Public-Key Encryption with Simulation-Based Sender Selective-Opening Security

Dali Zhu[1,2], Renjun Zhang[1,2], and Dingding Jia[2,3,4](✉)

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
{zhudali,zhangrenjun}@iie.ac.cn

[2] School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China

[3] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
jiadingding@iie.ac.cn

[4] Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing, China

Abstract. We study public key encryptions (PKE) of simulation-based security against sender selective-opening (SIM-SSO) attacks, where the attacker can corrupt a subset of senders, learning the plaintexts together with the corresponding randomness. Concretely:

- We present a generic construction of SIM-SSO security under chosen plaintext attacks (SIM-SSO-CPA) by combining a lossy encryption given by Hemenway *et al.* (Asiacrypt 2011), along with a tailored compression algorithm. Our construction gives a simple and modular security analysis. We then present an instantiation based on the Matrix Diffie-Hellman Assumption.
- We show that the PKE construction from Boneh-Gentry-Hamburg scheme (FOCS 2007), and construction from a (public-key based) variant of Cocks' scheme (Peikert, Vaikuntanathan and Waters, Crypto 2008) are SIM-SSO-CPA secure. Even if these results may seem natural, not surprising at all, their SIM-SSO-CPA security have not been explicitly reported so far.
- We further show that two PKE constructions from homomorphic trapdoor commitments (Groth, Ostrovsky and Sahai, Crypto 2006, Eurocrypt 2006) are SIM-SSO-CPA secure.

Keywords: Sender Selective-Opening Security · Lossy encryption · Hash proof system

1 Introduction

Sender selective-opening (SSO) attacks consider scenarios that adversary may corrupt a part of senders. More formally, suppose a receiver receives a n tuple of

This work is Supported by the "Strategic Priority Program" of Chinese Academy of Sciences, Grant No. Y2W0012306, and the National Nature Science Foundation of China (No.61502484).

T. Okamoto et al. (Eds.): ProvSec 2017, LNCS 10592, pp. 361–380, 2017.
https://doi.org/10.1007/978-3-319-68637-0_22

ciphertexts $\boldsymbol{c} = (c[1], \ldots, c[n])$, each ciphertext $c[i] = \mathrm{Enc}_{pk}(m_i; r_i)$ is created by sender i with a fresh randomness r_i under pk. Now, given $\boldsymbol{c}$, the adversary can adaptively chooses a subset $\mathcal{I} \subseteq \{1, \ldots, n\}$ of ciphertexts to open, learning the messages $\{m_i\}_{i \in \mathcal{I}}$ and corresponding randomness $\{r_i\}_{i \in \mathcal{I}}$. The security requires privacy of the unopened messages preserved.

The study of sender-selective opening in PKE scenarios was initiated by Bellare, Hofheinz and Yilek [2]. They formulated the notions in two styles: indistinguishability-based selective-opening (IND-SSO) security and simulation-based selective-opening (SIM-SSO) security. Compared with the standard IND-CPA/CCA security, IND/SIM-SSO security is more complicated, for the reason that the opening of the randomness allows the adversary to check the correspondence between ciphertext and message. Relations among IND-SSO, SIM-SSO and standard security attract much attention such as in [1,3,14,20,24,25].

IND-SSO security is restricted to efficiently re-samplable plaintext distributions. SIM-SSO security does not suffer from such restrictions, but is the preferable notion of SSO security. In a nutshell, SIM-SSO security requires that the output of any adversary can be simulated by a simulator that sees only the opened messages. Unfortunately, SIM-SSO security is nonessential hard to achieve [1], because for many natural encryption schemes, there does not exist such simulator that satisfies the definition given in [2,11].

Known constructions of SIM-SSO secure encryption schemes either from lossy encryption [2,15,21–23] or from deniable encryption (as well as non-committing encryption) [7,13,30]. Lossy encryption has been shown to be a very useful tool in achieving SIM-SSO security. In [2], Bellare *et al.* proved that lossy encryption with efficient opening implies SIM-SSO-CPA security. However, it seems that the property of efficient openability is limited to the decisional composite residuosity (DCR) settings [32]. Hemenway *et al.* [21] proposed a general construction of lossy encryption from hash proof system, but it is not clear whether it supports efficient opening or not. This line of research continued in [35], Wee presented a new framework of Dual-mode cryptosystems via smooth projective hashing, but it also ignores the efficient opening property. The results in [21,35] are inspired by the work in [29]. Recently, Hofheinz *et al.* [23] proposed a SIM-SSO-CPA secure PKE scheme in the discrete-log setting, and further showed that lossy encryption scheme with efficient *weak* opening implies SIM-SSO-CPA security. In their construction, the key component is a hash function that is used to compress the space of ciphertexts.

Related Work. Several IND-SO-CCA secure schemes have been constructed by using lossy trapdoor functions [34], All-But-N lossy trapdoor functions [21], and All-But-Many lossy trapdoor functions [22]. Furthermore, known constructions of SIM-SSO-CCA secure schemes follow dedicated approaches [13,22,26,30]. Heuer *et al.* proved that the practical schemes RSA-OAEP and DHIES are SIM-SSO-CCA secure in the random oracle model. Selective opening security under receiver corruption were considered in [20,27,28].

1.1 Our Contribution

In this paper, firstly we present a generic construction for building SIM-SSO-CPA secure scheme from hash proof system, and then give an instantiation based on the Matrix Diffie-Hellman Assumption. Our construction is a combination of lossy encryption in [21] (note that the related schemes appeared in [29,35], namely, the two-message oblivious transfer protocol in [29], and the Dual-mode encryption scheme in [35]), and a tailored compression algorithm that compresses the space of ciphertexts. Then we prove that the PKE construction from Boneh-Gentry-Hamburg (BGH) scheme in [5], and the PKE construction from a (public-key based) variant of Cocks' scheme (short: Cocks' scheme) in [33] are SIM-SSO-CPA secure. We further prove that two PKE constructions from homomorphic trapdoor commitment in [16–18] are SIM-SSO-CPA secure. In the following there are some technique overviews.

The generic lossy encryption scheme in [21] is IND-SSO-CPA secure. To modify it to be SIM-SSO-CPA secure, one should seek an efficient algorithm Opener that will find correctly distributed random coins to open a lossy ciphertext to an arbitrary plaintext. But the property of efficient openability suffers from specific algebraic structure, but the lossy encryption in [21] does not have this structure (Note that in [21] secret keys play the role of random coins). Inspired by the ideas in [10,19,23], we observe that if the space of ciphertexts shrinks to a smaller one, then the number of random coins will increase. Then Opener can randomly guesses them one after another in a confined space, and checks whether these random coins meet the requirements. To do so, we tailor a compression algorithm that compresses the ciphertexts space to a logarithmic space of size L (L is at most $O(\log l)$ where l is the security parameter). We also require that the output of tailored compression algorithm statistically indistinguishable from random bits over $\{0,1\}^L$. These approaches assure that Opener algorithm runs in expected polynomial time, but the accurate running time depends on concrete settings. On the downside, our approach suffers from a small message space.

Besides, we prove that two PKE constructions from BGH scheme and Cocks' scheme are SIM-SSO-CPA secure. Both schemes have natural lossiness properties, and these properties have contained implicitly in the security proof. However, it is not our purpose to make them explicit. We concern about whether BGH scheme and Cocks' scheme support efficient opening or not. Since two schemes are based on factoring-related assumptions, with the knowledge of factorization of N such that $N = pq$, it is true that the efficient opening algorithms exists. Hence, we can convert BGH scheme and Cocks' scheme to lossy encryption with efficient opening (and thus SIM-SSO security) by setting p or q as the lossy secret key.

In [18], Groth *et al.* concluded that "parameter-switching" methodology [16, 17] in encryptions keys leads to lossy encryption. In fact, their (non-interactive) homomorphic trapdoor commitments can be converted into lossy encryption schemes. We show that the converted schemes support efficient weak opening. That is, when Opener opens a lossy ciphertext to an arbitrary plaintext, it needs an additional random coins.

One may notice that schemes in this paper can only achieve SIM-SSO-CPA security. An interesting open problem is to extend them to the chosen-ciphertext (CCA) setting to obtain SIM-SSO-CCA secure schemes. Besides, both of BGH scheme and Cocks' scheme are based on quadratic residuosity assumption, and the lossy encryption with efficient opening can be seen as a general framework that unifies two specific constructions. But how to extend their security to SIM-SSO-CCA security is also an open interesting problem.

