8-2015

Identity-based lossy encryption from learning with errors

Jingnan HE

Bao LI

Xianhui LU

Dingding JIA

Haiyang XUE
Singapore Management University, haiyangxue@smu.edu.sg

See next page for additional authors

Identity-Based Lossy Encryption from Learning with Errors

Jingnan He[1,2,3(✉)], Bao Li[1,2], Xianhui Lu[1,2], Dingding Jia[1,2], Haiyang Xue[1,2], and Xiaochao Sun[1,2]

[1] State Key Laboratory of Information Security, Institute of Information Engineering of Chinese Academy of Sciences, Beijing, China
{jnhe13,lb,xhlu,ddjia,hyxue12,xchsun}@is.ac.cn
[2] Data Assurance and Communication Security Research Center of Chinese Academy of Sciences, Beijing, China
[3] University of Chinese Academy of Sciences, Beijing, China

Abstract. We extend the notion of lossy encryption to the scenario of identity-based encryption (IBE), and propose a new primitive called identity-based lossy encryption (IBLE). Similar as the case of lossy encryption, we show that IBLE can also achieve selective opening security. Finally, we present a construction of IBLE from the assumption of learning with errors.

Keywords: Lossy encryption · Learning with errors · Identity-based lossy encryption

1 Introduction

1.1 Background

Lossy encryption was proposed by Bellare, Hofheinz and Yilek [3] to achieve selective opening security. Briefly, the key generation algorithm of lossy encryption runs in two indistinguishable modes, the real mode and the lossy mode. In the real mode, a real pubic key $\mathsf{PK}_{\text{real}}$ is generated and scheme works just as standard public key encryption scheme. In the lossy mode, a lossy public key $\mathsf{PK}_{\text{loss}}$ is generated, and the plaintext is information-theoretically hidden.

Lossy encryption can be constructed from several primitives, such as lossy trapdoor functions (LTDF) [3], re-randomizable encryption [18] and oblivious transfer [18]. It also can be constructed from concrete assumptions, such as decision Diffie-Hellman (DDH) [3,19], quadratic residuosity (QR) [3], learning with errors (LWE) [22] and so on.

This research is supported by the National Nature Science Foundation of China (No. 61379137 and No. 61272040), the National Basic Research Program of China (973 project)(No. 2013CB338002), and IIE's Cryptography Research Project (No. Y4Z0061403 and No. Y4Z0061D03).

K. Tanaka and Y. Suga (Eds.): IWSEC 2015, LNCS 9241, pp. 3–20, 2015.
DOI: 10.1007/978-3-319-22425-1_1

As a strengthen version of public key encryption, identity-based encryption (IBE), proposed by Shamir [25], is a powerful primitive in which the public key can be an arbitrary string. Currently, IBE schemes can be constructed from pairings [7–9,24,26,27], lattices (LWE) [1,2,11,16] and QR [10,12,20].

Motivation. Currently the most important application of lossy encryption is to achieve selective opening security. However, in the scenario of IBE, the selective opening security is achieved by using one-sided public openability [5,21]. Whether the selective opening secure IBE scheme can be constructed via the idea of lossy encryption is an interesting problem.

1.2 Our Contributions

New Definition and Its Application. We give the definition of identity-based lossy encryption (IBLE). Similar to lossy encryption, there are also two indistinguishable modes in identity-based lossy encryption, the real mode and the lossy mode. The real mode is akin to a normal IBE, but the case of lossy mode is more delicate. Specifically, in the lossy mode the lossiness of the master public key $\mathsf{MPK}_{\mathsf{lossy}}$ can be triggered by a particular identity $\mathbf{id}_{\mathsf{lossy}}$ only. The reason is that in IBE the adversary can obtain the identity private keys $\mathsf{SK}_{\mathbf{id}}$ for arbitrary identities except the challenge identity by a series of extraction queries, it can distinguish $\mathsf{MPK}_{\mathrm{real}}$ from $\mathsf{MPK}_{\mathsf{lossy}}$ with the help of $\mathsf{SK}_{\mathbf{id}}$. With IBLE, we obtain indistinguishability-based selective opening security in the selective identity setting (IND-sID-SO).

Construction from LWE. Inspired by [1,2,11,16], we start the construction of our IBLE scheme by designing a dual Regev type lossy encryption. Specifically let $(\mathbf{A_1}\mathbf{s}+\mathbf{e_1}, \mathbf{A_2}\mathbf{s}+\mathbf{e_2}+\mathbf{m}\lfloor\frac{q}{2}\rceil)$ be the ciphertext of a dual Regev type encryption scheme, where $(\mathbf{A_1}, \mathbf{A_2})$ is the public key, $\mathbf{s}, \mathbf{e}_1, \mathbf{e}_2$ are random numbers, and $\mathbf{m}$ is the message. The main technical difficulty of constructing lossy encryption is to information-theoretically hide the plaintext message $\mathbf{m}$. However, the random number $\mathbf{s}$ is completely determined by the first item of the ciphertext, consequently, $\mathbf{m}$ is fixed by the second item of the ciphertext. Our solution is to lose the information of $\mathbf{s}$ with the technique proposed in [6,17]. Concretely, the randomly selected $\mathbf{A_1} \in \mathbb{Z}_{\mathbf{q}}^{\mathbf{m}\times\mathbf{n}}$ is replaced by an LWE sample $(\mathbf{BC}+\mathbf{Z})$ where $\mathbf{B} \in \mathbb{Z}_q^{m\times n_1}, \mathbf{C} \in \mathbb{Z}_q^{n_1\times n}, \mathbf{Z} \in \mathbb{Z}^{m\times n}$ sampled from the discrete Gaussians distribution. If $n_1 < n$ and the element of $\mathbf{Z}$ is small enough, then $\mathbf{s}$ is information-theoretically undetermined given $(\mathbf{BC}+\mathbf{Z})\mathbf{s}+\mathbf{e}$ [6,17].

Combining our dual Regev type lossy encryption and the technique for constructing IBE scheme in [1], we obtain an IBLE scheme. To hide the plaintext message information-theoretically for $\mathbf{id}_{\mathsf{lossy}}$ and simultaneously extract the identity private key for other identities, the main technical challenge is to guarantee that $\mathbf{s}$ is still information-theoretically undetermined given $(\begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}+\begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix})\mathbf{s}+\mathbf{e}$, where $\mathbf{R} \in \{-1,1\}^{m\times m}$. Luckily, we prove that it still holds when

$n_1 < n$ and the element of $\mathbf{Z}$ is small enough. From another point of view, it is not only an extension of the result proved in [6], but also provides another choice for constructing lossy branch.

1.3 Related Work

LTDF, which is closely related with lossy encryption, has been extended to the identity-based scenario by Bellare, Kiltz, Peikert and Waters [4]. Escala, Herranz, Libert, and Ráfols [15] further studied hierarchical identity-based LTDF. Similar to the construction of lossy encryption from LTDF, the primitive IBLE can also be obtained from identity-based LTDF.

1.4 Organization

The rest of this paper is organized as follows. In Sect. 2 we introduce some notations, definitions and previous results. In Sect. 3, we give the definition of IBLE, prove that IBLE scheme implies selective opening security, and propose a construction of IBLE from LWE.

2 Preliminaries

2.1 Notations

Unless otherwise noted, all operations in this paper are under the modulo operation of q, and log means $\log_2$. Throughout, we use λ to denote our security parameter. We use bold lower-case letters (e.g. $\mathbf{s}$) to denote vectors, and bold upper-case letters (e.g. $\mathbf{A}$) to denote matrices. We use $x \xleftarrow{\$} X$ to denote that x is drawn uniformly at random over a set X. We use $x \leftarrow \mathcal{X}$ to denote that x is drawn from a distribution $\mathcal{X}$. To denote the statistical distance between two distributions, we write $\Delta(\mathcal{X}, \mathcal{Y})$. For two distribution ensembles $\mathcal{X} = \mathcal{X}_\lambda, \mathcal{Y} = \mathcal{Y}_\lambda$, we write $\mathcal{X} \approx_s \mathcal{Y}$ if $\Delta(\mathcal{X}, \mathcal{Y})$ is a negligible function of λ, and we write $\mathcal{X} \approx_c \mathcal{Y}$ if for all probabilistic polynomial time (PPT) distinguishers D there is a negligible function $negl(\cdot)$ such that: $|\Pr[D(1^\lambda, \mathcal{X}_\lambda) = 1] - \Pr[D(1^\lambda, \mathcal{Y}_\lambda) = 1]| \leq negl(\lambda)$. We let $\lfloor x \rceil$ be the closest integer to x. We use $\|\mathbf{S}\|$ to denote the L_2 length of the longest vector in $\mathbf{S}$, and $\|\tilde{\mathbf{S}}\|$ to denote the Gram-Schmidt norm of $\mathbf{S}$. Let $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{e} \in \mathbb{Z}^m \ s.t. \ \mathbf{Ae} = \mathbf{0} \mod q\}$, and $\Lambda_q^{\mathbf{u}} = \{\mathbf{e} \in \mathbb{Z}^m \ s.t. \ \mathbf{Ae} = \mathbf{u} \mod q\}$, given a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$.

2.2 Min-Entropy

The **min-entropy** of a random variable X is $\tilde{H}_\infty(X) = -\log(\max_x \Pr[X = x])$, and the **average min-entropy** of X conditioned on Y, defined by [13], is $H_\infty(X|Y) = -\log(\mathbf{E}_{y \leftarrow Y}[\max_x \Pr[X = x|Y = y]]) = -\log(\mathbf{E}_{y \leftarrow Y}[2^{-H_\infty(X|Y=y)}])$.

Definition 1 ([13]). *For two random variables X and Y, the* **ϵ-smooth average min-entropy** *of X conditioned on Y, denoted $\tilde{H}_\infty^\epsilon(X|Y)$ is $\tilde{H}_\infty^\epsilon(X|Y) = \max_{(X',Y'):\Delta((X,Y),(X',Y'))<\epsilon} \tilde{H}_\infty(X'|Y')$.*

2.3 Learning with Errors

Learning with errors (LWE) problem initially stated in [23]. Here we recall the concepts and the hardness of LWE.

