. In *Pairing*, pages 347–366, 2010.
12. R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *IACR Cryptology ePrint Archive*, 2001:108, 2001.
13. S. Fehr, D. Hofheinz, E. Kiltz, and H. Wee. Encryption schemes secure against chosen-ciphertext selective opening attacks. In *EUROCRYPT*, pages 381–402, 2010.
14. D. M. Freeman, O. Goldreich, E. Kiltz, A. Rosen, and G. Segev. More constructions of lossy and correlation-secure trapdoor functions. In *Public Key Cryptography*, pages 279–295, 2010.
15. B. Hemenway, B. Libert, R. Ostrovsky, and D. Vergnaud. Lossy encryption: Constructions from general assumptions and efficient selective opening chosen ciphertext security. In *ASIACRYPT*, pages 70–88, 2011.
16. B. Hemenway and R. Ostrovsky. Lossy trapdoor functions from smooth homomorphic hash proof systems. *Electronic Colloquium on Computational Complexity (ECCC)*, 16:127, 2009.
17. B. Hemenway and R. Ostrovsky. Homomorphic encryption over cyclic groups implies chosen-ciphertext security. *IACR Cryptology ePrint Archive*, 2010:99, 2010.
18. D. Hofheinz. Possibility and impossibility results for selective decommitments. *IACR Cryptology ePrint Archive*, 2008:168, 2008.
19. D. Hofheinz. All-but-many lossy trapdoor functions. In *EUROCRYPT*, pages 209–227, 2012.
20. Z. Huang, S. Liu, and B. Qin. Sender equivocable encryption schemes secure against chosen-ciphertext attacks revisited. *IACR Cryptology ePrint Archive*, 2012:473, 2012.
21. Z. Huang, S. Liu, and B. Qin. Sender-equivocable encryption schemes secure against chosen-ciphertext attacks revisited. In *Public Key Cryptography*, pages 369–385, 2013.
22. E. Kiltz, P. Mohassel, and A. O'Neill. Adaptive trapdoor functions and chosen-ciphertext security. In *EUROCRYPT*, pages 673–692, 2010.
23. A. B. Lewko and B. Waters. New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In *TCC*, pages 455–479, 2010.
24. S. Myers and A. Shelat. Bit encryption is complete. In *FOCS*, pages 607–616, 2009.
25. C. Peikert and B. Waters. Lossy trapdoor functions and their applications. In *STOC*, pages 187–196, 2008.
26. A. Rosen and G. Segev. Chosen-ciphertext security via correlated products. In *TCC*, pages 419–436, 2009.
27. B. Waters. Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions. In *CRYPTO*, pages 619–636, 2009.