Organization. The rest of our paper is organized as follows: in Sect. 2 we present some basic notions as well as several tools that are used in our paper; in Sect. 3 we describe our generic construction of SIM-SSO-CPA secure scheme, and provide an instantiation based on Matrix Diffie-Hellman Assumption; in Sect. 4 we prove that two PKE constructions from BGH scheme and Cocks' scheme are SIM-SSO-CPA secure; in Sect. 5 we prove that two PKE constructions from homomorphic trapdoor commitments are SIM-SSO-CPA secure.

2 Preliminaries

2.1 Notation

In this paper, we use $\mathbb{N}$ to represent the set of natural numbers, and $\mathbb{Z}$ represents the set of integers. We also use PPT to denote probability polynomial time for short. Let $[k]$ be the set of $\{1, \ldots, k\}$, $x \leftarrow S$ is used to denote picking an element x uniformly at random from S when S is a finite set, and to denote sampling an element according to S when S is a distribution. The statistical distance of two probability ensembles $\mathcal{X}$, $\mathcal{Y}$ is defined as $SD(\mathcal{X}, \mathcal{Y}) := \frac{1}{2}\Sigma_x |\Pr[\mathcal{X} = x] - \Pr[\mathcal{Y} = x]|$. If $SD(\mathcal{X}, \mathcal{Y})$ is negligible, we say that $\mathcal{X}$ and $\mathcal{Y}$ are statistical indistinguishability (abbr. $X \approx_s Y$). The length of a string x is denoted by $|x|$.

2.2 Public Key Encryption

A public key encryption (PKE) scheme consists of the following three PPT algorithms:

Keygen**:** the key generation algorithm that takes as input a security parameter 1^λ, and outputs a public/secret key pair $(pk, sk) \leftarrow \text{Keygen}(1^\lambda)$.

Enc**:** the encryption algorithm that takes as input the public key pk, a plaintext $m \in \mathcal{M}$, and outputs a ciphertext $c \leftarrow \text{Enc}(pk, m)$.

Dec**:** the decryption algorithm that takes the secret key sk, a ciphertext c as input, and outputs either a message $m \leftarrow \text{Dec}(sk, c) \in \mathcal{M}$ or a special $\perp$ to indicate that c is not a valid ciphertext.

Correctness. The PKE scheme satisfies correctness if $\text{Dec}(sk, c) = m$ with all but negligible probability whenever pk, sk is produced by $\text{Keygen}(1^\lambda)$ and c is produced by $\text{Enc}(pk, m)$.

2.3 Sender Selective-Opening Security

Following [2,3,13], we recall the definition of simulation-based sender selective-opening security against chosen plaintext attacks (SIM-SSO-CPA).

Definition 1 (SIM-SSO-CPA Security). *A PKE scheme* $\mathrm{PKE} = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ *is SIM-SSO-CPA secure iff for every polynomially bound* $n = n(1^\lambda) > 0$*, every PPT relation* R*, and every stateful PPT adversary* $\mathcal{A}$*, there exists a stateful PPT simulator* S *such that*

$$\mathbf{Adv}^{\mathrm{sim-sso-cpa}}_{\mathrm{PKE},\mathcal{A},S,R}(1^\lambda) = |\Pr[\mathrm{Exp}^{\mathrm{real}}_{\mathrm{PKE},\mathcal{A},R}(1^\lambda) = 1] - \Pr[\mathrm{Exp}^{\mathrm{ideal}}_{S,R}(1^\lambda) = 1]|$$

is negligible. The experiments $\mathrm{Exp}^{\mathrm{real}}_{\mathrm{PKE},\mathcal{A},R}$ *and* $\mathrm{Exp}^{\mathrm{ideal}}_{S,R}$ *are defined as follows (Fig. 1):*

```
Experiment. $\mathrm{Exp}^{\mathrm{real}}_{\mathrm{PKE},\mathcal{A}}(1^\lambda)$:
$(pk, sk) \leftarrow \mathrm{Gen}(1^\lambda)$
$\mathrm{dist} \leftarrow \mathcal{A}(pk)$
$(M_i)_{i\in[n]} \leftarrow \mathrm{dist}$
$(R_i)_{i\in[n]} \leftarrow (\mathcal{R}_{\mathrm{Enc}})_n$
$(C_i)_{i\in[n]} = \mathrm{Enc}(pk, M_i; R_i)_{i\in[n]}$
$I \leftarrow \mathcal{A}(select, (C_i)_{i\in[n]})$
$out_{\mathcal{A}} \leftarrow \mathcal{A}(output, (M_i, R_i)_{i\in I})$
return $R(\mathrm{dist}, (M_i)_{i\in[n]}, I, out_{\mathcal{A}})$
```

```
Experiment. $\mathrm{Exp}^{\mathrm{ideal}}_{S}(1^\lambda)$:
$\mathrm{dist} \leftarrow S(1^\lambda)$
$(M_i)_{i\in[n]} \leftarrow \mathrm{dist}$
$I \leftarrow S(select, (1^{|M_i|})_{i\in[n]})$
$out_S \leftarrow S(output, (M_i)_{i\in I})$
return $R(\mathrm{dist}, (M_i)_{i\in[n]}, I, out_S)$
```

Fig. 1. The REAL-SIM-SSO-CPA and IDEAL-SIM-SSO-CPA experiment

2.4 Sender Selective-Opening Security from Lossy Encryption

Lossy Encryption with Efficient Opening. In [2], Bellare *et al.* defined lossy encryption, and proved that any lossy encryption scheme with efficient opening (short: LPKE, thus ciphertexts can be efficiently opened to arbitrary messages) is SIM-SSO-CPA secure. A LPKE consists of four algorithms (Gen, LGen, Enc, Dec) such that:

$\mathrm{Gen}(1^\lambda)$**:** The key generation algorithm that takes as input the security parameter 1^λ, and outputs a key pair (pk, sk) where pk is a real public key.

$\mathrm{LGen}(1^\lambda)$**:** The lossy key generation algorithm that takes as input the security parameter 1^λ, and outputs a key pair (pk, sk) where pk is a lossy public key.

$\mathrm{Enc}(pk, m)$**:** The encryption algorithm that takes as input a public key pk and a message m, where pk is either generated by $\mathrm{Gen}(1^\lambda)$ or by $\mathrm{LGen}(1^\lambda)$, and outputs a ciphertext c.

$\mathrm{Dec}(sk, c)$**:** The decryption algorithm that takes as input a ciphertext c and a secret sk, outputs either a message m if $c \leftarrow \mathrm{Enc}(pk, m)$, or a special symbol $\perp$ to indicate that c is not a valid ciphertext.

LPKE should satisfy properties of correctness, indistinguishability, lossiness and efficient openability.

Correctness. For all $(pk, sk) \leftarrow \mathrm{Gen}(1^\lambda)$, $c \leftarrow \mathrm{Enc}(pk, m)$, it must be the case that $\mathrm{Dec}(sk, c) = m$.

Indistinguishability. The first outputs of $\mathrm{Gen}(1^\lambda)$ and $\mathrm{LGen}(1^\lambda)$ can not be distinguished for any PPT adversary.

Lossiness. For any $(pk, sk) \leftarrow \mathrm{LGen}(1^\lambda)$ and two distinct messages m_0, m_1, it holds that $\mathrm{Enc}(pk,\ m_0) \approx_s \mathrm{Enc}(pk, m_1)$. Thus, two distributions statistically close.

Efficient Openability. There exists an efficient algorithm Opener that, takes as input lossy keys sk and pk, message m, ciphertext $c \leftarrow \mathrm{Enc}(pk,\ m; r)$, outputs random coins r' such that $\mathrm{Enc}(pk, m; r') = c$.

Hofheinz, Jager and Rupp [23] defined lossy encryption with efficient *weak* opening (short: wLPKE) and proved that wLPKE is indeed SIM-SSO-CPA secure. The only difference between LPKE and wLPKE is that the Opener algorithm for wLPKE may receive an additional random coins that have been used to generate the ciphertext. More generally, the property of efficient weak openability is described as follows.

Efficient weak openability. There exists an efficient algorithm Opener that, takes as input lossy keys sk and pk, message m_0, the random coins r, ciphertext $c \leftarrow \mathrm{Enc}(pk, m_0; r)$, and a message m_1, outputs random coins r' such that $\mathrm{Enc}(pk, m_1; r') = c$.