Learning with Errors (LWE)**.** Let $m = m(n),\ q = q(n)$ be integers, and χ be a distribution on $\mathbb{Z}_q$. Let $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \mathbf{e} \leftarrow \chi^m$, then the LWE$(m, n, q, \chi)$ problem is to find $\mathbf{s}$, given $(\mathbf{A}, \mathbf{As} + \mathbf{e})$.

This is the search version of the LWE problem, and there is a decisional version of the LWE problem.

(Decisional) Learning with Errors (DLWE)**.** Let $m = m(n),\ q = q(n)$ be integers, and χ be a distribution on $\mathbb{Z}_q$. Let $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m\times n}, \mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n, \mathbf{e} \leftarrow \chi^m$, then the DLWE$(m, n, q, \chi)$ problem is that given $(\mathbf{A}, \mathbf{b})$, decide whether $\mathbf{b}$ is distributed by $\mathbf{As} + \mathbf{e}$ or chosen uniformly at random from $\mathbb{Z}_q^m$.

The hardness of the matrix-version of the DLWE problem is as below.

Lemma 1 ([14])**.** *Let $m(n), k(n) = \mathsf{poly}(n)$. Assume that DLWE$(m, n, q, \chi)$ is pseudorandom [23]. Then the distribution $(\mathbf{A}, \mathbf{AX} + \mathbf{E})$ is also pseudorandom, where $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ and $\mathbf{X} \in \mathbb{Z}_q^{n\times k}$ are chosen uniformly at random and $\mathbf{E}$ is chosen according to $\mathcal{D}_{\mathbb{Z},\alpha q}^{m\times k}$.*

2.4 Discrete Gaussians

For any $s > 0$ and $\boldsymbol{c} \in \mathbb{R}^n$, define the Gaussian function: $\forall \mathbf{x} \in \mathbb{R}^n, \rho_{s,\mathbf{c}}(\mathbf{x}) = \exp(-\pi\|\mathbf{x} - \mathbf{c}\|^2/s^2)$.

For any $\mathbf{c} \in \mathbb{R}^n$, real $s > 0$, and n-dimensional lattice Λ, define the discrete Gaussian distribution over Λ as: $\forall \mathbf{x} \in \Lambda, \mathcal{D}_{\Lambda,s,\mathbf{c}}(\mathbf{x}) = \frac{\rho_{s,\mathbf{c}}(\mathbf{x})}{\rho_{s,\mathbf{c}}(\Lambda)}$ where $\rho_{s,\mathbf{c}}(\Lambda) = \sum_{\mathbf{y}\in\mathbf{\Lambda}} \rho_{s,\mathbf{c}}(\mathbf{y})$. We omit the parameter $\mathbf{c}$ when $\mathbf{c} = \mathbf{0}$.

2.5 Lossy Encryption

Lossy Encryption Scheme is defined in [3]. It is given by a tuple of PPT algorithms {KeyGen$_{real}$, KeyGen$_{loss}$, Enc, Dec}. The details are as below.

- **KeyGen$_{\mathsf{real}}$**(1^λ): a key generation algorithm takes a security parameter λ as input, and outputs a pair of real public key and corresponding secret key $(\mathsf{PK}_{\mathsf{real}}, \mathsf{SK})$.
- **KeyGen$_{\mathsf{loss}}$**(1^λ): a key generation algorithm takes a security parameter λ as input, and outputs a pair of lossy public key and $\perp$ instead of SK $(\mathsf{PK}_{\mathsf{lossy}}, \perp)$.
- **Enc**(PK, m): an encryption algorithm takes either $\mathsf{PK}_{\mathsf{real}}$ or $\mathsf{PK}_{\mathsf{loss}}$ and message m as input, and outputs a ciphertext C.
- **Dec**$(\mathsf{SK}, \mathsf{C})$: a decryption algorithm takes a secret key SK and a ciphertext C as input, and outputs either a message m or $\perp$ in the case of failure.

A *Lossy Encryption Scheme* should have the properties below.

1. *Correctness on Real Keys.* For all $(\mathsf{PK}_{\mathsf{real}}, \mathsf{SK})$ generated by $\mathbf{KeyGen}_{\mathbf{real}}(1^k)$ and all message m, $\mathbf{Dec}(\mathsf{SK}, \mathbf{Enc}(\mathsf{PK}_{\mathsf{real}}, m)) = m$.
2. *Lossiness of Encryption with Lossy Keys.* For any lossy keys $\mathsf{PK}_{\mathsf{loss}}$ generated by $\mathbf{KeyGen}_{\mathbf{loss}}(1^k)$ and any two messages $m_0 \neq m_1$, there is $\mathbf{Enc}(\mathsf{PK}_{\mathsf{loss}}, m_0) \approx_s \mathbf{Enc}(\mathsf{PK}_{\mathsf{loss}}, m_1)$.
3. *Indistinguishability Between Real Public Key and Lossy Public Key.* For any $\mathsf{PK}_{\mathrm{real}}$ generated by $\mathbf{KeyGen}_{\mathbf{real}}$ and any $\mathsf{PK}_{\mathsf{loss}}$ generated by $\mathbf{KeyGen}_{\mathbf{loss}}$, there is $\mathsf{PK}_{\mathsf{real}} \approx_c \mathsf{PK}_{\mathsf{loss}}$.

2.6 Some Results About Randomness

Randomness plays an important role in constructing lossy encryption schemes, so we introduce some results about randomness which will be used as tools in the later section.

Lemma 2 ([17]). *Let $\mathcal{D}$ be a distribution over $\mathbb{Z}_q^n$ with min-entropy k. For any $\varepsilon > 0$ and $l \leq (k - 2\log(1/\varepsilon) - O(1))/\log q$, the joint distribution of $(\mathbf{C}, \mathbf{C} \cdot \mathbf{s})$ where $\mathbf{C} \leftarrow \mathbb{Z}_q^{l \times n}$ is uniformly random and $\mathbf{s} \in \mathbb{Z}_q^{l \times n}$ is drawn from the distribution $\mathcal{D}$ is ε-close to the uniform distribution over $\mathbb{Z}_q^{l \times n} \times \mathbb{Z}_q^l$.*

Lemma 3 ([16]). *Let n and q be positive integers with q prime, and let $m \geq 2n\log q$. Then for all but a $2q^{-n}$ fraction of all $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ and for any $s \geq \omega(\sqrt{\log m})$, the distribution of the syndrome $\mathbf{u}^t = \mathbf{e}^t\mathbf{A}$ mod q is statistically close to uniform over $\mathbb{Z}_q^n$, where $\mathbf{e} \sim \mathcal{D}_{\mathbb{Z},s}^m$.*

Lemma 4 ([6]). *There exists a distribution Lossy such that $\bar{\mathbf{A}} \leftarrow \mathsf{Lossy} \approx_c \mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ and given $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, and $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z},\beta q}^{m \times n}$, $\tilde{H}_\infty^\epsilon(\mathbf{s}|\bar{\mathbf{A}}, \bar{\mathbf{A}}\mathbf{s} + \mathbf{x}) \geq n$, where $\epsilon = negl(\lambda)$. Lossy is as follows,*

- *Choose $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{m \times k}$, $\mathbf{C} \xleftarrow{\$} \mathbb{Z}_q^{k \times n}$, and $\mathbf{Z} \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}^{m \times n}$, where $\frac{\alpha}{\beta} = negl(\lambda)$ and $k\log q \leq n - 2\lambda + 2$.*
- *Let $\bar{\mathbf{A}} = \mathbf{BC} + \mathbf{Z}$.*
- *Output $\bar{\mathbf{A}}$.*

3 Identity-Based Lossy Encryption

In this section, we give the definition of IBLE. An IBLE scheme works in two modes. One is the real mode which is the same as an IBE scheme with standard master key generation algorithm and extraction algorithm. The other is the lossy mode with a lossy master key generation algorithm, and the corresponding extraction algorithm. The two modes share the same encryption and decryption algorithms. For identities $\mathbf{id} \neq \mathbf{id}_{\mathsf{lossy}}$, encryptions with the lossy master public key $\mathsf{MPK}_{\mathrm{lossy}}$ are committing as the same in the real mode. For $\mathbf{id}_{\mathsf{lossy}}$, encryptions are not committing.

Formally, the real mode is a tuple of PPT algorithms $\{\mathsf{Setup}_{\mathsf{real}}, \mathsf{Extract}_{\mathsf{real}}, \mathsf{Enc}, \mathsf{Dec}\}$:

- $\mathbf{Setup_{real}}(1^\lambda)$: a master key generation algorithm takes a security parameter λ as input, and outputs a pair of real master public key and corresponding master secret key $(\mathsf{MPK_{real}}, \mathsf{MSK})$.
- $\mathbf{Extract_{real}}(\mathbf{id}, \mathsf{MPK_{real}}, \mathsf{MSK})$: a user secret key generation algorithm takes an identity $\mathbf{id}$, the master public key $\mathsf{MPK_{real}}$ and the master secret key MSK as inputs, and outputs a user secret key $\mathsf{SK_{id}}$ for the identity.
- $\mathbf{Enc}(\mathbf{id}, \mathsf{MPK}, \mathbf{m})$: a user encryption algorithm takes an identity $\mathbf{id}$, the master public key MPK and a message $\mathbf{m}$ as inputs, and outputs a ciphertext C.
- $\mathbf{Dec}(\mathbf{id}, \mathsf{SK_{id}}, \mathsf{C})$: a user decryption algorithm takes an identity $\mathbf{id}$, the user secret key $\mathsf{SK_{id}}$ and a ciphertext C as inputs, and outputs either a message $\mathbf{m}$ or $\perp$ in the case of failure.

The lossy mode is a tuple of PPT algorithms $\{\mathsf{Setup_{lossy}}, \mathsf{Extract_{lossy}}, \mathsf{Enc}, \mathsf{Dec}\}$:

- $\mathbf{Setup_{lossy}}(\mathbf{id_{lossy}})$: a master key generation algorithm takes an identity $\mathbf{id_{lossy}}$ as input, and outputs a pair of lossy master public key and corresponding master secret key $(\mathsf{MPK_{lossy}}, \mathsf{MSK})$.
- $\mathbf{Extract_{lossy}}(\mathbf{id}, \mathsf{MPK_{lossy}}, \mathsf{MSK})$: a user secret key generation algorithm takes an identity $\mathbf{id}$, the master public key $\mathsf{MPK_{lossy}}$ and the master secret key MSK as inputs, and outputs either a user secret key $\mathsf{SK_{id}}$ when $\mathbf{id} \neq \mathbf{id_{lossy}}$ or $\perp$ when $\mathbf{id} = \mathbf{id_{lossy}}$.
- **Enc** and **Dec** algorithms are the same as those in the real mode.

