Key Dependent Message Security for Revocable Identity-Based Encryption and Identity-Based Encryption

Rui Zhang[1,2] and Yang Tao[1,2(✉)]

[1] State Key Laboratory of Information Security (SKLOIS),
Institute of Information Engineering (IIE),
Chinese Academy of Sciences (CAS), Beijing, China
{r-zhang,taoyang}@iie.ac.cn
[2] School of Cyber Security,
University of Chinese Academy of Sciences (UCAS), Huairou, China

Abstract. In a revocable identity-based encryption (RIBE) system, the private key and update key are generated separately and combined together to obtain the decryption key. Since the update key is distributed in a public channel, for each user, the private key and the decryption key are essential to his information security. Careless key management, e.g. full disk encryption may leak the encryption of the private key or decryption key, which actually needs to consider the key dependent message (KDM) security. However, previous research mainly focus on the KDM security of IBE and revocability separately and the KDM security for RIBE scheme is still unclear. In this paper, we consider the KDM security for RIBE schemes for the first time and investigate two KDM security models with respect to the private key and decryption key respectively. First, we present a generic construction of KDM-secure RIBE with the private key from any KDM-secure IBE and RIBE in the selective/adaptive chosen-identity model. Second, we construct a concrete KDM-secure RIBE scheme with the decryption key in the selective chosen-identity model from lattices under the *polynomial* modulus. As an independent interest, we also present an efficient lattice-based KDM-secure IBE scheme in the random oracle model. However, it is only secure in the single key setting in the quantum random oracle model.

Keywords: Lattice-based schemes
Key dependent message security
Revocable identity-based encryption

1 Introduction

Identity-based encryption (IBE) is a special public key encryption (PKE), where a user's public key can be an arbitrary string. It was first advocated by Shamir [19] in 1984, mainly to leverage the difficulty of managing certificates for traditional public key infrastructure (PKI). Similar to its PKE counterpart, IBE was

D. Naccache et al. (Eds.): ICICS 2018, LNCS 11149, pp. 426–441, 2018.
https://doi.org/10.1007/978-3-030-01950-1_25

also born without the revocation mechanism. To solve this problem, Boneh and Franklin [5] mentioned to append the current time t to an id, namely, to encrypt a message, the sender uses $\mathsf{id}||\mathsf{t}$ instead of id, and the private key will be refreshed according to the time. But it is very inefficient, actually linear in the number of remaining users for both computation and bandwidth, since the private keys of all remaining users should be reissued and distributed at the beginning of each time period. Later, in ACM CCS'08, using broadcast encryption for tree-based structures, Boldyreva, Goyal, and Kumar [4] introduced revocable IBE (RIBE), which reduced the complexity of key update information from linear to logarithmic in the number of users. Subsequent work [8,11,18,20] based on bilinear pairings and lattices made further improvements and/or trade-offs.

On the other hand, key management is essential to the security of any practical system. E.g., in full disk encryption, an adversary may see the encryption of the secret key, which was known as key dependent message (KDM) security [3,6][1]. There are great efforts on KDM-secure PKE [2,6,7,21], but less attention on KDM-secure IBE. The first KDM-secure IBE was introduced by Alperin-Sheriff and Peikert [1]. They considered the scenario of revocation and proved the KDM security against selective chosen-identity attack (KDM-sID-CPA) with respect to the users' private keys in the multi-key setting. However, since the selective security is a weaker security model and the scheme with large keys is less efficient. Hereafter, there are some further improvements [9,14] on [1] in the aspects of efficiency and security. In the selective security model, Chen et al. [9] optimized the efficiency of the scheme in [1] with indistinguishability obfuscation ($i\mathcal{O}$) and puncturable PRF, where $i\mathcal{O}$ seems impractical by far. As for security optimization, in [9] and [14], they were both interested in the KDM security against adaptive chosen-identity attack (KDM-ID-CPA). Chen et al. [9] proposed a generic construction of KDM-ID-CPA secure IBE from identity-based hash proof system (IB-HPS) with homomorphic property. In the recent work [14], Kitagawa and Tanaka constructed a generic construction of KDM-ID-CPA secure IBE from KDM-secure symmetric key encryption using IND-ID-CPA IBE and garbled circuits.