3 SIM-SSO-CPA Secure PKE from Hash Proof System

In this section, we present a generic construction of SIM-SSO-CPA secure by combining a lossy encryption in [21](as well as the schemes in [29,35]), and a tailored compression algorithm that compresses the space of ciphertexts. We further give an instantiation based on the Matrix Diffie-Hellman Assumption. Before turning to the generic construction, we first recall the notions of hash proof system as introduced by Cramer and Shoup [9].

3.1 Hash Proof System

Smooth Projective Hashing. A smooth projective hash family consists of $(\Lambda, \mathcal{SK},\ \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$, where $\mathcal{X}, \mathcal{Y}, \mathcal{L}, \mathcal{W}, \mathcal{SK}, \mathcal{PK}$ are finite, non-empty sets, and $\mathcal{L} \subset \mathcal{X}$ is a language. Let $\Lambda : \mathcal{X} \to \mathcal{Y}$ be a collection of hash functions indexed by keys $sk \in \mathcal{SK}$ mapping from $\mathcal{X}$ to $\mathcal{Y}$. Also there exists an efficiently computable projection μ from $\mathcal{SK}$ to $\mathcal{PK}$. A hash family $\mathbf{H} = (\Lambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$ is projective if for all $sk \in \mathcal{SK}$, the action of Λ_{sk} on $\mathcal{L}$ is determined by $\mu(sk)$. A hash family $\mathbf{H} = (\Lambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{W},\ \mathcal{Y}, \mathcal{PK}, \mu)$ is smoothness if for randomly chosen $sk \in \mathcal{SK}$, given $\mu(sk)$ and $x \in \mathcal{X} \setminus \mathcal{L}$, $\Lambda_{sk}(x)$ is statistically close to uniform distributions over $\mathcal{Y}$.

We also require that for $sk \in \mathcal{SK}$, it can be efficiently sampled sk' such that $\mu(sk) = \mu(sk')$, which will be used not in the actual scheme but in the security proof. In fact, all known hash proof systems have this property.

Subset Membership Assumption. We will consider two related subset membership assumptions pertaining to the non-empty set $\mathcal{X}$. The first assumption states that the uniform distributions over $\mathcal{L}$ and $\mathcal{X}$ are computationally indistinguishable, even given the public parameter. The second assumption requires that the uniform distributions over $\mathcal{L}$ and $\mathcal{X} \setminus \mathcal{L}$ are computationally indistinguishable, even knowing the public parameter. The two assumptions are equivalent when $\mathcal{L}$ is sparse in $\mathcal{X}$, i.e., $|\mathcal{L}|/|\mathcal{X}| = \text{negl}(1^\lambda)$, since the distributions over $\mathcal{X}$ and $\mathcal{X} \setminus \mathcal{L}$ are then statistically indistinguishable.

Hash Proof System. Let $\mathbf{H} = (\Lambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$ be a projective hash family, and let $\Lambda[\mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{R}]$ be any instance of a subset membership assumption, where $\mathcal{W}$ is the set of witness, and $\mathcal{R} \subset \mathcal{X} \times \mathcal{W}$ is a binary relation such that $x \in \mathcal{L}$ iff there exists a w satisfying $(x, w) \in \mathcal{R}$. A hash proof system provides efficient algorithm to randomly choose $sk \in \mathcal{SK}$ and $x \in \mathcal{X}$, efficient algorithm to compute $\mu(sk)$, and efficient algorithm (Priv, Pub) to compute $\Lambda_{sk}(x)$ for $x \in \mathcal{L}$ with witness w:

$$\Lambda_{sk}(x) = \text{Priv}(sk, x) = \text{Pub}(\mu(sk), x, w)$$

3.2 Generic Construction

Tailored Compression Algorithm. The study of instance compression was initiated by Harnik and Naor [19]. Inspired by the ideas in [10,19,31], we tailor a compression algorithm for the hash proof system. Roughly speaking, the tailored compression algorithm Z can shrink $\Lambda_{sk}(x)$ to a smaller bit string, and the output of Z statistically indistinguishable from random bits. Note that our definition is the generalization of the universal hash function that compress elements to bits in [23].

Definition 2 (Tailored Compression Algorithm for HPS). *Let* $\boldsymbol{H} = (\Lambda, \mathcal{SK}, \mathcal{X}, \mathcal{L}, \mathcal{W}, \mathcal{Y}, \mathcal{PK}, \mu)$ *be a smooth projective hash proof system. A tailored compression algorithm for HPS is a PPT algorithm* Z *such that for large enough* l

- *For any* $\pi \in \mathcal{Y}$*, the length* L *of* $Z(\pi)$ *is at most* $O(\log l)$*.*
- Z *outputs bits that uniformly distributed over* $\{0, 1\}^L$*.*

Construction. Based on these building blocks, we can construct a generic lossy encryption with efficient weak opening with message space $\{0, 1\}^{O(\log l)}$ (For simplicity, we stipulate that the length of $Z(\pi)$ is $O(\log l)$. Thus, only small message spaces are allowed.) The SIM-SSO-CPA secure scheme is described as follows.

Injective key generation: Samples an $x \in \mathcal{L}$, together with a corresponding witness w. Sets $pk = x$, $sk = w$.

Lossy key generation: Samples an $x \in \mathcal{X}$. Sets $pk = x$, $sk = \perp$.

Encryption: To encrypt a message $m \in \{0,1\}^{O(\log l)}$, chooses $sk \leftarrow \mathcal{SK}$, and returns the ciphertext $c = (c_1, c_2)$ as:

$$c_1 = \mu(sk), c_2 = Z(\Lambda_{sk}(x)) \oplus m.$$

Decryption: Given a ciphertext (c_1, c_2) and secret key $sk = w$, the algorithm first computes $\Lambda_{sk}(x)$, then returns $m = Z(\Lambda_{sk}(x)) \oplus c_2$.

3.3 Security Proof

The following theorem will be used in the security proof of the generic construction. The writing style of the proof in the rest of our paper refers to [2,23,35].

Theorem 1 **([2,23]).** *The lossy encryption scheme with efficient opening (or efficient weak opening) is SIM-SSO-CPA secure.*

We prove that the construction in Sect. 3.2 satisfies the four properties of lossy encryption with efficient weak opening.

Theorem 2. *If* $\boldsymbol{H}$ *is a smooth projective HPS with the corresponding subset membership assumption hard, and the output of tailored compression algorithm* Z *statistically indistinguishable from uniform, then the generic construction yields a SIM-SSO-CPA secure scheme.*

Proof. **Correctness.** This is guaranteed by the projective property of the smooth projective hashing.

Indistinguishability. This follows immediately from the subset membership assumption.

Lossiness. In lossy mode, the lossy public key $x \leftarrow \mathcal{X}$, according to the smoothness property of HPS, $\Lambda_{sk}(x)$ is uniformly distributed over $\mathcal{Y}$ even given $\mu(sk)$ and x. Since the output of Z are statistically close to uniform, $Z(\Lambda_{sk}(x)) \oplus m$ will also be statistically close to uniform over $\{0,1\}^{O(\log l)}$ for any message m. Hence, lossiness follows readily.

Efficient weak openability. We note that in the generic setting, secret keys play the role of random coins. Consider the algorithm Opener, takes as input a lossy public key $x \leftarrow \mathcal{X}$, lossy secret key $sk \in \mathcal{SK}$, message $m' \in \{0,1\}^{O(\log l)}$, and ciphertext $c = (c_1, c_2) = (\mu(sk), Z(\Lambda_{sk}(x)) \oplus m)$ for some $m \in \{0,1\}^{O(\log l)}$, outputs sk' such that $\mu(sk') = c_1$ and $Z(\Lambda_{sk'}(x)) \oplus m' = c_2$. To do so, Opener samples sk' randomly and creates a set

$$\{sk' \in \mathcal{SK} : \mu(sk') = c_1 \wedge Z(\Lambda_{sk'}(x)) = m' \oplus c_2\}$$

We now analyze the behavior of the algorithm Opener. First, Opener can efficiently determine $\mu(sk') = c_1$. Second, Opener randomly guesses sk' one after another and check to see whether $Z(\Lambda_{sk'}(x)) = m' \oplus c_2$. As the output of Z is close to uniform, and the size of $Z(\Lambda_{sk'}(x))$ is at most $2^{O(\log l)}$, this will require about $O(l)$ steps. Also note that Opener algorithm runs in expected polynomial time, and has small probability of running for a long time.