An *Identity-based Lossy Encryption Scheme* should have the properties as below.

1. *Correctness on Keys for All* $\boldsymbol{id} \neq \boldsymbol{id}_{\mathsf{lossy}}$. For any $(\mathsf{MPK}, \mathsf{MSK})$ generated by $\mathbf{Setup_{real}}(1^k)$ or $\mathbf{Setup_{lossy}}(\mathbf{id_{lossy}})$, any $\mathsf{SK_{id}}$ generated by $\mathbf{Extract_{real/lossy}}(\mathbf{id}, \mathsf{MPK}, \mathsf{MSK})$, and any message $\mathbf{m}$, $\mathbf{Dec}(\mathbf{id}, \mathsf{SK_{id}}, \mathbf{Enc}(\mathbf{id}, \mathsf{MPK}, \mathbf{m})) = \mathbf{m}$.
2. *Lossiness of Encryption with Lossy Keys for* $\boldsymbol{id} = \boldsymbol{id}_{\mathsf{lossy}}$. For any lossy keys $\mathsf{MPK_{lossy}}$ generated by $\mathbf{Setup_{lossy}}(\mathbf{id_{lossy}})$ and any two messages $\mathbf{m}_0 \neq \mathbf{m}_1$, there is $\mathbf{Enc}(\mathbf{id_{lossy}}, \mathsf{MPK_{lossy}}, \mathbf{m}_0) \approx_s \mathbf{Enc}(\mathbf{id_{lossy}}, \mathsf{MPK_{lossy}}, \mathbf{m}_1)$. The advantage of $\mathcal{A}$ whose target is to distinguish those two ciphertexts (i.e. $Adv^{\mathsf{lossy}}_{\mathcal{A},\mathcal{IBLE}}$-ind) means the advantage of $\mathcal{A}$ in the standard IND-CPA game when the public key in the IND-CPA game is lossy.
3. *Indistinguishability Between Real Keys and Lossy Keys*. We use a game to describe this property.

   The advantage of the adversary is $Adv^{\mathsf{lossy\text{-}keys}}_{\mathcal{A},\mathcal{IBLE}} = |2Pr[b' = b] - 1|$. If for all PPT adversaries $\mathcal{A}$ we have that $Adv^{\mathsf{lossy}-keys}_{\mathcal{A},\mathcal{IBLE}}$ is a negligible function, then we say that the real keys generated in the real mode is indistinguishable with the lossy keys generated in the lossy mode.

Obviously the definition of IBLE implies IND-CPA security of IBE.

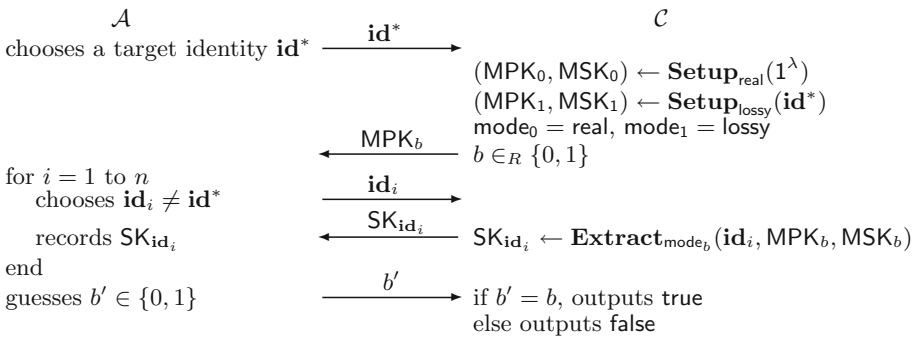

Fig. 1. Game of indistinguishability between real keys and lossy keys

3.1 Selective Opening Security

Here we prove that the notion of IBLE implies indistinguishability-based selective opening secure (IND-sID-SO) under chosen-plaintext attack. Firstly, we use a game to define IND-sID-SO. Let $\mathcal{D}_{\mathcal{M}}$ be any message sampler.

Init: The adversary outputs a target identity $\mathbf{id}^*$.

Setup: The challenger runs $\mathbf{Setup}(1^\lambda)$ and keeps the master secret key MSK. The challenger samples n messages $\{\mathbf{m}_0^i\}_{i=1..n}$ from $\mathcal{D}_{\mathcal{M}}$ and gets n ciphertexts by using algorithm $\mathbf{Enc}(\mathbf{id}^*, \mathsf{MPK}, \mathbf{m}_0^i)$, $i = 1..n$. The master public key MPK and the n ciphertexts $\mathbf{c}_1, \mathbf{c}_2, ..., \mathbf{c}_n$ are sent to the adversary.

Phase 1: The adversary issues queries $q_1, ..., q_k$ where the i-th query q_i is a query on $\mathbf{id}_i$. We require that $\mathbf{id}_i \neq \mathbf{id}^*$. The challenger responds by using algorithm $\mathsf{Extract}$ to obtain a private key $\mathsf{SK}_{\mathbf{id}_i}$ for $\mathbf{id}_i$, and sends $\mathsf{SK}_{\mathbf{id}_i}$ to the adversary. All queries may be made adaptively, that is, the adversary may ask q_i with knowledge of the challenger's responses to $q_1, ..., q_{i-1}$.

Open and Challenge: Once the adversary decides that Phase 1 is over it specifies a set J and sends it to the challenger. Then the challenger resamples n messages $\{\mathbf{m}_1^i\}_{i=1..n}$ from $\mathcal{D}_{\mathcal{M}}$ such that $\mathbf{m}_1^{[J]} = \mathbf{m}_0^{[J]}$. The challenger picks a random bit $b \in \{0,1\}$ and sends the adversary the messages $\mathbf{m}_b$ and the randomnesses $\mathbf{r}[J]$ used in ciphertexts $\mathbf{c}[J]$.

Phase 2: The adversary issues additional adaptive queries $q_{k+1}, ..., q_m$ where q_i is a private-key extraction query on $\mathbf{id}_i$, where $\mathbf{id}_i \neq \mathbf{id}^*$. The challenger responds the same as in **Phase 1**.

Guess: Finally, the adversary outputs a guess $b' \in \{0,1\}$ and wins if $b' = b$. The advantage of $\mathcal{A}$ in attacking an IBE scheme $\mathcal{E}$ is $Adv^{\mathsf{IND}}_{\mathcal{A},\mathcal{E},\mathcal{D}_{\mathcal{M}},n}\text{-}\mathsf{sID\text{-}SO}(\lambda) = |2 \cdot \Pr[b = b'] - 1|$. The probability is over the random bits used by the challenger and the adversary.

Definition 2. *We say that an IBE system $\mathcal{E}$ is* IND-sID-SO *secure if for all* IND-sID-SO *PPT adversaries $\mathcal{A}$ we have that $Adv^{\mathsf{IND\text{-}sID\text{-}SO}}_{\mathcal{A},\mathcal{E},\mathcal{M},n}(\lambda)$ is a negligible function.*

Theorem 1 (Identity-Based Lossy Encryption Implies IND-sID-SO Security). *Let λ be a security parameter. If $\mathcal{IBLE}$ is any identity-based lossy encryption scheme, then for all* IND-sID-SO *PPT adversaries $\mathcal{A}$, $Adv^{\mathsf{IND\text{-}sID\text{-}SO}}_{\mathcal{A},\mathcal{IBLE}}(\lambda)$ is a negligible function.*

Proof. At the beginning, we describe an algorithm called Opener. By the properties of IBLE, a ciphertext can be explained to any message with high probability. It means that, given a ciphertext C and a message $\mathbf{m}$, the algorithm Opener can find a set of random numbers r such that $\mathbf{Enc}(\mathbf{id}_{\mathsf{lossy}}, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{m}; r) = \mathsf{C}$ and outputs a random element of that set by traversing all values of the random number. The distribution of randomness is correct and the algorithm Opener is unbounded. Let $\mathcal{A}$ be any IND-sID-SO PPT adversary of $\mathcal{IBLE}$. The game sequence is as below.

$\mathbf{G_0}$: The IND-sID-SO original game as the definition.

$\mathbf{G_1}$: $\mathbf{Setup_{real}}$ in $\mathbf{G}_0$ is replaced by $\mathbf{Setup_{lossy}}$, and correspondingly, $\mathbf{Extra\text{-}ct_{real}}$ in $\mathbf{G}_0$ is replaced by $\mathbf{Extract_{lossy}}$.

$\mathbf{H_0}$: Based on $\mathbf{G}_1$, in the process of Open & Challenge, the challenger uses the algorithm $\mathsf{Opener}(\mathbf{id}^*, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{c}_i, \mathbf{m}^i_0)$ to generate the random numbers corresponding to the $|J|$ ciphertexts.

$\mathbf{H_k}$: We generalize $\mathbf{H}_0$ with a sequence of hybrid games. In this game, besides the true messages $\mathbf{m}_0$ sampled from $\mathcal{D}_{\mathcal{M}}$, the challenger randomly chooses another k messages $\mathbf{m'}^1_0, \mathbf{m'}^2_0, ..., \mathbf{m'}^k_0$ from the plaintext space $\mathcal{M}$ as fake messages and encrypts them in the lossy mode $(\mathbf{c'}_1, \mathbf{c'}_2, ..., \mathbf{c'}_k)$ to replace the first k ciphertexts. The challenger sends $\mathbf{c'}_1, ..., \mathbf{c'}_k, \mathbf{c}_{k+1}, ..., \mathbf{c}_n$ to the adversary in the Setup process. In the Open & Challenge process, the challenger still uses Opener to reveal the random numbers by the true messages $\mathbf{m}_0$, i.e. $\mathbf{r}_i = \mathsf{Opener}(\mathbf{id}^*, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{c'}_i, \mathbf{m}^i_0)$ when $i \leq k$ and $\mathbf{r}_i = \mathsf{Opener}(\mathbf{id}^*, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{c}_i, \mathbf{m}^i_0)$ when $i > k$.