Similar to its IBE counterpart, RIBE may also share the same practical problem. In an RIBE system, the private key and update key are generated separately, and combined together to generate the decryption key. In the real world, the private key serves as a long-term key, while the update key (an ephemeral key) is distributed through a public channel. Since for each user, the private key and decryption key are the main secrecy of the system, it may damage the user's data confidentiality when such keys are lost or some information is leaked.

[1] If we consider the KDM security in d pairs of public/secret keys, i.e., the multi-key setting, we denote it as d-KDM security and if $d = 1$, it refers to the KDM security in a single key setting, a weaker security notion than d-KDM with $d \geq 2$.

Therefore, it is necessary to consider the KDM security for RIBE. However, the previous research on revocability and KDM security is discussed separately[2].

As a result, the problems whether one can construct a KDM-secure RIBE system are still open.

1.1 Our Results

In this paper, we pose an affirmative answer to the above problems. Since there are two kinds of secret keys for each user in the RIBE scheme—private key and decryption key, we investigate the KDM security with respect to the private key and decryption key respectively. We view our work as one step ahead towards bringing IBEs to the real-world usage. Our techniques are summarized as follows. Due to the space limit, our proofs are given in the full version of this paper.

First, we propose a generic construction of KDM-secure RIBE with the private key from a KDM-secure IBE and a RIBE scheme, where the KDM-security with the private key is gained from the underlying KDM-secure IBE and revocation mechanism stems from the underlying RIBE. When encrypting a message, we randomly split the message into two parts and encrypt each part using the corresponding IBE and RIBE respectively. As long as the two building blocks is secure in the selective/adaptive chosen-identity model, our generic construction preserves the security in the selective/adaptive chosen-identity model.

Second, as for the KDM security with the decryption key, instead of combining two unrelated building blocks to achieve KDM security and key revocation, we propose a KDM-sID-CPA secure RIBE scheme from lattices by modifying the RIBE proposed by Chen et al. [8]. Recall such RIBE in the selective chosen-identity model utilized two IBE schemes, one of which is used to deal with the identity and the other is corresponding to the time. To achieve the revocation mechanism, Chen et al. adopted the binary data structure and randomly split the public parameter into two parts to link the identity and time. The private key of each user is a set of vectors corresponding to the nodes in the binary tree. Each non-revoked user can get the update key of one node and generate the decryption key relating to such node. Inspired by the work of [8] and [1], we exploit the framework of [8] and replace the IBE building block corresponding to the identity with a KDM-secure IBE of [1]. If guessing the decryption node correctly (with non-negligible probability), we can answer the KDM queries of the decryption key following the strategy of [1]. Therefore, we can obtain a KDM-sID-CPA secure RIBE but suffering from a super-polynomial modulus as [1]. Furthermore, we optimize the modulus from super-polynomial to polynomial by the noise re-randomization technique [12], which leads to a reasonably weak assumption and much efficiency. By the way, our modulus optimization is also applicable to [1].

As an independent interest, we also present an efficient KDM-ID-CPA secure IBE for arbitrary constant identity clique d under the LWE assumption in the

[2] In [1], scenarios of revocation has been considered for the IBE scheme, but in the concrete construction, they proposed the KDM-secure IBE instead of KDM-secure RIBE.

random oracle. Unlike [9,14] using the complicated tools, such as $i\mathcal{O}$ and garbled circuits, our IBE scheme is a GPV-style construction [10] and for each identity id, it is actually an image of the KDM-PKE instance in [1]. In the classical random oracle model, we can link the KDM-PKE public key $\mathbf{A}_i$ and the public parameter $\mathbf{A}_{\mathsf{id}}$ of IBE with the help of a trapdoor, thus successfully transforming a KDM-challenge ciphertext of PKE scheme to a KDM-challenge response for our IBE scheme. Therefore, our security of KDM-IBE merely relies on the security of the underlying KDM-PKE scheme. In the quantum random oracle, our security is a direct adaption of [22] and only 1-KDM secure. However, when extending the security to d-KDM security, the existing strategy fails and the detailed discussion is put in Sect. 6.2.

Related Work. As for RIBE, there is another stronger security notion—decryption key exposure resistance (DKER), which is introduced by Seo and Emura [18]. Recently, Katsumata et al. [11] proposed a generic construction of RIBE with DKER and gave the first construction based on lattices. However, it is worth mentioning that our concrete RIBE scheme does not support DKER security, since our decryption key is a simple concatenation of the private key and update key.