3.4 Instantiation Based on Matrix Diffie-Hellman Assumption

Here, we describe one instantiation of the generic construction in Sect. 3.2. We then compare the efficency of this instantiation with the scheme in [23]. To instantiate our construction, we need to utilize a $\mathcal{D}_{l,k}$-Matrix Diffie-Hellman (short: $\mathcal{D}_{l,k}$-MDDH) Assumption, a $\mathcal{D}_{l,k}$-MDDH-based hash proof system in [12], and a universal hash function in [23] that maps group elements to bits.

Representing Elements in Groups. Let Gen be a PPT algorithm that takes as input 1^λ and outputs a description $\mathcal{G} = (\mathbb{G}, q, g)$, where $\mathbb{G}$ is a cyclic group with prime-order q, and g is the generator of $\mathbb{G}$. Following [12], we define $[a] = g^a \in \mathbb{G}$ as the implicit representation of a in $\mathbb{G}$. More generally, we also define such representations for matrix $\mathbf{A} = (a_{ij}) \in \mathbb{Z}_q^{n\times m}$ by:

$$[\mathbf{A}] = \begin{pmatrix} g^{a_{11}} & \dots & g^{a_{1m}} \\ \vdots & \ddots & \vdots \\ g^{a_{n1}} & \dots & g^{a_{nm}} \end{pmatrix} \in \mathbb{G}^{n\times m}$$

Matrix Diffie-Hellman Assumption. We recall the definition of the Matrix Diffie-Hellman Assumption as introduced in [12].

Definition 3 (Matrix Distribution). *Let $l, k \in \mathbb{N}$ such that $l > k$. The distribution $\mathcal{D}_{l,k}$ is called a matrix distribution if it outputs matrices in $\mathbb{Z}_q^{l\times k}$ of full rank k in probability polynomial time with all but negligible probability.*

Definition 4 ($\mathcal{D}_{l,k}$-Matrix Diffie-Hellman Assumption). *Let $\mathcal{D}_{l,k}$ be a matrix distribution. We say that the $\mathcal{D}_{l,k}$-Matrix Diffie-Hellman Assumption holds in $\mathbb{G}$ and relative to* Gen *if for all non-uniform polynomial time adversary $\mathcal{A}$, we have*

$$\mathbf{Adv}_{\mathcal{D}_{l,k},\mathrm{Gen}}(\mathcal{A}) = |\Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}], [\mathbf{A}\boldsymbol{w}]) = 1] - \Pr[\mathcal{A}(\mathcal{G}, [\mathbf{A}], [\boldsymbol{u}]) = 1]|$$

is negligible, where the probability is taken over the output $\mathcal{G} = (\mathbb{G}, q, g) \leftarrow \mathrm{Gen}(1^\lambda)$, $\mathbf{A} \leftarrow \mathcal{D}_{l,k}$, $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$, $\boldsymbol{u} \leftarrow \mathbb{Z}_q^l$ and the coin tosses of adversary $\mathcal{A}$.

Instantiation. For instantiation, we need a hash function $\mathrm{H} : G \to \{0, 1\}$ to replace the tailored compression algorithm Z. The hash function H should satisfies the following property in [23]: for randomly choose $a \in G$, $\mathrm{H}(a)$ is statistically indistinguishable from the uniform distribution over $\{0, 1\}$; if $\boldsymbol{a}$ is a vector of group elements from G, then $\mathrm{H}(\boldsymbol{a})$ is the component-wise application of the hash function, which outputs a bit vector of the same length as $\boldsymbol{a}$. The details of the instantiation are given below.

Setup: Runs $(\mathbb{G}, q, g) \leftarrow \mathrm{Gen}(1^\lambda)$ and picks $\mathbf{A} \leftarrow \mathcal{D}_{l,k}$. Define the language

$$\mathcal{L} = \{[\mathbf{A}\boldsymbol{w}] \in \mathbb{G}^l : \boldsymbol{w} \in \mathbb{Z}_q^k\} \subset \mathcal{X}$$

The value $\boldsymbol{w} \in \mathbb{Z}_q^k$ is a witness.

Injective key generation: Picks $\boldsymbol{w} \leftarrow \mathbb{Z}_q^k$, and computes $[\boldsymbol{x}] = [\mathbf{A}\boldsymbol{w}]$. Let $pk = [\boldsymbol{x}]$, $sk = \boldsymbol{w}$.

Lossy key generation: Picks $\boldsymbol{u} \leftarrow \mathbb{Z}_q^l$, and computes $[\boldsymbol{x}] = [\boldsymbol{u}]$. Let $pk = [\boldsymbol{x}]$, $sk = \mathbf{A}$.

Encryption: On inputs a message $m \in \{0, 1\}$, picks $\boldsymbol{k} \leftarrow \mathbb{Z}_q^l$, then computes $\boldsymbol{c}_1 = [\boldsymbol{k}^{\mathrm{T}}\mathbf{A}]$, $c_2 = \mathrm{H}([\boldsymbol{k}^{\mathrm{T}}\boldsymbol{x}]) \oplus m$, and outputs ciphertext $c = (\boldsymbol{c}_1, c_2)$.

Decryption: Given a ciphertext $c = (\boldsymbol{c}_1, c_2)$, and $sk = \boldsymbol{w}$, returns $m = \mathrm{H}([\boldsymbol{c}_1\boldsymbol{w}]) \oplus c_2$.

Correctness follows readily from the projective property of $\mathcal{D}_{l,k}$-MDDH-based hash proof system in [12]. We put the concrete security proof in Appendix A, and present the property of efficient weak openability in the following.

Consider the algorithm Opener that takes as input a lossy public key $pk = (\mathcal{G}, [\boldsymbol{x}])$ where $[\boldsymbol{x}] = [\boldsymbol{u}]$, a lossy secret key $\mathbf{A}$, the message m, random coins $\boldsymbol{k}^{\mathrm{T}} \in \mathbb{Z}_q^l$, and ciphertext $c = (\boldsymbol{c}_1, c_2) = ([\boldsymbol{k}^{\mathrm{T}}\mathbf{A}], \mathrm{H}([\boldsymbol{k}^{\mathrm{T}}\boldsymbol{x}]) \oplus m)$. The outputs of Opener is random coins $\boldsymbol{k'}^{\mathrm{T}}$ which is just a random vector in $\mathbb{Z}_q^l$. To this end, Opener samples $\boldsymbol{k'}^{\mathrm{T}} \in \mathbb{Z}_q^l$ randomly subject to $\boldsymbol{k'}^{\mathrm{T}}\mathbf{A} = \boldsymbol{k}^{\mathrm{T}}\mathbf{A}$ until $\mathrm{H}([\boldsymbol{k'}^{\mathrm{T}}\boldsymbol{x}]) \oplus m' = c_2$.

As Opener knows secret key $\mathbf{A}$, this increases the dimension of the random coins space, and introduce the redundancy into the first equation $\boldsymbol{k'}^{\mathrm{T}}\mathbf{A} = \boldsymbol{k}^{\mathrm{T}}\mathbf{A}$. Thus, there are many different $\boldsymbol{k'}$ satisfying $\boldsymbol{k'}^{\mathrm{T}}\mathbf{A} = \boldsymbol{k}^{\mathrm{T}}\mathbf{A}$. Opener can randomly guesses $\boldsymbol{k'}$ one after another and checks whether the second equation $\mathrm{H}([\boldsymbol{k'}^{\mathrm{T}}\boldsymbol{x}]) \oplus m' = c_2$ is true. On average, it takes 2 such samplings until $\boldsymbol{k'}$ is found.

We emphasize that the opening algorithm needs to receive $\boldsymbol{k}$ as an additional input, hence our instantiation meets the notion of lossy encryption with efficient weak opening.

Comparison. In [23], Hofheinz *et al.* compared their scheme to other SSO-secure PKE schemes such as [2,13,21]. We tabulate the efficiency of our scheme, and only compare it to HJR16 scheme [23] (which we refer to as HJR scheme) in Fig. 2. The HJR scheme is more efficient, and the plaintext space scales better (indeed, only small message space are allowed). But HJR scheme has a large public key size, and the encryption and decryption procedures are computationally expensive (because it needs to define a matrix constructor). In our scheme, the size of public key and secret key is linear, and the encryption and decryption procedures are efficient, but the price is a rather small plaintext space. We conclude that both our scheme and HJR scheme is a feasibility result, and further improvements would be desirable.