$\mathbf{H_n}$: In this game, the n ciphertexts sent to $\mathcal{A}$ are all replaced by encryptions of other n fake messages $\{\mathbf{m'}^i_0\}_{i=1..n}$. The revealed random numbers are opened by $\mathsf{Opener}(\mathbf{id}^*, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{c'}_i, \mathbf{m}^i_0)$.

Then we will analyze this game sequence. First, the change of $\mathbf{G}_1$ is that the real keys $(\mathsf{MPK}_{\mathrm{real}}, \mathrm{SK}_{\mathbf{id}\_\mathrm{real}})$ are replaced by lossy keys $(\mathsf{MPK}_{\mathrm{lossy}}, \mathrm{SK}_{\mathbf{id}\_\mathrm{lossy}})$. Then if an adversary can distinguish $\mathbf{G}_0$ and $\mathbf{G}_1$, there is an adversary can distinguish the real keys and the lossy keys in $\mathcal{IBLE}$. It means that there is an PPT adversary $\mathcal{B}_1$ such that

$$\Pr[\mathbf{G}_0] - \Pr[\mathbf{G}_1] = Adv^{\mathsf{lossy\text{-}key}}_{\mathcal{B}_1,\mathcal{IBLE}}(\lambda).$$

By the third property of IBLE, $Adv^{\mathsf{lossy\text{-}key}}_{\mathcal{B}_1,\mathcal{IBLE}}(\lambda)$ is $negl(\lambda)$.

Second, the algorithm Opener in $\mathbf{H}_0$ uses the true message m_0^i and its corresponding ciphertext c_i, so the distribution of random number revealed by Opener is the same as in $\mathbf{G}_1$. Then there is

$$\Pr[\mathbf{G}_1] = \Pr[\mathbf{H}_0].$$

Third, compared with $\mathbf{H}_0$, the change of $\mathbf{H}_1$ is that the first ciphertext $\mathbf{c}'_1$ sent to $\mathcal{A}$ is encrypted by the fake message $\mathbf{m'}^1_0$ instead of the true message $\mathbf{m}^1_0$. However, $\mathbf{H}_1$ still uses the true message $\mathbf{m}^1_0$ to open the random number of the ciphertext $\mathbf{c}'_1$. In other words, $\mathbf{r}'_1 = \mathsf{Opener}(\mathbf{id}^*, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{c}'_1, \mathbf{m}^1_0)$, satisfies $\mathbf{Enc}(\mathbf{id}^*, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{m}^1_0; \mathbf{r}'_1) = \mathbf{c}'_1 = \mathbf{Enc}(\mathbf{id}^*, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{m'}^1_0; \mathbf{r}_1)$. Therefore, if there is an adversary can distinguish $\mathbf{H}_0$ from $\mathbf{H}_1$, there is an unbounded (because the algorithm Opener is unbounded) adversary $\mathcal{B}_2$ can distinguish the ciphertexts in $\mathcal{IBLE}$. That is

$$\Pr[\mathbf{H}_0] - \Pr[\mathbf{H}_1] = Adv^{\mathsf{lossy\text{-}ind}}_{\mathcal{B}_2,\mathcal{IBLE}}(\lambda).$$

$\mathbf{H}$ is a hybrid sequence, and the only difference between $\mathbf{H}_i$ and $\mathbf{H}_{i+1}$ is the ciphertext $\mathbf{c}'_{i+1}$. Therefore,

$$\Pr[\mathbf{H}_0] - \Pr[\mathbf{H}_n] = n \cdot Adv^{\mathsf{lossy\text{-}ind}}_{\mathcal{B}_2,\mathcal{IBLE}}(\lambda).$$

Because the distribution of ciphertexts encrypted by any messages in identity-based lossy encryption are statistically close, $Adv^{\mathsf{lossy\text{-}ind}}_{\mathcal{B}_2,\mathcal{IBLE}}(\lambda)$ is $negl(\lambda)$.

Last, in $\mathbf{H}_n$, all n ciphertexts $\mathbf{c}'_1, \mathbf{c}'_2, ..., \mathbf{c}'_n$ are encrypted by fake messages $\mathbf{m'}^1_0, \mathbf{m'}^2_0, ..., \mathbf{m'}^n_0$ which has no information of the true messages $\mathbf{m}^1_0, \mathbf{m}^2_0, ..., \mathbf{m}^n_0$. So the adversary can just randomly guess b. That is,

$$\Pr[\mathbf{H}_n] = \frac{1}{2}.$$

Above all, $Adv^{\mathsf{ind\text{-}sid\text{-}so}}_{\mathcal{A},\mathcal{IBLE},\mathcal{M},n}(\lambda) = |2Pr[\mathbf{G}_0] - 1| \leq 2 \cdot Adv^{\mathsf{lossy\text{-}key}}_{\mathcal{B}_1,\mathcal{IBLE}}(\lambda) + 2n \cdot Adv^{\mathsf{lossy\text{-}ind}}_{\mathcal{B}_2,\mathcal{IBLE}}(\lambda) = negl(\lambda)$ states that identity-based lossy encryption implies $\mathsf{IND\text{-}sID\text{-}SO}$ secure. □

3.2 Construction from LWE

The dual Regev's cryptosystem was proposed to construct IBE with random oracle in [16]. Then, Agrawal, Boneh and Boyen [1] used it to construct an IBE scheme in the standard model. Before constructing IBLE, we construct a dual Regev type lossy encryption to get some inspiration.

3.2.1 Construction of Dual Regev Type Lossy Encryption

We construct a lossy encryption based on dual Regev's cryptosystem. However, the process of encryption is different from dual Regev's cryptosystem. We only

$\mathbf{KeyGen_{real}}(1^\lambda)$	$\mathbf{KeyGen_{loss}}(1^\lambda)$	$\mathbf{Enc}(\mathsf{PK}, \mathbf{m})$	$\mathbf{Dec}(\mathsf{SK}, \mathsf{C})$
$\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$	$\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{m\times k}$	$\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$	$(\mathbf{c}_1, \mathbf{c}_2) := \mathsf{C}$
$\mathbf{T} \xleftarrow{\$} \mathcal{D}_{\mathbb{Z},r}^{m\times l}$	$\mathbf{C} \xleftarrow{\$} \mathbb{Z}_q^{k\times n}$	$\mathbf{e} \longleftarrow \mathcal{D}_{\mathbb{Z},\beta q}^m$	$\mathbf{m}' := \mathbf{c}_2 - \mathsf{SK}^{\mathsf{t}}\mathbf{c}_1$
$\mathsf{PK}_{\mathsf{real}} := (\mathbf{A}, \mathbf{AT})$	$\mathbf{Z} \longleftarrow \mathcal{D}_{\mathbb{Z},\alpha q}^{m\times n}$	$(\mathbf{PK}_1, \mathbf{PK}_2) := \mathsf{PK}$	$\mathbf{m} := decode(\mathbf{m}')$
$\mathsf{SK} := \mathbf{T}$	$\mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{l\times n}$	$\mathbf{c}_1 := \mathbf{PK}_1^t\mathbf{s} + \mathbf{e}$	return $\mathbf{m}$
return $(\mathsf{PK}_{\mathsf{real}}, \mathsf{SK})$	$\mathsf{PK}_{\mathsf{loss}} := ((\mathbf{BC} + \mathbf{Z})^t, \mathbf{U}^t)$	$\mathbf{c}_2 := \mathbf{PK}_2^t\mathbf{s} + \mathbf{m}\lfloor\frac{q}{2}\rceil$	
	return $(\mathsf{PK}_{\mathsf{loss}}, \perp)$	return $(\mathbf{c}_1, \mathbf{c}_2)$	

Fig. 2. Construction of dual Regev type lossy encryption

choose the noisy vector $\mathbf{e}$ once in our construction instead of twice in the original cryptosystem. The message space $\mathcal{M}$ is $\{0,1\}^l$, and the concrete construction is as follows.

The $decode(\mathbf{m}')$ means that for every element m_i' of the vector $\mathbf{m}'$, outputs 0 if m_i' is closer to 0 than to $\lfloor\frac{q}{2}\rceil$ modulo q, otherwise outputs 1.

Parameters. Consider requirements of correct decryption, and the lossiness and so on, parameters are as below. $m \geq 2n\log q, k\log q \leq n - 2\lambda + 2, l \leq (k - 2\log(1/\varepsilon) - O(1))/\log q, q \geq 5rm, r \geq \omega(\sqrt{\log m}), \beta \leq 1/(r\sqrt{m}\omega(\sqrt{\log m})), \beta q > O(2\sqrt{n}), \frac{\alpha}{\beta} = negl(\lambda)$. To satisfy these requirements, q should be super-polynomial of the secure parameter λ.

Then, we show this scheme fulfills the properties of lossy encryption.

1. *Correctness on Real Keys.* For all $(\mathsf{PK}_{\mathsf{real}}, \mathsf{SK})$ generated by $\mathbf{KeyGen_{real}}(1^\lambda)$ and all message $\mathbf{m}$,

$$\begin{aligned}
\mathbf{Dec}(\mathsf{SK}, \mathbf{Enc}(\mathsf{PK}_{\mathsf{real}}, \mathbf{m})) &= \mathbf{Dec}(\mathbf{T}, \mathbf{Enc}((\mathbf{A}, \mathbf{AT}), \mathbf{m})) \\
&= \mathbf{Dec}(\mathbf{T}, (\mathbf{A}^t\mathbf{s} + \mathbf{e}, \mathbf{T}^t\mathbf{A}^t\mathbf{s} + \mathbf{m}\lfloor\frac{q}{2}\rceil)) \\
&= decode(\mathbf{T}^t\mathbf{A}^t\mathbf{s} + \mathbf{m}\lfloor\frac{q}{2}\rceil - \mathbf{T}^t\mathbf{A}^t\mathbf{s} - \mathbf{T}^t\mathbf{e}) \\
&= decode(\mathbf{m}\lfloor\frac{q}{2}\rceil - \mathbf{T}^t\mathbf{e}) \\
&= \mathbf{m}
\end{aligned}$$

   By Lemma 5, the algorithm $decode()$ will get the correct message with overwhelming probability.
2. *Lossiness of Encryption with Lossy Keys.*

$$\begin{aligned}
\mathbf{Enc}(\mathsf{PK}_{\mathsf{loss}}, \mathbf{m}) &= \mathbf{Enc}(((\mathbf{BC} + \mathbf{Z})^t, \mathbf{U}^t), \mathbf{m}) \\
&= ((\mathbf{BC} + \mathbf{Z})\mathbf{s} + \mathbf{e}, \mathbf{Us} + \mathbf{m}\lfloor\frac{q}{2}\rceil)
\end{aligned}$$

   By Lemma 4, $\tilde{H}_\infty(\mathbf{s}|(\mathbf{BC} + \mathbf{Z})\mathbf{s} + \mathbf{e}) \geq n$. Because $l \leq (k - 2\log(1/\varepsilon) - O(1))/\log q$, and by Lemma 2, given $(\mathbf{BC} + \mathbf{Z})\mathbf{s} + \mathbf{e}$, $\mathbf{Us}$ is ε-close to $\mathcal{U}(\mathbb{Z}_q^l)$.