2 Preliminary

Notations. Denote real numbers by $\mathbb{R}$ and integers by $\mathbb{Z}$. Denote column vectors over $\mathbb{R}$ and $\mathbb{Z}$ with lower-case bold letters (e.g. $\mathbf{x}$), and matrices by upper-case bold letters (e.g. $\mathbf{A}$). Denote the matrix $[\mathbf{A}_1|\mathbf{A}_2]$ the concatenating the matrix $\mathbf{A}_1$ and $\mathbf{A}_2$. For a positive integer d, let $[d]$ denote the integer set $\{1, \cdots, d\}$. If S is a set, $s \overset{r}{\leftarrow} S$ denotes sampling randomly s from uniform distribution over S. A function $negl(n) : \mathbb{R}_{\geq 0} \rightarrow \mathbb{R}_{\geq 0}$ is negligible if sufficiently large $n > n_0$ (n_0 is a constant), $negl(n) < 1/poly(n)$. The statistical distance between two random variables X and Y over a countable set D is $\varDelta(X, Y) = \frac{1}{2}\sum_{w \in D} |\Pr[X = w] - \Pr[Y = w]|$. Let $\{X_n\}$ and $\{Y_n\}$ be ensembles of random variables indexed by a security parameter n, we say that $\{X_n\}$ and $\{Y_n\}$ are statistically close if $\varDelta(X_n, Y_n)$ is negligible function of n. For a matrix $\mathbf{R} \in \mathbb{R}^{l \times t}$, the largest singular value of $\mathbf{R}$ is defined as $s_1(\mathbf{R}) = \max_{\|\mathbf{u}\|=1} \|\mathbf{Ru}\|$. We fix a universal gadget matrix $\mathbf{G} = \mathbf{I}_n \otimes (1, 2, 4, \ldots, 2^{k-1}) \in \mathbb{Z}_q^{n \times w}$ for $k = \lceil \log q \rceil$ and $w = nk = n\lceil \log q \rceil$. In this paper, we use $negl(n)$ to denote a class of negligible functions instead of some fixed function.

2.1 Lattices and Gaussian Measures

An n-dimension (full-rank) lattice $\varLambda \subseteq \mathbb{R}^n$ is the set of all integer linear combinations of some set of independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^{n \times n}$, $\varLambda = \mathcal{L}(\mathbf{B}) = \{\sum_{i=1}^n z_i \mathbf{b}_i : z_i \in \mathbb{Z}\}$. The dual lattice of $\varLambda \subseteq \mathbb{R}^n$ is defined as $\varLambda^* = \{\mathbf{x} \in \mathbb{R}^n : \langle \varLambda, \mathbf{x} \rangle \subseteq \mathbb{Z}\}$. For integers $n \geq 1$, modulus $q \geq 2$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, an m-dimensional lattice is defined as $\varLambda^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{Ax} = \mathbf{0} \in \mathbb{Z}_q^n\} \subseteq \mathbb{Z}^m$.

For any $\mathbf{y}$ in the subgroup of $\mathbb{Z}_q^n$, we also define the coset $\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{y} \mod q\} = \Lambda^{\perp}(\mathbf{A}) + \bar{\mathbf{x}}$, where $\bar{\mathbf{x}} \in \mathbb{Z}^m$ is an arbitrary solution to $\mathbf{A}\bar{\mathbf{x}} = \mathbf{y}$.

Gaussian Measures. Let Λ be a lattice in $\mathbb{Z}^n$. For any vector $\mathbf{c} \in \mathbb{R}^n$ and parameter $r > 0$, the n-dimensional Gaussian function $\rho_{r,\mathbf{c}} : \mathbb{R}^n \to (0, 1]$ is defined as $\rho_{r,\mathbf{c}}(\mathbf{x}) := \exp(-\pi\|\mathbf{x} - \mathbf{c}\|^2/r^2)$. The discrete Gaussian distribution over Λ with parameter r and center $\mathbf{c}$ (abbreviated as $D_{\Lambda,r,\mathbf{c}}$) is defined as $\forall \mathbf{y} \in \Lambda, D_{\Lambda,r,\mathbf{c}}(\mathbf{y}) := \frac{\rho_{r,\mathbf{c}}(\mathbf{y})}{\rho_{r,\mathbf{c}}(\Lambda)}$, where $\rho_{r,\mathbf{c}}(\Lambda) = \sum_{\mathbf{y}\in\Lambda} \rho_{r,\mathbf{c}}(\mathbf{y})$. When $\mathbf{c} = \mathbf{0}$, we write $D_{\Lambda,r}$ for short.