Scheme	Security	Assumption	$\lvert pk\rvert$	$\lvert sk\rvert$	$\lvert m\rvert$	$\lvert c\rvert - \lvert m\rvert$
HJR16 [23]	SIM-SSO-CPA	$\mathcal{D}_{l,k}$−MDDH	$(l \times k)\lvert G\rvert$	$(l-d) \times k$	$l-d$	$d \times \lvert G\rvert$
Ours	SIM-SSO-CPA	$\mathcal{D}_{l,k}$−MDDH	$l \times \lvert G\rvert$	k	1	$k \times \lvert G\rvert$

Fig. 2. Comparison of our scheme with HJR16 scheme in [23]. We use the same symbol as introduced in [23]. For a group G, $|G|$ denotes its size. For a matrix $\mathbf{A}$, d denotes the rank of $\mathbf{A}$. $|m|$ denotes the plaintext bitsize. $|c| - |m|$ denotes the ciphertext overhead.

4 SIM-SSO-CPA Secure Construction from Quadratic Residuosity

4.1 SIM-SSO-CPA Secure Construction from BGH Scheme

In this section, we show that the public-key scheme constructed from Boneh-Gentry-Hamburg (BGH) scheme [5] is SIM-SSO-CPA secure. Theorem 1 described in Sect. 3.3 will also be used in the security proof.

Quadratic Residuosity Assumption. Let $N = pq$ where p, q are two distinct safe primes, let $\left(\frac{x}{N}\right)$ denote the Jacobi symbol of $x \in \mathbb{Z}_N^*$, and let $J(N)$ be the set $\{x \in \mathbb{Z}_N^* : \left(\frac{x}{N}\right) = 1\}$. We denote by $QR(N)$ the subgroup of quadratic residues in $J(N)$. The quadratic residuosity assumption states that when the factorization of N is unknown, it is hard to distinguish random elements in $J(N) \setminus QR(N)$ from random elements in $QR(N)$.

Definition 5 (Quadratic Residuosity Assumption). *Let RSAGen be a PPT algorithm which, given a security parameter 1^λ, outputs two distinct primes p and q with their product $N = pq$. We say that the quadratic residuosity assumption holds for RSAGen if for all PPT distinguisher D, the function*

$$|\Pr[\mathcal{D}(x, N) = 1 | x \leftarrow \mathbb{QR}_N] - \Pr[\mathcal{D}(x, N) = 1 | x \leftarrow \mathbb{J}(N) \setminus \mathbb{QR}(N)|$$

is negligible; where the probabilities are taken over $(N, p, q) \leftarrow RSAGen(1^\lambda)$ and sampling $x \in \mathbb{QR}_N$ and $x \in \mathbb{J}_N \setminus \mathbb{QR}_N$ uniformly at random.

IBE/PKE Compatible. Most of the concept of IBE/PKE compatible is copied from [5]. Let $\mathcal{Q}$ be a deterministic algorithm that takes as input (N, R, S) where $N \in \mathbb{Z}^+$ and $R, S \in \mathbb{Z}_N^*$, outputs two polynomials $f, g \in \mathbb{Z}_N^*[x]$. We say that $\mathcal{Q}$ is IBE/PKE compatible if $\mathcal{Q}$ satisfies the following two conditions:

- (Condition 1) If R and S are quadratic residues, then $f(r)g(s)$ is also a quadratic residue for all square roots r of R and s of S.
- (Condition 2) If R is a quadratic residue, then $f(r)f(-r)S$ is also a quadratic residue for all square roots r of R.

(Condition 1) will be used to decrypt ciphertexts, (Condition 2) is only used to prove security, and satisfies the conditions of the following lemma in [5].

Lemma 1. *Let $N = pq$ be an RSA modulus, $X \in QR(N)$, and $S \in J(N) \setminus QR(N)$. Let x be a value that is randomly chosen from the four square roots of X, and let f be a polynomial with the property that $f(x)f(-x)S$ is a quadratic residue. Then the Jacobi symbol $\left(\frac{f(x)}{N}\right)$ is uniformly distributed over $\{-1, +1\}$.*

Construction. Next we prove that the PKE scheme constructed from BGH satisfies the four properties of a lossy encryption scheme with efficient opening.

Let $RSAgen(1^\lambda)$ be an algorithm that generates two distinct primes p and q, and outputs p, q along with their product N. The SIM-SSO-CPA secure construction is described as follows.

Gen(1^λ)**:** generates $(N, p, q) \leftarrow RSAGen(1^\lambda)$. Chooses $v \in \mathbb{Z}_N^*$ uniformly at random, and computes $V = v^2$. Let $pk = (N, V)$, and $sk = v$.

LGen(1^λ)**:** generates $(N, p, q) \leftarrow RSAGen(1^\lambda)$. Chooses $V \in J(N) \setminus \mathrm{QR}(N)$ uniformly at random. Let $pk = (N, V)$, and $sk = (p, q)$.

Enc(N, pk, m)**:** To encrypt a message $m \in \{-1, +1\}$, chooses $r \in \mathbb{Z}_N^*$ uniformly at random and sets $R = r^2$. Then computes:

$$(f, g) = \mathcal{Q}(N, R, V) \text{ and } c = m \cdot \left(\frac{f(r)}{N}\right)$$

Outputs the ciphertext (R, c).

Dec(sk, c)**:** Takes as input (R, c) and $sk = v$. Do:

$$(f, g) = \mathcal{Q}(N, R, V) \text{ and } m = c \cdot \left(\frac{g(v)}{N}\right)$$

Outputs m.

Theorem 3. *If the quadratic residuosity assumption holds for RSAGen, then the above construction is a lossy encryption scheme with efficient opening.*

Proof. **Correctness.** Given a real public key $pk = (N, V)$ where $V \in \mathrm{QR}(N)$ as well as a ciphertext (R, c). The deterministic algorithm $\mathcal{Q}(N, R, V)$ outputs two polynomials f and g. Because both R and V is quadratic residues, (Condition 1) implies that

$$\left(\frac{f(r)}{N}\right) = \left(\frac{g(v)}{N}\right)$$

Given the secret key $sk = c$, the plaintext is decrypted by computing

$$c \cdot \left(\frac{g(v)}{N}\right) = m \cdot \left(\frac{f(r)}{N}\right)\left(\frac{g(v)}{N}\right) = m.$$

Indistinguishability. It immediately follows from the quadratic residuosity assumption.

Lossiness. The lossiness property has been contained in the security proof of the PKE scheme in [5], appendix B. In lossy mode, public keys are (N, V) where $V \in J(N) \setminus \mathrm{QR}(N)$. Consider the ciphertext (R, c), where $c = m \cdot \left(\frac{f(r)}{N}\right) \in \{-1, +1\}$, and $r^2 = R$ modulo N. According to Condition (2), $f(r)f(-r)V$ is a quadratic residue for all square roots of R. Then Lemma 1 shows that $\left(\frac{f(r)}{N}\right)$ is uniformly distributed over $\{-1, +1\}$, hence $m \cdot \left(\frac{f(r)}{N}\right)$ will also be uniformly random over $\{-1, +1\}$ for any plaintext m.

Efficient openability. To see this, consider the opening algorithm Opener which, takes as input a lossy secret key $sk = (p, q)$, lossy public key $pk = (N, V)$ where $V \in J(N) \setminus \mathrm{QR}(N)$, message m, and ciphertext (R, c), and outputs an r' such that $m \cdot \left(\frac{f(r')}{N}\right) = c$. Because the factorization of $N = pq$ is known, Opener can use p and q to efficiently compute the four square roots of R, and let r' be a randomly chosen from the four squares roots. The output of Opener is r', which is just a random elements in $\mathbb{Z}_N^*$.

4.2 SIM-SSO-CPA Secure Construction from Cocks' Scheme

Cocks [8] proposed an elegant IBE scheme based on the quadratic residuosity assumption modulo an RSA composite N. In [33], Peikert *et al.* defined a (public-key based) variant of Cocks' scheme. In this section, we prove that the public key scheme constructed from the version of Cocks' cryptosystem in [33] is SIM-SSO-CPA secure.

Construction. Let $RSAGen(1^\lambda)$ be an algorithm that generates two distinct primes p and q, and outputs p, q along with their product N. The SIM-SSO-CPA secure construction is described as follows.

Gen(1^λ)**:** Generates $(N, p, q) \leftarrow RSAGen(1^\lambda)$. Picks $r \in \mathbb{Z}_N^*$ uniformly at random, and let $y = r^2$. Let $pk = (N, y)$, $sk = r$. Outputs (pk, sk).