When $\varepsilon = negl(\lambda)$, $\mathbf{Us} \approx_s \mathcal{U}(\mathbb{Z}_q^l)$ given $(\mathbf{BC}+\mathbf{Z})\mathbf{s}+\mathbf{e}$. Therefore, for any $\mathbf{m} \in \mathcal{M}$, $(\mathbf{Us}+\mathbf{m}\lfloor\frac{q}{2}\rceil)$ is statistically close to $\mathcal{U}(\mathbb{Z}_q^l)$, given $(\mathbf{BC}+\mathbf{Z})\mathbf{s}+\mathbf{e}$, i.e. for any lossy keys $\mathsf{PK}_{\mathsf{loss}}$ generated by $\mathbf{KeyGen}_{\mathbf{loss}}(1^\lambda)$ and any two messages $\mathbf{m}_0 \neq \mathbf{m}_1$, $\mathbf{Enc}(\mathsf{PK}_{\mathsf{loss}}, \mathbf{m}_0) \approx_s \mathbf{Enc}(\mathsf{PK}_{\mathsf{loss}}, \mathbf{m}_1)$ holds.

3. *Indistinguishability Between Real Public Key and Lossy Public Key.* $\mathsf{PK}_{\mathsf{real}}$ is $(\mathbf{A}, \mathbf{AT})$, and $\mathsf{PK}_{\mathsf{loss}}$ is $((\mathbf{BC}+\mathbf{Z})^t, \mathbf{U}^t)$. Because $m \geq 2n\log q$, by Lemma 3, $(\mathbf{A}^t, (\mathbf{TA})^t) \approx_s (\mathbf{U}_1, \mathbf{U}_2), \mathbf{U}_1 \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$ and $\mathbf{U}_2 \xleftarrow{\$} \mathbb{Z}_q^{l\times n}$. Under the hardness of LWE, $(\mathbf{BC}+\mathbf{Z}, \mathbf{U}) \approx_c (\mathbf{U}_1, \mathbf{U}_2)$. Therefore, $(\mathbf{BC}+\mathbf{Z}, \mathbf{U}) \approx_c (\mathbf{A}^t, (\mathbf{TA})^t)$, i.e. $\mathsf{PK}_{\mathsf{real}}$ and $\mathsf{PK}_{\mathsf{loss}}$ are computationally indistinguishable.

Lemma 5 ([16]). *Let $q \geq 5rm$, let $\beta \leq 1/(r\sqrt{m}\cdot\omega(\sqrt{\log n}))$. Then $\mathbf{Dec}(\mathsf{SK}, \mathsf{C})$ in Fig. 2 decrypts correctly with overwhelming probability (over the random choices of $\mathbf{KeyGen}_{\mathbf{real}}(1^\lambda)$ and $\mathbf{Enc}(\mathsf{PK}, \mathbf{m})$).*

3.2.2 Construction of IBLE

Before describing the construction, we will introduce some algorithms which will be used.

Lemma 6 ([1]). *Let $q \geq 3$ be odd and $m := \lceil 6n\log q\rceil$. There is a probabilistic polynomial-time algorithm $\mathsf{TrapGen}(q, n)$ that outputs a pair ($\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{S} \in \mathbb{Z}^{m\times m}$) such that $\mathbf{A}$ is statistically close to a uniform matrix in $\mathbb{Z}_q^{n\times m}$ and $\mathbf{S}$ is a basis for $\Lambda_q^\perp(\mathbf{A})$ satisfying $\|\tilde{\mathbf{S}}\| \leq O(\sqrt{n\log q})$ and $\|\mathbf{S}\| \leq O(n\log q)$ with all but negligible probability in n.*

Lemma 7 ([1]). *Let $q > 2$, $m > 2n\log q$ and $\sigma > \|\tilde{\mathbf{T}}_A\|\cdot\omega(\sqrt{\log(m+m_1)})$. There is a probabilistic polynomial-time algorithm $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{M}_1, \mathbf{T}_A, \mathbf{u}, \sigma)$ that, given a rank n matrix $\mathbf{A}$ in $\mathbb{Z}_q^{n\times m}$, a matrix $\mathbf{M}_1$ in $\mathbb{Z}_q^{n\times m_1}$, a "short" basis $\mathbf{T}_A$ of $\Lambda_q^\perp(\mathbf{A})$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, outputs a vector $\mathbf{e} \in \mathbb{Z}^{m+m-1}$ distributed statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{F}_1),\sigma}$ where $\mathbf{F}_1 := (\mathbf{A}\|\mathbf{M}_1)$.*

Lemma 8 ([1]). *Let $q > 2$, $m > n$ and $\sigma > \|\tilde{\mathbf{T}}_B\|\cdot\sqrt{m}\cdot\omega(\log m)$. There is a probabilistic polynomial-time algorithm $\mathsf{SampleRight}(\mathbf{A}, \mathbf{B}, \mathbf{R}, \mathbf{T}_B, \mathbf{u}, \sigma)$ that, given a matrix $\mathbf{A}$ in $\mathbb{Z}_q^{n\times m}$, a rank n matrix $\mathbf{B}$ in $\mathbb{Z}_q^{n\times m}$, a uniform random matrix $\mathbf{R} \in \{-1, 1\}^{m\times m}$, a basis $\mathbf{T}_B$ of $\Lambda_q^\perp(\mathbf{B})$ and a vector $\mathbf{u} \in \mathbb{Z}_q^n$, outputs a vector $\mathbf{e} \in \mathbb{Z}^{2m}$ distributed statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{u}}(\mathbf{F}_2),\sigma}$ where $\mathbf{F}_2 := (\mathbf{A}\|\mathbf{AR}+\mathbf{B})$.*

If the input vector $\mathbf{u}$ is replaced by a matrix $\mathbf{U}$, the algorithms of $\mathsf{SampleLeft}$ and $\mathsf{SampleRight}$ still work normally and the outputs of them are matrices. We will use the matrix version of them in the construction.

Next we prove an extension of Lemma 4 using the similar method of [6], which is important to our construction of IBLE.

Lemma 9. *There is a distribution Lossy such that $\bar{\mathbf{A}} \leftarrow \mathsf{Lossy} \approx_c \mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{2m\times n}$ and given $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, and $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z},\beta q}^{2m\times n}$, $\tilde{H}_\infty^\epsilon(\mathbf{s}|\bar{\mathbf{A}}, \bar{\mathbf{A}}\mathbf{s}+\mathbf{x}) \geq n$, where $\epsilon = negl(\lambda)$. Lossy is as follows.*

- *Choose* $\mathbf{B} \xleftarrow{\$} \mathbb{Z}_q^{m\times k}$, $\mathbf{C} \xleftarrow{\$} \mathbb{Z}_q^{k\times n}$, $\mathbf{Z} \leftarrow \mathcal{D}_{\mathbb{Z},\alpha q}^{m\times n}$, *and* $\mathbf{R} \xleftarrow{\$} \{1,-1\}^{m\times m}$, *where* $\frac{\alpha}{\beta} = negl(\lambda)$, $k\log q \le n - 2\lambda + 2$, *and* $n\log q \le m - 2\lambda + 2$.
- *Let* $\bar{\mathbf{A}} = \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C} + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}$.
- *Output* $\bar{\mathbf{A}}$.

Proof. 1. $\bar{\mathbf{A}} \approx_c \mathbf{U} \xleftarrow{\$} \mathbb{Z}_q^{2m\times n}$:

$$(\mathbf{BC}+\mathbf{Z}, \mathbf{R}^t(\mathbf{BC}+\mathbf{Z})) \overset{(1)}{\approx}_c (\mathbf{U}_1, \mathbf{R}^t\mathbf{U}_1) \overset{(2)}{\approx}_c (\mathbf{U}_1, \mathbf{U}_2), \qquad \mathbf{U}_1, \mathbf{U}_2 \xleftarrow{\$} \mathbb{Z}_q^{m\times n}$$

- Under the hardness of LWE assumption, approximate formula (1) holds.
- Let $\mathbf{r}_i$ be the i-th column of $\mathbf{R}$ where $\mathbf{r}_i \leftarrow \{-1,1\}^m$ is uniformly random. Because $n\log q \le m - 2\lambda + 2$, by Lemma 2, $(\mathbf{U}_1^t, \mathbf{U}_1^t\mathbf{r}_i)$ is statistically close to the uniform distribution over $\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$. Because the columns of $\mathbf{R} = [\mathbf{r}_1\ \mathbf{r}_2\ \ldots\ \mathbf{r}_m]$ are sampled independently, $(\mathbf{U}_1^t, \mathbf{U}_1^t\mathbf{R})$ is statistically close to the uniform distribution over $\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n\times m}$. Taking the transpose, (2) holds.