Lemma 1. ([10], Theorem 4.1). There is a probabilistic polynomial-time algorithm SampleGaussian that, given a basis $\mathbf{B}_\Lambda$ of an n-dimensional lattice Λ, a parameter $r \geq \|\widetilde{\mathbf{B}}_\Lambda\| \cdot \omega(\sqrt{\log n})$, and a center $\mathbf{c} \in \mathbb{R}^n$, outputs a sample from a distribution that is statistically close to $D_{\Lambda,r,\mathbf{c}}$.

Lemma 2. ([10,15,16]). Let $m \geq Cn \log q$ for some constant $C > 1$.

1. For any n-dimensional lattice Λ, any $\mathbf{c} \in \mathbb{Z}^n$, and any $r \geq \eta_\varepsilon(\Lambda)$,[3] where $\varepsilon(n) = negl(n)$, we have $\|D_{\Lambda+\mathbf{c},r}\| \leq r\sqrt{n}$ with all but $negl(n)$ probability. In addition, for $\Lambda = \mathbb{Z}$ we have $|D_{\mathbb{Z},r}| \leq r \cdot \omega(\sqrt{\log n})$ except with $negl(n)$ probability.
2. For any $r > 0$, and for $\mathbf{R} \leftarrow D_{\mathbb{Z},r}^{n\times k}$, we have $s_1(\mathbf{R}) \leq r \cdot O(\sqrt{n} + \sqrt{k})$ except with $negl(n)$ probability.
3. With all but $negl(n)$ probability over the uniformly random choice of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the following holds: For $\mathbf{e} \leftarrow D_{\mathbb{Z},r}^m$, where $r = \omega(\sqrt{\log n})$, the distribution of $\mathbf{y} = \mathbf{A}\mathbf{e} \mod q$ is within $negl(n)$ statistical distance of uniform, and the conditional distribution of $\mathbf{e}$ given $\mathbf{y}$ is $D_{\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}),r}$.

Lemma 3. ([12], Lemma 1). Let q, l, m be positive integers and r a positive real satisfying $r > \max\{\omega(\sqrt{\log m}), \omega(\sqrt{\log l})\}$. Let $\mathbf{b} \in \mathbb{Z}_q^m$ be arbitrary and $\mathbf{x}$ chosen from $D_{\mathbb{Z},r}^m$. Then for any $\mathbf{V} \in \mathbb{Z}^{m\times l}$ and positive real $\sigma > s_1(\mathbf{V})$, there exists a PPT algorithms $\mathbf{ReRand}(\mathbf{V}, \mathbf{b} + \mathbf{x}, r, \sigma)$ that outputs $\mathbf{b}' = \mathbf{b}\mathbf{V} + \mathbf{x}' \in \mathbb{Z}_q^l$ where $\mathbf{x}'$ is distributed statistically close to $D_{\mathbb{Z},2r\sigma}^l$.

A new trapdoor notion was introduced in [15]. The strong trapdoor $\mathbf{R}$ for a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ refers that for some invertible matrix $\mathbf{H} \in \mathbb{Z}_q^{n\times n}$, we have $\mathbf{R} \in \mathbb{Z}^{(m-w)\times w}$ such that $\mathbf{A}\begin{bmatrix}\mathbf{R}\\ \mathbf{I}\end{bmatrix} = \mathbf{H}\mathbf{G}$.

Lemma 4. ([15], Theorem 5.1). Let $\mathbf{R}$ be a strong trapdoor for $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. There is an efficient randomized algorithm that given $\mathbf{R}$, any $\mathbf{u} \in \mathbb{Z}_q^n$, and any $r \geq s_1(\mathbf{R}) \cdot \omega(\sqrt{\log n}) \geq \eta_\varepsilon(\Lambda^{\perp}(\mathbf{A}))$ (for some $\varepsilon(n) = negl(n)$), samples from a distribution within $negl(n)$ distance of $D_{\Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}),r}$.

[3] For a lattice Λ and a positive real $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\Lambda)$ is defined as the smallest real $r > 0$ such that $\rho_{1/r}(\Lambda^*\backslash\{\mathbf{0}\}) \leq \varepsilon$. Especially, for any $\omega(\sqrt{\log n})$ function, $\eta_\varepsilon(\mathbb{Z}^n) \leq \omega(\sqrt{\log n})$.