LGen(1^λ)**:** Generates $(N, p, q) \leftarrow RSAGen(1^\lambda)$. Picks $y \in J(N) \setminus \mathrm{QR}(N)$ uniformly at random. Let $pk = (N, y)$, $sk = (p, q)$. Outputs (pk, sk).

Enc(pk, m)**:** To encrypt a message $m \in \{-1, +1\}$, picks $s \leftarrow \mathbb{Z}_N^*$ such that $\left(\frac{s}{N}\right) = m$, outputs $c = s + y/s$.

Dec(sk, c)**:** Outputs the Jacobi symbol of $(c + 2 \cdot sk)$.

To prove the SIM-SSO-CPA security of the above construction, we recall a lemma that presented in [33].

Lemma 2. *Let $N = pq$ be the product of two distinct primes, let $y \in \mathbb{Z}_N^*$ and set $pk = (N, y)$. If $y \in J(N) \setminus \mathrm{QR}(N)$, then the ciphertext is statistically independent of the plaintext.*

Theorem 4. *If the quadratic residuosity assumption holds for RSAGen, then the above construction is a lossy encryption scheme with efficient opening.*

Proof. **Correctness.** The correctness of the scheme under real keys is guaranteed by the completeness of Cocks' cryptosystem.

Indistinguishability. This follows readily from the quadratic residuosity assumption.

Lossiness. In lossy mode, $y \in J(N) \setminus \mathrm{QR}(N)$. Consider the ciphertext $c = s + y/s$, and the plaintext $m = \left(\frac{s}{N}\right)$, according to Lemma 2, the ciphertext c is statistically independent of the plaintext m.

Efficient openability. We say that the scheme is also efficiently openability, and the property implicitly contained in the proof of Lemma 2 in [33]. To see this, consider the algorithm Opener that on input a lossy secret key $sk = (p, q)$, lossy public key $pk = (N, y)$, plaintext m, ciphertext c. To claim c to any plaintext $m' \in \{-1, +1\}$, Opener has to find s' such that $s' + y/s' = s + y/s \bmod N$ and $\left(\frac{s'}{N}\right) = m'$. Since Opener knows the factorization of N, it can efficiently compute four solutions of the equation $c = s + y/s \bmod N$. Suppose s_0 is one of the solutions, then the other solutions are $(s_0 \bmod p, y/s_0 \bmod q)$, $(y/s_0 \bmod p, s_0 \bmod q)$, $(y/s_0 \bmod p, y/s_0 \bmod q)$. Let s' be a randomly chosen one of the four solutions, and the output of Opener is s', which is just a random element in $\mathbb{Z}_N^*$.

5 SIM-SSO-CPA Secure Construction from Homomorphic Trapdoor Commitment

The homomorphic trapdoor commitment in [16–18] consist of the following algorithms: Perfectly binding key generation, Perfectly hiding key generation, Commitment, Extraction, Trapdoor opening, Witness indistinguishability proof, Verification. The homomorphic trapdoor commitment can be converted into lossy encryption. That is, Perfectly binding key generation in homomorphic trapdoor commitment corresponds to Injective key generation in lossy encryption, Perfectly hiding key generation in homomorphic trapdoor commitment corresponds to Lossy key generation in lossy encryption, Commitment in homomorphic trapdoor commitment corresponds to Encryption in lossy encryption, Extraction in homomorphic trapdoor commitment corresponds to Decryption in lossy encryption, Trapdoor opening in homomorphic trapdoor commitment corresponds to Opening algorithm in lossy mode of the lossy encryption. Note that Trapdoor opening algorithm explicitly exists in homomorphic trapdoor commitment, but Opening algorithm is implicit in the lossy mode of the lossy encryption.

In this section, we prove that PKE constructions from the homomorphic trapdoor commitments only have the property of efficient weak openability, but still achieve SIM-SSO-CPA security. Theorem 1 in Sect. 3.3 will also be used for security proof.

5.1 SIM-SSO-CPA Secure Construction from Subgroup Decision Assumption

Let $\mathcal{G}$ be a PPT algorithm that takes as input security parameter 1^λ, outputs a tuple $(p, q, \mathbb{G}, \mathbb{G}_1, e, g)$ where p, q are distinct safe primes, $\mathbb{G}$ and $\mathbb{G}_1$ are cyclic groups with order $n = pq$, e is a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$, g and $e(g, g)$ are the generators of $\mathbb{G}$ and $\mathbb{G}_1$, respectively. The definition of subgroup decision assumption is described as follows.

Definition 6. *We say that the generator $\mathcal{G}$ satisfies the subgroup decision assumption if for any PPT adversary $\mathcal{A}$, we have*

$$|\Pr[(p, q, \mathbb{G}, \mathbb{G}_1, e, g) \leftarrow \mathcal{G}(1^\lambda); n = pq; x \leftarrow \mathbb{Z}_n^*; h = g^x : \mathcal{A}(n, \mathbb{G}, \mathbb{G}_1, e, g, h) = 1]$$
$$- \Pr[(p, q, \mathbb{G}, \mathbb{G}_1, e, g) \leftarrow \mathcal{G}(1^\lambda); n = pq; x \leftarrow \mathbb{Z}_q^*; h = g^{px} : \mathcal{A}(n, \mathbb{G}, \mathbb{G}_1, e, g, h) = 1]|$$

is negligible.

Construction. Boneh-Goh-Nissim (BGN) scheme [6] is the main building block of the homomorphic trapdoor commitment scheme in [17,18], which based on the subgroup decision assumption. The SIM-SSO-CPA secure construction is described as follows.

Gen(1^λ) : Given a security parameter 1^λ, runs $\mathcal{G}(1^\lambda)$ to obtain a tuple $(p, q, \mathbb{G}, \mathbb{G}_1, e, g)$, let $n = pq$. Picks $x \leftarrow \mathbb{Z}_q^*$, sets $h = g^{px}$. The public key is $pk = (n, \mathbb{G}, \mathbb{G}_1, e, g, h)$, the secret key is $sk = q$.

LGen(1^λ) : Given a security parameter 1^λ, runs $\mathcal{G}(1^\lambda)$ to obtain a tuple $(p, q, \mathbb{G}, \mathbb{G}_1, e, g)$, let $n = pq$. Picks $x \leftarrow \mathbb{Z}_n^*$, sets $h = g^x$. The public key is $pk = (n, \mathbb{G}, \mathbb{G}_1, e, g, h)$, the secret key is $sk = x$.

Enc(pk, m) : To encrypt a message $m \in \{0, 1, 2, \ldots, T\}$ where T is a prime and $T < p$, picks $r \leftarrow \mathbb{Z}_n^*$, computes $c = g^m h^r$. Outputs c as the ciphertext.

Dec(c, sk) : To decrypt a ciphertext c, takes as input the secret key $sk = q$, computes $c^q = (g^m h^r)^q = (g^q)^m$, then uses Pollard's ρ algorithm to recover m.

We turn to proving SIM-SSO-CPA security of the above construction under subgroup decision assumption. The security has been embodied implicitly in the construction of homomorphic trapdoor commitment in [17].

Theorem 5. *The construction in Sect. 5.1 is a lossy encryption scheme with efficient weak opening assuming $\mathcal{G}$ satisfies the subgroup decision assumption.*

Proof. **Correctness.** Correctness of decryption follows from the completeness of the BGN cryptosystem.

Indistinguishability. The subgroup decision assumption implies that two kinds of keys are computational indistinguishability.

Lossiness. Given lossy public key $pk = (n, \mathbb{G}, \mathbb{G}_1, e, g, h)$ for $h = g^x$, where x is chosen uniformly from the set $\mathbb{Z}_n^*$. Because h has order n, so $h = g^x$ is uniformly random over $\mathbb{G}$. Now, for random $r \in \mathbb{Z}_n^*$, the ciphertext $c = g^m h^r = g^m (g^x)^r$ will also be uniformly distributed over $\mathbb{G}$.

Efficient weak openability. The scheme is efficiently weak openability. Consider the algorithm Opener that takes as input a lossy secret key $sk = x$, lossy public key $pk = (n, \mathbb{G}, \mathbb{G}_1, e, g, h)$ where $h = g^x$, plaintext m and m', random coins r, and ciphertext c such that $c = \text{Enc}(pk, m; r)$. To claim c to any plaintext m', Opener has to find r' such that $\text{Enc}(pk, m; r) = \text{Enc}(pk, m; r')$. Since Opener holds the secret key x, it can efficiently return $r' = r - \frac{(m'-m)}{x} \bmod n$ which is just a random value in $\mathbb{Z}_n^*$.