2. $\tilde{H}_\infty^\epsilon(\mathbf{s}|\bar{\mathbf{A}}, \bar{\mathbf{A}}\mathbf{s}+\mathbf{x}) \ge n$, where $\epsilon = negl(\lambda)$: Let $\mathbf{s}_0 \xleftarrow{\$} \{0,1\}^n$, $\mathbf{s}_1 \xleftarrow{\$} \mathbb{Z}_q^n$, then, think of $\mathbf{s} = \mathbf{s}_0 + \mathbf{s}_1$. Because $\tilde{H}_\infty^\epsilon(\mathbf{s}|\bar{\mathbf{A}}\mathbf{s}+\mathbf{e}) \ge \tilde{H}_\infty^\epsilon(\mathbf{s}_0|\bar{\mathbf{A}}\mathbf{s}+\mathbf{e})$, we will consider $\tilde{H}_\infty^\epsilon(\mathbf{s}_0|\bar{\mathbf{A}}\mathbf{s}+\mathbf{e})$.

$$\begin{aligned}\bar{\mathbf{A}}\mathbf{s}+\mathbf{e} &= \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_0 + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_0 + \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_1 + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_1 + \mathbf{e}\\ &\overset{(1)}{\approx}_s \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_0 + \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_1 + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_1 + \mathbf{e}\\ &\overset{(2)}{\approx}_s \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{u}_0 + \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_1 + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_1 + \mathbf{e}\end{aligned}$$

- Since $\frac{\alpha}{\beta} = negl(\lambda)$, each element of $\mathbf{Z}\mathbf{s}_0$ is negligibly small compared to the corresponding element of $\mathbf{e}$. And $\mathbf{R}^t\mathbf{Z}\mathbf{s}_0$ is polynomial number of adds operating on elements of $\mathbf{Z}\mathbf{s}_0$ where the elements of $\mathbf{R}$ are uniformly random chosen from $\{-1,1\}$, so each element of $\mathbf{R}^t\mathbf{Z}\mathbf{s}_0$ is negligibly small compared to the corresponding element of $\mathbf{e}$. Therefore, $\mathbf{e} + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_0 \approx_s \mathbf{e}$, and the approximate formula (1) holds. It means that their statistical distance is some $\epsilon_1 = negl(\lambda)$.
- Since $\mathbf{s}_0 \xleftarrow{\$} \{0,1\}^n$ and $k\log q \le n - 2\lambda + 2$, by Lemma 2, the approximate formula (2) holds where $\mathbf{u}_0 \xleftarrow{\$} \mathbb{Z}_q^k$. It means that their statistical distance is some $\epsilon_2 = negl(\lambda)$.

Then, for $\epsilon = \epsilon_1 + \epsilon_2 = negl(\lambda)$,

$$\begin{aligned}&\tilde{H}_\infty^\epsilon(\mathbf{s}_0|\begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_0 + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_0 + \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_1 + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_1 + \mathbf{e})\\ \ge\ &\tilde{H}_\infty^\epsilon(\mathbf{s}_0|\begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_0 + \begin{bmatrix}\mathbf{B}\\ \mathbf{R}^t\mathbf{B}\end{bmatrix}\mathbf{C}\mathbf{s}_1 + \begin{bmatrix}\mathbf{Z}\\ \mathbf{R}^t\mathbf{Z}\end{bmatrix}\mathbf{s}_1 + \mathbf{e})\end{aligned}$$

$$\geq \tilde{H}_{\infty}^{\epsilon}(\mathbf{s}_0 | \begin{bmatrix} \mathbf{B} \\ \mathbf{R}^t\mathbf{B} \end{bmatrix} \mathbf{u}_0 + \begin{bmatrix} \mathbf{B} \\ \mathbf{R}^t\mathbf{B} \end{bmatrix} \mathbf{C}\mathbf{s}_1 + \begin{bmatrix} \mathbf{Z} \\ \mathbf{R}^t\mathbf{Z} \end{bmatrix} \mathbf{s}_1 + \mathbf{e})$$
$$\overset{(3)}{=} \tilde{H}_{\infty}(\mathbf{s}_0)$$
$$= n$$

Because each of $\mathbf{B}, \mathbf{R}, \mathbf{C}, \mathbf{Z}, \mathbf{u}_0, \mathbf{s}_1, \mathbf{e}$ is independent of $\mathbf{s}_0$, (3) holds. □

Next we describe our construction of IBLE from LWE inspired by the construction of IBE in [1]. There are some changes compared with [1]. In [1], there are errors chosen from gaussian distribution in both two ciphertexts. And the error used in the second ciphertext consists of two parts, one part $\mathbf{e}$ is from gaussian distribution, and the other is $\mathbf{R}^t\mathbf{e}$. However, in our construction, only the first ciphertext needs an error from gaussian distribution. The concrete construction is as Fig. 3. $\mathbf{H} : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \times n}$ is an encoding function constructed in [1]. This encoding function has the property that, for any two distinct inputs $\mathbf{id}_1$ and $\mathbf{id}_2$, the difference between the outputs $\mathbf{H}(\mathbf{id}_1)$ and $\mathbf{H}(\mathbf{id}_2)$ is never singular.

$\mathbf{Setup_{real}}(1^\lambda)$

$(\mathbf{A}, \mathbf{S}_A) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{m \times m} \leftarrow \mathsf{TrapGen}(q, n)$
$\mathbf{A}_1 \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times m}$, $\mathbf{A}_2 \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times m}$
$\mathbf{Y} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times l}$
$\mathsf{MPK} := (\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{Y})$
$\mathsf{MSK} := \mathbf{S}_A$
return $(\mathsf{MPK}, \mathsf{MSK})$

$\mathbf{Setup_{lossy}}(1^\lambda, \mathbf{id}^*)$

$\mathbf{B} \overset{\$}{\leftarrow} \mathbb{Z}_q^{m \times k}$, $\mathbf{C} \overset{\$}{\leftarrow} \mathbb{Z}_q^{k \times n}$, $\mathbf{Z} \leftarrow \mathcal{D}_{\mathbb{Z}, \alpha q}^{m \times n}$
$\mathbf{A} := (\mathbf{BC} + \mathbf{Z})^t$
$\mathbf{R} \overset{\$}{\leftarrow} \{-1, 1\}^{m \times m}$, $\mathbf{Y} \overset{\$}{\leftarrow} \mathbb{Z}_q^{n \times l}$
$(\mathbf{A}_2, \mathbf{S}_{A_2}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^{m \times m} \leftarrow \mathsf{TrapGen}(q, n)$
$\mathbf{A}_1 := \mathbf{AR} - \mathbf{H}(\mathbf{id}^*)\mathbf{A}_2$
$\mathsf{MPK} := (\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{Y})$
$\mathsf{MSK} := (\mathbf{S}_{A_2}, \mathbf{R})$
return $(\mathsf{MPK}, \mathsf{MSK})$

$\mathbf{Extract_{real}}(\mathbf{id}, \mathsf{MPK}, \mathsf{MSK})$

$(\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{Y}) := \mathsf{MPK}$
$\mathbf{S}_A := \mathsf{MSK}$
$\mathbf{M} := \mathbf{A}_1 + \mathbf{H}(\mathbf{id})\mathbf{A}_2$
$\mathbf{X_{id}} \leftarrow \mathsf{SampleLeft}(\mathbf{A}, \mathbf{M}, \mathbf{S}_A, \mathbf{Y}, \sigma)$
$\mathsf{SK_{id}} := \mathbf{X_{id}}$
return $\mathsf{SK_{id}}$

$\mathbf{Extract_{lossy}}(\mathbf{id}, \mathsf{MPK}, \mathsf{MSK})$

$(\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{Y}) := \mathsf{MPK}$
$(\mathbf{S}_{A_2}, \mathbf{R}) := \mathsf{MSK}$
$\mathbf{M} := \mathbf{A}_1 + \mathbf{H}(\mathbf{id})\mathbf{A}_2 - \mathbf{AR}$
$\mathbf{X_{id}} \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{M}, \mathbf{R}, \mathbf{S}_{A_2}, \mathbf{Y}, \sigma)$
$\mathsf{SK_{id}} := \mathbf{X_{id}}$
return $\mathsf{SK_{id}}$

$\mathbf{Enc}(\mathbf{id}, \mathsf{MPK}, \mathbf{m})$

$\mathbf{s} \overset{\$}{\leftarrow} \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}, \beta q}^{2m}$
$(\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{Y}) := \mathsf{MPK}$
$\mathbf{A}(\mathbf{id}) := (\mathbf{A} \| \mathbf{A}_1 + \mathbf{H}(\mathbf{id})\mathbf{A}_2)$
$\mathbf{c_1} := \mathbf{A}(\mathbf{id})^t\mathbf{s} + \mathbf{e}$
$\mathbf{c_2} := \mathbf{Y}^t\mathbf{s} + \mathbf{m}\lfloor \frac{q}{2} \rceil$
return $(\mathbf{c}_1, \mathbf{c}_2)$

$\mathbf{Dec}(\mathsf{MPK}, \mathsf{SK_{id}}, \mathsf{C})$

$(\mathbf{c}_1, \mathbf{c}_2) := \mathsf{C}$
$(\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{Y}) := \mathsf{MPK}$
$\mathbf{m}' := \mathbf{c}_2 - \mathsf{SK}_{\mathbf{id}}^{\mathsf{t}}\mathbf{c}_1$
$\mathbf{m} := decode(\mathbf{m}')$
return $\mathbf{m}$

Fig. 3. Construction of identity-based lossy encryption

The algorithm *decode*() is the same in Sect. 3.2.1. In the algorithm $\mathbf{Extract}_{\mathbf{lossy}}(\mathbf{id}, \mathsf{MPK}, \mathsf{MSK})$, the matrix $\mathbf{M}$ is $(\mathbf{H}(\mathbf{id}) - \mathbf{H}(\mathbf{id}^*))\mathbf{A}_2$. When $\mathbf{id} \neq \mathbf{id}^*$, the trapdoor $\mathbf{S}_{A_2}$ of $\Lambda_q^{\perp}(\mathbf{A}_2)$ is also a trapdoor for $\Lambda_q^{\perp}(\mathbf{M})$ since $(\mathbf{H}(\mathbf{id}) - \mathbf{H}(\mathbf{id}^*))$ is non-singular.

Parameters. Consider requirements of correct decryption, and the lossiness and so on, parameters are as below, $m = \lceil 6n \log q \rceil, l \log q \leq k - 2\lambda + 2, k \log q \leq n - 2\lambda + 2, n \log q \leq m - 2\lambda + 2, q \geq 10\sigma m, \sigma \geq O(\sqrt{n \log qm})\omega(\log m), \beta \leq 1/(\sigma\sqrt{2m}\omega(\sqrt{\log 2m})), \frac{\alpha}{\beta} = negl(\lambda), \beta q > O(2\sqrt{n}), \alpha q > O(2\sqrt{n})$. To satisfy these requirements, q should be super-polynomial of the secure parameter λ.

Then, we show this scheme fulfills the properties of IBLE.

1. *Correctness on Keys for All* $\boldsymbol{id} \neq \boldsymbol{id}_{\mathsf{lossy}}$. For all $(\mathsf{MPK}, \mathsf{MSK})$ generated by $\mathbf{Setup}_{\mathbf{real}}(1^k)$ and $\mathbf{Setup}_{\mathbf{lossy}}(id_{\mathsf{lossy}})$, all $\mathsf{SK}_{\mathbf{id}}$ generated by $\mathbf{Extract}_{\mathbf{real},\mathbf{lossy}}(\mathbf{id}, \mathsf{MPK}, \mathsf{MSK})$, and all messages $\mathbf{m}$,

$$
\begin{aligned}
&\mathbf{Dec}(\mathbf{id}, \mathsf{SK}_{\mathbf{id}}, \mathbf{Enc}(\mathbf{id}, \mathsf{MPK}, \mathbf{m})) \\
&= \mathbf{Dec}(\mathbf{id}, \mathsf{SK}_{\mathbf{id}}, \mathbf{Enc}((\mathbf{A}, \mathbf{A}_1, \mathbf{A}_2, \mathbf{Y}), \mathbf{m})) \\
&= \mathbf{Dec}(\mathbf{id}, \mathsf{SK}_{\mathbf{id}}, ((\mathbf{A} \| \mathbf{A}_1 + \mathbf{H}(\mathbf{id})\mathbf{A}_2)^t \mathbf{s} + \mathbf{e}, \mathbf{Y}^t \mathbf{s} + \mathbf{m} \lfloor \frac{q}{2} \rceil)) \\
&= decode(\mathbf{Y}^t \mathbf{s} + \mathbf{m} \lfloor \frac{q}{2} \rceil - \mathsf{SK}_{\mathbf{id}}^t \mathbf{A}(\mathbf{id})^t \mathbf{s} - \mathsf{SK}_{\mathbf{id}}^t \mathbf{e}) \\
&\overset{(1)}{=} decode(\mathbf{Y}^t \mathbf{s} + \mathbf{m} \lfloor \frac{q}{2} \rceil - \mathbf{Y}^t \mathbf{s} - \mathsf{SK}_{\mathbf{id}}^t \mathbf{e}) \\
&= decode(\mathbf{m} \lfloor \frac{q}{2} \rceil - \mathsf{SK}_{\mathbf{id}}^t \mathbf{e}) \\
&= \mathbf{m}
\end{aligned}
$$

   Because $\mathsf{SK}_{\mathbf{id}}$ is generated by $\mathsf{SampleLeft}$, $\mathsf{SK}_{\mathbf{id}}^t = \mathbf{Y}^t$, and (1) holds. By Lemma 5, the algorithm *decode*() will get the correct message with overwhelming probability.
2. *Lossiness of Encryption with Lossy Keys for* $\boldsymbol{id} = \boldsymbol{id}_{\mathsf{lossy}}$.

$$
\begin{aligned}
&\mathbf{Enc}(\mathbf{id}, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{m}) \\
&= \mathbf{Enc}(\mathbf{id}, (\mathbf{BC} + \mathbf{Z})^t, (\mathbf{BC} + \mathbf{Z})^t \mathbf{R} - \mathbf{H}(\mathbf{id})\mathbf{A}_2, \mathbf{A}_2, \mathbf{Y}), \mathbf{m}) \\
&= (\begin{bmatrix} \mathbf{BC} + \mathbf{Z} \\ ((\mathbf{BC} + \mathbf{Z})^t \mathbf{R} - \mathbf{H}(\mathbf{id})\mathbf{A}_2 + \mathbf{H}(\mathbf{id})\mathbf{A}_2)^t \end{bmatrix} \mathbf{s} + \mathbf{e}, \mathbf{Y}^t \mathbf{s} + \mathbf{m} \lfloor \frac{q}{2} \rceil) \\
&= (\begin{bmatrix} \mathbf{BC} + \mathbf{Z} \\ \mathbf{R}^t(\mathbf{BC} + \mathbf{Z}) \end{bmatrix} \mathbf{s} + \mathbf{e}, \mathbf{Y}^t \mathbf{s} + \mathbf{m} \lfloor \frac{q}{2} \rceil) \\
&= ((\begin{bmatrix} \mathbf{B} \\ \mathbf{R}^t \mathbf{B} \end{bmatrix} \mathbf{C} + \begin{bmatrix} \mathbf{Z} \\ \mathbf{R}^t \mathbf{Z} \end{bmatrix}) \mathbf{s} + \mathbf{e}, \mathbf{Y}^t \mathbf{s} + \mathbf{m} \lfloor \frac{q}{2} \rceil)
\end{aligned}
$$

   Let $\mathbf{A}' = \begin{bmatrix} \mathbf{B} \\ \mathbf{R}^t \mathbf{B} \end{bmatrix} \mathbf{C} + \begin{bmatrix} \mathbf{Z} \\ \mathbf{R}^t \mathbf{Z} \end{bmatrix}$. Because the parameters satisfy the requirements of Lemma 9, we know that $\tilde{H}_{\infty}(\mathbf{s} | \mathbf{A}'\mathbf{s} + \mathbf{e}) \geq n$. Then because

$l \leq (k - 2\log(1/\varepsilon) - O(1))/\log q$, and by Lemma 2, given $\mathbf{A}'\mathbf{s} + \mathbf{e}$, $\mathbf{Y}^t\mathbf{s}$ is ε-close to $\mathcal{U}(\mathbb{Z}_q^l)$. When $\varepsilon = negl(\lambda)$, $\mathbf{Y}^t\mathbf{s} \approx_s \mathcal{U}(\mathbb{Z}_q^l)$ given $\mathbf{A}'\mathbf{s} + \mathbf{e}$. Therefore, for any $\mathbf{m} \in \mathcal{M}$, $(\mathbf{Y}^t\mathbf{s} + \mathbf{m}\lfloor\frac{q}{2}\rceil)$ is statistically close to $\mathcal{U}(\mathbb{Z}_q^l)$, given $\mathbf{A}'\mathbf{s} + \mathbf{e}$, i.e. for the lossy identity $\mathbf{id}$, any lossy keys $\mathsf{MPK}_{\mathsf{lossy}}$ generated by $\mathbf{Setup}_{\mathbf{lossy}}(\mathbf{id})$ and any two messages $\mathbf{m}_0 \neq \mathbf{m}_1$, there is $\mathbf{Enc}(\mathbf{id}, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{m}_0) \approx_s \mathbf{Enc}(\mathbf{id}, \mathsf{MPK}_{\mathsf{lossy}}, \mathbf{m}_1)$.

3. *Indistinguishability Between Real Keys and Lossy Keys*. We use a game sequence to prove this property.
$\mathbf{G}_0$: This is the original game from the definition of the third property of identity-based lossy encryption described as Fig. 1.
$\mathbf{G}_1$: In $\mathbf{G}_0$, the master public key MPK_1 generated by the challenger is $((\mathbf{BC} + \mathbf{Z})^t, (\mathbf{BC} + \mathbf{Z})^t\mathbf{R} - \mathbf{H}(\mathbf{id}^*)\mathbf{A}_2, \mathbf{A}_2, \mathbf{Y})$. In $\mathbf{G}_1$, we use a random matrix $\mathbf{U}$ in $\mathbb{Z}_q^{n\times m}$ to replace $(\mathbf{BC} + \mathbf{Z})^{\mathbf{t}}$. It means that MPK_1 in this game is $(\mathbf{U}, \mathbf{UR} - \mathbf{H}(\mathbf{id}^*)\mathbf{A}_2, \mathbf{A}_2, \mathbf{Y})$. The remainder of the game is unchanged.

Suppose there is an adversary $\mathcal{A}$ has non-negligible advantage in distinguishing $\mathbf{G}_0$ and $\mathbf{G}_1$. Then we use $\mathcal{A}$ to construct an algorithm $\mathcal{S}$ as Fig. 4 to distinguish a random matrix $\mathbf{U}$ and an LWE instance $((\mathbf{BC} + \mathbf{Z})^t)$. In words, the algorithm $\mathcal{S}$ proceeds as follows. $\mathcal{S}$ requests the oracle $\mathcal{O}$ which outputs a random matrix $\mathbf{U}$ or an LWE instance $(\mathbf{BC} + \mathbf{Z})^t$, and receives a matrix $\mathbf{A}'$. After receiving the target identity $\mathbf{id}^*$ sent by $\mathcal{A}$, $\mathcal{S}$ works as the $\mathbf{Setup}_{\mathbf{real}}$ algorithm in Fig. 3 to generate the real keys $\mathsf{MPK}_0, \mathsf{MSK}_0$, and uses $\mathbf{A}'$ to generate the lossy keys $\mathsf{MPK}_1, \mathsf{MSK}_1$. Then $\mathcal{S}$ randomly chooses b from $\{0, 1\}$ and sends MPK_b to $\mathcal{A}$. Then $\mathcal{A}$ issues private key extraction queries on $\mathbf{id}_i$ where $\mathbf{id}_i \neq \mathbf{id}^*$.

We argue that when the oracle $\mathcal{O}$ outputs an LWE instance $(\mathbf{BC} + \mathbf{Z})^t$, MPK_b is distributed exactly as in $\mathbf{G}_0$. If $b = 0$, MPK_0 is the real public key, and else $b = 1$, MPK_1 is $((\mathbf{BC} + \mathbf{Z})^t, (\mathbf{BC} + \mathbf{Z})^t\mathbf{R} - \mathbf{H}(\mathbf{id}^*)\mathbf{A}'_2, \mathbf{A}'_2, \mathbf{Y}')$. This is the same as in $\mathbf{G}_0$. When the oracle $\mathcal{O}$ outputs a random matrix $\mathbf{U}$, MPK_0 is unchanged and MPK_1 is $(\mathbf{U}, \mathbf{UR} - \mathbf{H}(\mathbf{id}^*)\mathbf{A}'_{\mathbf{2}}, \mathbf{A}'_{\mathbf{2}}, \mathbf{Y}')$. In this case, MPK is the same as in $\mathbf{G}_{\mathbf{1}}$.