Remarks. Note that the opening algorithm needs to receive an additional input, the random coins r that have been used to generate the ciphertext. So the construction meets the notion of weak opening. Also note that there is a gap in our proof. That is, we only succeed in proving weak opening. But this does not mean the above construction does not support a stronger opening algorithm.

5.2 SIM-SSO-CPA Secure Construction from Decisional Linear Assumption

Boneh, Boyen, and Shacham first proposed the decisional linear assumption [4]. Let $\mathcal{G}_{\text{DLIN}}$ be a PPT algorithm that takes as input security parameter 1^λ and outputs a tuple $(p, \mathbb{G}, g)$ where p is a prime, $\mathbb{G}$ is a cyclic group of order p, and g is a random generator of $\mathbb{G}$. The definition of decisional linear assumption is described as follows.

Definition 7 (Decisional Linear Assumption). *We say that the decisional linear assumption holds for the generator $\mathcal{G}_{\text{DLIN}}$ if for all PPT adversary $\mathcal{A}$ we have*

$$\begin{aligned} &|\Pr[(p,\mathbb{G},g) \leftarrow \mathcal{G}_{\text{DLIN}}(1^\lambda); x,y \leftarrow \mathbb{Z}_p^*; r,s \leftarrow \mathbb{Z}_p : \mathcal{A}(g, g^x, g^y, g^{xr}, g^{ys}, g^{r+s}) = 1] \\ &- \Pr[(p,\mathbb{G},g) \leftarrow \mathcal{G}_{\text{DLIN}}(1^\lambda); x,y \leftarrow \mathbb{Z}_p^*; r,s,d \leftarrow \mathbb{Z}_p : \mathcal{A}(g, g^x, g^y, g^{xr}, g^{ys}, g^{d}) = 1]| \end{aligned}$$

is negligible.

Construction. Next we show that the PKE scheme constructed from homomorphic trapdoor commitment in [16,18] is a lossy encryption scheme with efficient weak opening, and this property has been contained implicitly in the construction of the original commitment scheme. Now, we present the SIM-SSO-CPA secure construction in the following.

Gen(1^λ) : Runs $(p, \mathbb{G}, g) \leftarrow \mathcal{G}_{\text{DLIN}}(1^\lambda)$, picks $x, y \leftarrow \mathbb{Z}_p^*$, sets $f = g^x$, $h = g^y$, picks $r_u, s_v \leftarrow \mathbb{Z}_p$, $z \leftarrow \mathbb{Z}_p^*$, and computes $(u, v, w) = (f^{r_u}, h^{s_v}, g^{r_u + s_v + z})$. Let $pk = (p, \mathbb{G}, g, f, h, u, v, w)$, $sk = (x, y, z)$.

LGen(1^λ) : Runs $(p, \mathbb{G}, g) \leftarrow \mathcal{G}_{\text{DLIN}}(1^\lambda)$, picks $x, y \leftarrow \mathbb{Z}_p^*$, let $f = g^x$, $h = g^y$, picks $r_u, s_v \leftarrow \mathbb{Z}_p$, and computes $(u, v, w) = (f^{r_u}, h^{s_v}, g^{r_u + s_v})$. Let $pk = (p, \mathbb{G}, g, f,\ h, u, v, w)$, $sk = (r_u, s_v)$.

Enc(pk, m) : On inputs pk and a message $m \in \{0, 1, 2, \ldots, T\}$ where T is a prime and $T < p$, picks $(r, s) \leftarrow \mathbb{Z}_p \times \mathbb{Z}_p$, and computes

$$c = (c_1, c_2, c_3) = (u^m f^r, v^m h^s, w^m g^{r+s})$$

Dec(c, sk) : On inputs the ciphertext $c = (c_1, c_2, c_3)$, and $sk = (x, y, z)$, computes $(g^z)^m = c_3 c_1^{-1/x} c_2^{-1/y}$, then recovers m by using Pollard's ρ method in the confined message space.

Theorem 6. *The above construction is a lossy encryption scheme with efficient weak opening assuming $\mathcal{G}_{\text{DLIN}}$ satisfies the decisional linear assumption.*

Proof. **Correctness.** Correctness of decryption follows from the completeness of *Extraction algorithm* from homomorphic trapdoor commitment.

Indistinguishability. Since real public keys $(u, v, w) = (f^{r_u}, h^{s_v}, g^{r_u + s_v + z})$ are not linear tuple, and lossy public key $(u, v, w) = (f^{r_u}, h^{s_v}, g^{r_u + s_v})$ are random linear tuple. Under the decision linear assumption, real public keys and lossy public keys are computational indistinguishability.

Lossiness. Given the lossy public key $pk = (f^{r_u}, h^{s_v}, g^{r_u + s_v})$, pk is a linear tuple, and pk is also the perfect hiding commitment key. Following the statistically hiding property of the homomorphic trapdoor commitment, the ciphertext $(u^m f^r, v^m h^s, w^m g^{r+s})$ hides m perfectly.

Efficient weak openability. To see this, consider the algorithm Opener that takes as input a lossy secret key (r_u, s_v), lossy public key $(f^{r_u}, h^{s_v}, g^{r_u + s_v})$, plaintexts m and m', random coins (r, s), ciphertext c such that $c = \mathrm{Enc}(pk, m;\ r, s)$. To claim c to any plaintext m', Opener has to find (r', s') such that satisfy $\mathrm{Enc}(pk, m;\ r, s) = \mathrm{Enc}(pk, m; r', s')$. Since Opener holds secret key $sk = (r_u, s_v)$, it can efficiently outputs $r' = r - (m' - m)r_u \bmod p$ and $s' = s - (m' - m)s_v \bmod p$, where r' and s' are random elements in $\mathbb{Z}_p$.

Remarks. Note that in the input of the opening algorithm, the random coins r and s are also necessary. Hence, the above construction meets the notion of weak opening. Also note that there is a gap in our proof, please see the Remarks in Sect. 5.1.

6 Conclusion

In this paper we study public key encryptions of simulation-based security against sender selective-opening attacks. In concrete, we present a generic construction that achieves SIM-SSO-CPA security from lossy encryption, and give an instantiation based on the Matrix Diffie-Hellman Assumption. In fact, our instantiation is inefficient, and a further improvement would be desirable.

We further prove that the PKE constructions from Boneh-Gentry-Hamburg scheme, Cocks' scheme and homomorphic trapdoor commitments are SIM-SSO-CPA secure. These schemes have natural lossiness property, but it is not our purpose to make them explicit. We focus on whether the efficient opening algorithm exists or not, and succeed in building PKE schemes that support efficient opening.

Acknowledgments. The authors would like to thank the anonymous reviewers for their invaluable comments and suggestions. The authors are also grateful to Xin Wang and Haiyang Hu for helpful discussions and advice.

A: Security Proof of the Instantiation in Sect. 3.4

We show that the instantiation satisfies the four properties of a lossy encryption scheme with efficient weak opening.

Proof. **Correctness.** This follows readily from the correctness of $\mathcal{D}_{l,k}$-MDDH-based hash proof system.

Indistinguishability. It is obvious that $(\mathcal{G}, [\mathbf{A}\boldsymbol{w}])$ and $(\mathcal{G}, [\boldsymbol{u}])$ are computationally indistinguishable under the $\mathcal{D}_{l,k}$-MDDH assumption.

Lossiness. Consider the lossy public key $[\boldsymbol{x}] = [\boldsymbol{u}]$ where $\boldsymbol{u} \leftarrow \mathbb{Z}_q^l$. According to the smoothness property of the $\mathcal{D}_{l,k}$-MDDH-based hash proof system, $[\boldsymbol{k}^{\mathrm{T}}\boldsymbol{u}]$ is statistically indistinguishable from a random element in $\mathbb{G}$. Since $\mathrm{H}([\boldsymbol{k}^T\boldsymbol{u}])$ is statistically close to uniform distribution over $\{0,1\}$, hence $\mathrm{H}([\boldsymbol{k}^T\boldsymbol{u}]) \oplus m$ will also be statistically close to uniform distribution over $\{0,1\}$ for any message m.

Efficient weak openability. Please read Sect. 3.2.

Remarks. Note that if we do not require the property of efficient weak openability, the compress function H is unnecessary. In this case, we need to make some changes of the construction. The Injective key generation algorithm and Lossy key generation algorithm will not change. It only needs to modify the encryption and decryption algorithm.