At last, $\mathcal{A}$ guesses if it is interacting with $\mathbf{G}_0$ or $\mathbf{G}_1$. $\mathcal{S}$ uses $\mathcal{A}$'s guess to answer whether $\mathbf{A}'$ is a random matrix or an LWE instance. Hence, $\mathcal{S}$'s advantage in distinguishing $\mathbf{U}$ and $(\mathbf{BC} + \mathbf{Z})^t$ is the same as $\mathcal{A}$'s advantage in distinguishing $\mathbf{G_0}$ and $\mathbf{G_1}$. Because $(\mathbf{BC} + \mathbf{Z})^t \approx_c \mathbf{U}$ by Lemma 4, $\mathbf{G_0}$ and $\mathbf{G_1}$ are computationally indistinguishable.

In $\mathbf{G_1}$, $\mathsf{MPK}_1 = (\mathbf{U}, \mathbf{UR} - \mathbf{H}(\mathbf{id}^*)\mathbf{A}'_{\mathbf{2}}, \mathbf{A}'_{\mathbf{2}}, \mathbf{Y}') \approx_c (\mathbf{U_1}, \mathbf{U_2}, \mathbf{A}'_{\mathbf{2}}, \mathbf{Y}')$ by Lemma 2 where $\mathbf{U_1}, \mathbf{U_2}$ are random matrices. Hence, MPK_1 is statistically indistinguishable with MPK_0 which is $(\mathbf{A}, \mathbf{A_1}, \mathbf{A_2}, \mathbf{Y})$. Let $\mathbf{F}_1 = (\mathbf{A}\|\mathbf{A}_1 + \mathbf{H}(\mathbf{id})\mathbf{A}_2), \mathbf{F}_2 = (\mathbf{U}\|\mathbf{UR} + (\mathbf{H}(\mathbf{id}) - \mathbf{H}(\mathbf{id}^*))\mathbf{A}'_2)$. For all $\mathbf{id} \neq \mathbf{id}^*$, $\mathbf{Extract}_{\mathbf{real}}(\mathbf{id}, \mathsf{MPK}_0, \mathsf{MSK}_0)$ uses algorithm $\mathsf{SampleLeft}$ to extract $\mathsf{SK}_{\mathbf{id}}$, so by Lemma 7, the distribution of $\mathsf{SK}_{\mathbf{id}}$ is statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{Y}}(\mathbf{F}_1),\sigma}$. $\mathbf{Extract}_{\mathbf{lossy}}(\mathbf{id}, \mathsf{MPK}_1, \mathsf{MPK}_1)$ uses algorithm $\mathsf{SampleRight}$ to extract $\mathsf{SK}_{\mathbf{id}}$, so by Lemma 8, the distribution of $\mathsf{SK}_{\mathbf{id}}$ is statistically close to $\mathcal{D}_{\Lambda_q^{\mathbf{Y}}(\mathbf{F}_2),\sigma}$. And because $\mathsf{MPK}_0 \approx_s \mathsf{MPK}_1$, $\mathbf{F}_1$ and $\mathbf{F}_2$ are statistically indistinguishable.

The process of $\mathcal{S}$

$\mathbf{A}' \leftarrow \mathcal{O}$
$\mathbf{id}^* \leftarrow \mathcal{A}$
$(\mathsf{MPK}_0, \mathsf{MSK}_0) \leftarrow \mathbf{Setup}_{\mathsf{real}}(1^\lambda)$
$(\mathbf{A}'_2, \mathbf{S}_{A'_2}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{m\times m} \leftarrow \mathbf{TrapGen}$
$\mathbf{R} \xleftarrow{\$} \{1,-1\}^{m\times m}, \mathbf{Y}' \xleftarrow{\$} \mathbb{Z}_q^{n\times l}$
$\mathbf{A}'_1 := \mathbf{A}'\mathbf{R} - \mathbf{H}(\mathbf{id}^*)\mathbf{A}'_2$
$\mathsf{MPK}_1 := (\mathbf{A}', \mathbf{A}'_1, \mathbf{A}'_2, \mathbf{Y}')$
$\mathsf{MSK}_1 := \mathbf{S}_{A'_2}$
$\mathsf{mode}_0 := \mathsf{real}$
$\mathsf{mode}_1 := \mathsf{lossy}$
$b \in_R \{0,1\}$
sends MPK_b
for $i = 1$ to t
  $\mathbf{id}_i \leftarrow \mathcal{A}$
  $\mathsf{SK}_{\mathbf{id}_i} \leftarrow \mathbf{Extract}_{\mathsf{mode_b}}(\mathbf{id}_i, \mathsf{MPK}_b, \mathsf{MSK}_b)$
  sends $\mathsf{SK}_{\mathbf{id}_i}$
end

Fig. 4. The process of $\mathcal{S}$

Therefore, $\mathcal{D}_{\Lambda_q^{\mathbf{Y}}(\mathbf{F}_1)}$ is statistically indistinguishable with $\mathcal{D}_{\Lambda_q^{\mathbf{Y}}(\mathbf{F}_2)}$, i.e. any $\mathsf{SK}_{\mathbf{id}}$ generated by $\mathbf{Extract}_{\mathbf{real}}(\mathbf{id}, \mathsf{MPK}_{\mathbf{0}}, \mathsf{MPK}_{\mathbf{0}})$ is statistically indistinguishable with any $\mathsf{SK}_{\mathbf{id}}$ generated by $\mathbf{Extract}_{\mathbf{lossy}}(\mathbf{id}, \mathsf{MPK}_1, \mathsf{MPK}_1)$ for all $\mathbf{id} \neq \mathbf{id}^*$. Therefore, the advantage of the adversary of $\mathbf{G_1}$ is $negl(\lambda)$.

Above all, the advantage of $\mathbf{G_0}$'s adversary is $negl(\lambda)$. This completes the proof. □

4 Conclusion

In this paper, we extend the notion of lossy encryption proposed by [3] to the scenario of identity-based encryption. This new notion, identity-based lossy encryption, implies IND-sID-SO security under selective identity. And we provide a construction of identity-based lossy encryption based on LWE.

Acknowledgments. We would like to thank the anonymous reviewers for their helpful comments. We would further like to thank Yamin Liu for the helpful revision suggestion.

References

1. Agrawal, S., Boneh, D., Boyen, X.: Efficient lattice (H)IBE in the standard model. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 553–572. Springer, Heidelberg (2010)

2. Agrawal, S., Boneh, D., Boyen, X.: Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 98–115. Springer, Heidelberg (2010)
3. Bellare, M., Hofheinz, D., Yilek, S.: Possibility and impossibility results for encryption and commitment secure under selective opening. In: Joux, A. (ed.) EUROCRYPT 2009. LNCS, vol. 5479, pp. 1–35. Springer, Heidelberg (2009)
4. Bellare, M., Kiltz, E., Peikert, C., Waters, B.: Identity-based (lossy) trapdoor functions and applications. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 228–245. Springer, Heidelberg (2012)
5. Bellare, M., Waters, B., Yilek, S.: Identity-based encryption secure against selective opening attack. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 235–252. Springer, Heidelberg (2011)
6. Berkoff, A., Liu, F.-H.: Leakage resilient fully homomorphic encryption. In: Lindell, Y. (ed.) TCC 2014. LNCS, vol. 8349, pp. 515–539. Springer, Heidelberg (2014)
7. Boneh, D., Boyen, X.: Efficient selective-id secure identity-based encryption without random oracles. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 223–238. Springer, Heidelberg (2004)
8. Boneh, D., Boyen, X.: Secure identity based encryption without random oracles. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 443–459. Springer, Heidelberg (2004)
9. Boneh, D., Franklin, M.: Identity-based encryption from the weil pairing. In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 213–229. Springer, Heidelberg (2001)
10. Boneh, D., Gentry, C., Hamburg, M.: Space-efficient identity based encryption-without pairings. In: 48th Annual IEEE Symposium on Foundations of Computer Science, 2007, FOCS 2007, pp. 647–657. IEEE (2007)
11. Cash, D., Hofheinz, D., Kiltz, E., Peikert, C.: Bonsai trees, or how to delegate a lattice basis. J. Cryptol. **25**(4), 601–639 (2012)
12. 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)
13. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: how to generate strong keys from biometrics and other noisy data. In: Cachin, C., Camenisch, J.L. (eds.) EUROCRYPT 2004. LNCS, vol. 3027, pp. 523–540. Springer, Heidelberg (2004)
14. Döttling, N., Müller-Quade, J.: Lossy codes and a new variant of the learning-with-errors problem. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 18–34. Springer, Heidelberg (2013)
15. Escala, A., Herranz, J., Libert, B., Ràfols, C.: Identity-based lossy trapdoor functions: new definitions, hierarchical extensions, and implications. In: Krawczyk, H. (ed.) PKC 2014. LNCS, vol. 8383, pp. 239–256. Springer, Heidelberg (2014)
16. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the Fortieth Annual ACM Symposium on Theory of computing, pp. 197–206. ACM (2008)
17. Goldwasser, S., Kalai, Y., Peikert, C., Vaikuntanathan, V.: Robustness of the learning with errors assumption. In: Yao, A.C.-C. (ed.) ICS, pp. 230–240. Tsinghua University Press, Beijing (2010)
18. 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)

19. Hemenway, B., Ostrovsky, R.: Building lossy trapdoor functions from lossy encryption. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part II. LNCS, vol. 8270, pp. 241–260. Springer, Heidelberg (2013)
20. Jhanwar, M.P., Barua, R.: A variant of Boneh-Gentry-Hamburg's pairing-free identity based encryption scheme. In: Yung, M., Liu, P., Lin, D. (eds.) Inscrypt 2008. LNCS, vol. 5487, pp. 314–331. Springer, Heidelberg (2009)
21. Lai, J., Deng, R.H., Liu, S., Weng, J., Zhao, Y.: Identity-based encryption secure against selective opening chosen-ciphertext attack. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 77–92. Springer, Heidelberg (2014)
22. 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)
23. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the Thirty-seventh Annual ACM Symposium on Theory of Computing, STOC 2005, pp. 84–93. ACM, New York, NY, USA (2005)
24. Sakai, R., Ohgishi, K., Kasahara, M.: Cryptosystems based on pairing. In: The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, pp. 135–148 (2000)
25. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985)
26. Waters, B.: Efficient identity-based encryption without random oracles. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 114–127. Springer, Heidelberg (2005)
27. Waters, B.: Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 619–636. Springer, Heidelberg (2009)