- **Encryption:** On input a message $m \in \mathbb{G}$, picks $\boldsymbol{k} \in \mathbb{Z}_q^l$, $\boldsymbol{c}_1 = [\boldsymbol{k}^{\mathrm{T}}\mathbf{A}]$, $c_2 = [\boldsymbol{k}^{\mathrm{T}}\boldsymbol{x}] \cdot m$. Outputs ciphertext $c = (\boldsymbol{c}_1, c_2)$.
- **Decryption:** Given ciphertext $c = (\boldsymbol{c}_1, c_2)$, $sk = \boldsymbol{w}$. Outputs $m = (c_2 \cdot m)/[\boldsymbol{c}_1 \cdot \boldsymbol{w}]$.

The modified construction is an instantiation of the generic lossy encryption in [21] (as well as the dual Cramer-Shoup scheme in [35], Sect. 2.2), and correctness can be easily verified. While $[\boldsymbol{x}] \in \mathcal{X}$, smoothness property shows that $[\boldsymbol{k}^{\mathrm{T}}\boldsymbol{x}]$ is completely undetermined. But without the compress function H, the space of random coins is large, so algorithm Opener needs to compute the set of all $\boldsymbol{k}$' $\in \mathbb{Z}_q^l$ such that $[\boldsymbol{k}'^{\mathrm{T}}\mathbf{A}] = [\boldsymbol{k}^{\mathrm{T}}\mathbf{A}]$ until $[\boldsymbol{k}'^{\mathrm{T}}\boldsymbol{x}] \cdot m' = [\boldsymbol{k}^{\mathrm{T}}\boldsymbol{x}] \cdot m$. Hence, Opener may not efficient. According to the result in [2], the modified scheme only achieves IND-SSO-CPA security.

References

1. Bellare, M., Dowsley, R., Waters, B., Yilek, S.: Standard security does not imply security against selective-opening. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 645–662. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_38
2. 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, Heidelberg (2009). doi:10.1007/978-3-642-01001-9_1
3. Böhl, F., Hofheinz, D., Kraschewski, D.: On definitions of selective opening security. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 522–539. Springer, Heidelberg (2012). doi:10.1007/978-3-642-30057-8_31
4. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_3

5. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption without pairings. In: 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007), pp. 647–657 (2007)
6. Boneh, D., Goh, E.-J., Nissim, K.: Evaluating 2-DNF formulas on ciphertexts. In: Kilian, J. (ed.) TCC 2005. LNCS, vol. 3378, pp. 325–341. Springer, Heidelberg (2005). doi:10.1007/978-3-540-30576-7_18
7. Canetti, R., Dwork, C., Naor, M., Ostrovsky, R.: Deniable encryption. In: Kaliski, B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 90–104. Springer, Heidelberg (1997). doi:10.1007/BFb0052229
8. Cocks, C.: An identity based encryption scheme based on quadratic residues. In: Honary, B. (ed.) Cryptography and Coding 2001. LNCS, vol. 2260, pp. 360–363. Springer, Heidelberg (2001). doi:10.1007/3-540-45325-3_32
9. 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, Heidelberg (2002). doi:10.1007/3-540-46035-7_4
10. Deng, Y., Song, X., Yu, J., Chen, Y.: On instance compression, schnorr/guillou-quisquater, and the security of classic protocols for unique witness relations. IACR Cryptol. ePrint Archive **2017**, 390 (2017)
11. Dwork, C., Naor, M., Reingold, O., Stockmeyer, L.J.: Magic functions. In: 40th Annual Symposium on Foundations of Computer Science, FOCS 1999, pp. 523–534 (1999)
12. Escala, A., Herold, G., Kiltz, E., Ràfols, C., Villar, J.: An algebraic framework for Diffie-Hellman assumptions. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013. LNCS, vol. 8043, pp. 129–147. Springer, Heidelberg (2013). doi:10.1007/978-3-642-40084-1_8
13. Fehr, S., Hofheinz, D., Kiltz, E., Wee, H.: Encryption schemes secure against chosen-ciphertext selective opening attacks. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 381–402. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13190-5_20
14. Fuchsbauer, G., Heuer, F., Kiltz, E., Pietrzak, K.: Standard security does imply security against selective opening for markov distributions. In: Kushilevitz, E., Malkin, T. (eds.) TCC 2016. LNCS, vol. 9562, pp. 282–305. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49096-9_12
15. Fujisaki, E.: All-but-many encryption – a new framework for fully-equipped UC commitments. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 426–447. Springer, Heidelberg (2014). doi:10.1007/978-3-662-45608-8_23
16. Groth, J., Ostrovsky, R., Sahai, A.: Non-interactive zaps and new techniques for NIZK. In: Dwork, C. (ed.) CRYPTO 2006. LNCS, vol. 4117, pp. 97–111. Springer, Heidelberg (2006). doi:10.1007/11818175_6
17. Groth, J., Ostrovsky, R., Sahai, A.: Perfect non-interactive zero knowledge for NP. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 339–358. Springer, Heidelberg (2006). doi:10.1007/11761679_21
18. Groth, J., Ostrovsky, R., Sahai, A.: New techniques for noninteractive zero-knowledge. J. ACM **59**(3), 11:1–11:35 (2012)
19. Harnik, D., Naor, M.: On the compressibility of *NP* instances and cryptographic applications. SIAM J. Comput. **39**(5), 1667–1713 (2010)
20. Hazay, C., Patra, A., Warinschi, B.: Selective opening security for receivers. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 443–469. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48797-6_19

21. 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, Heidelberg (2011). doi:10.1007/978-3-642-25385-0_4
22. Hofheinz, D.: All-but-many lossy trapdoor functions. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 209–227. Springer, Heidelberg (2012). doi:10.1007/978-3-642-29011-4_14
23. Hofheinz, D., Jager, T., Rupp, A.: Public-key encryption with simulation-based selective-opening security and compact ciphertexts. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 146–168. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53644-5_6
24. Hofheinz, D., Rao, V., Wichs, D.: Standard security does not imply indistinguishability under selective opening. In: Hirt, M., Smith, A. (eds.) TCC 2016. LNCS, vol. 9986, pp. 121–145. Springer, Heidelberg (2016). doi:10.1007/978-3-662-53644-5_5
25. Hofheinz, D., Rupp, A.: Standard versus selective opening security: separation and equivalence results. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 591–615. Springer, Heidelberg (2014). doi:10.1007/978-3-642-54242-8_25
26. Huang, Z., Liu, S., Qin, B.: Sender-equivocable encryption schemes secure against chosen-ciphertext attacks revisited. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 369–385. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36362-7_23
27. Jia, D., Lu, X., Li, B.: Receiver selective opening security from indistinguishability obfuscation. In: Dunkelman, O., Sanadhya, S.K. (eds.) INDOCRYPT 2016. LNCS, vol. 10095, pp. 393–410. Springer, Cham (2016). doi:10.1007/978-3-319-49890-4_22
28. Jia, D., Lu, X., Li, B.: Constructions secure against receiver selective opening and chosen ciphertext attacks. In: Handschuh, H. (ed.) CT-RSA 2017. LNCS, vol. 10159, pp. 417–431. Springer, Cham (2017). doi:10.1007/978-3-319-52153-4_24
29. Kalai, Y.T.: Smooth projective hashing and two-message oblivious transfer. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 78–95. Springer, Heidelberg (2005). doi:10.1007/11426639_5
30. Liu, S., Paterson, K.G.: Simulation-based selective opening CCA security for PKE from key encapsulation mechanisms. In: Katz, J. (ed.) PKC 2015. LNCS, vol. 9020, pp. 3–26. Springer, Heidelberg (2015). doi:10.1007/978-3-662-46447-2_1
31. Naor, M., Segev, G.: Public-key cryptosystems resilient to key leakage. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 18–35. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03356-8_2
32. Paillier, P.: Public-key cryptosystems based on composite degree residuosity classes. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 223–238. Springer, Heidelberg (1999). doi:10.1007/3-540-48910-X_16
33. Peikert, C., Vaikuntanathan, V., Waters, B.: A framework for efficient and composable oblivious transfer. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 554–571. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85174-5_31
34. Peikert, C., Waters, B.: Lossy trapdoor functions and their applications. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, pp. 187–196 (2008)
35. Wee, H.: KDM-security via homomorphic smooth projective hashing. In: Cheng, C.-M., Chung, K.-M., Persiano, G., Yang, B.-Y. (eds.) PKC 2016. LNCS, vol. 9615, pp. 159–179. Springer, Heidelberg (2016). doi:10.1007/978-3-662-49387-8_7