Learning with Errors Assumption. The learning with errors (LWE) problem was introduced by Regev [17], which is at least as hard as several lattice problems in the worst case. For security parameter λ, let $n = n(\lambda)$ be an integer dimension, let $q = q(\lambda) \geq 2$ be an integer, and let $\chi = \chi(\lambda)$ be a distribution over $\mathbb{Z}$. The $\mathrm{LWE}_{n,q,\chi}$ problem is to distinguish the two distributions: $\{\mathbf{A}, \mathbf{A}^t\mathbf{s} + \mathbf{x}\}$ and $\{\mathbf{A}, \mathbf{u}\}$ where $\mathbf{A} \overset{r}{\leftarrow} \mathbb{Z}_q^{n\times m}, \mathbf{s} \overset{r}{\leftarrow} \mathbb{Z}_q^n, \mathbf{u} \overset{r}{\leftarrow} \mathbb{Z}_q^m$, and $\mathbf{x} \leftarrow \chi^m$. When the error distribution $\chi = D_{\mathbb{Z},\alpha q}$, the problem is abbreviated as $\mathrm{LWE}_{n,q,\alpha}$.

2.2 KDM-PKE Scheme in [1]

KDM Security. We mainly consider the KDM security from [1,3]. In their definitions, the adversary $\mathcal{A}$ plays a game with the challenger $\mathcal{C}$, and is able to make queries for encryptions of functions of secret keys. The functions which the adversary queries are restricted in a certain family $\mathcal{F} \subset \{f : \mathcal{K} \rightarrow \mathcal{M}\}$ ($\mathcal{F}$ contains constant functions on $\mathcal{M}$), where $\mathcal{K}$ is the keyspace of secret keys and $\mathcal{M}$ is the message space of the encryption scheme. In the definition of [1], the adversary assigns two functions $(f_0, f_1) \in \mathcal{F}$ with each query, and must distinguish between the encryptions of f_0 and encryptions of f_1. Concretely, for the PKE scheme $(\mathsf{Setup}, \mathsf{Enc}, \mathsf{Dec})$, the d-KDM-CPA security game between an adversary and the challenger parameterized by $\beta \in \{0, 1\}$ proceeds as follows.

- **Setup**: The challenger runs $(\mathsf{PK}_i, \mathsf{SK}_i) \leftarrow \mathrm{Setup}(1^n)$ for $i \in [d]$ and the adversary $\mathcal{A}$ is given the challenge public keys $I = \{\mathsf{PK}_1, \cdots, \mathsf{PK}_l\}$ for some $l \leq d$.
- **Query**: $\mathcal{A}$ may adaptively make a polynomial number of queries: $\mathcal{A}$ can make encryption query of the form (i, f_0, f_1), where $f_0, f_1 \in \mathcal{F}$ and $1 \leq i \leq l$. The challenger computes $\mu \leftarrow f_\beta(\mathsf{SK}_1, \cdots, \mathsf{SK}_l)$ and $c \leftarrow \mathrm{Enc}(\mathsf{PK}_i, \mu)$, and responses a ciphertext c.

We say the scheme is d-KDM-CPA secure with respect to $\mathcal{F}$ if the game for $\beta = 0, 1$ are computationally indistinguishable.

The d-KDM security against selective chosen-identity and chosen-message attack for IBE scheme (d-KDM-sID-CPA) was defined in [1]. A stronger security model for IBE, i.e., adaptive chosen-identity and chosen-message attack (d-KDM-ID-CPA), is similar to the above definition for d target identities with the KDM ciphertext of $f(\mathsf{SK}_{\mathsf{id}_1^*}, \cdots, \mathsf{SK}_{\mathsf{id}_d^*})$ except that the challenge identities can be chosen adaptively even after seeing the public key.

KDM-PKE Scheme. Let a modulus be $q = p^2$ for a polynomial prime $p \geq r^2\sqrt{n+m} \cdot \omega(\sqrt{\log n})$, where n, m are integers, r is a Gaussian parameter satisfying $r \geq 2\sqrt{n}$ and λ be a security parameter. The message space is $\mathbb{Z}_p$. The KDM-secure PKE scheme Π_{PKE} in [1] consists of three algorithms:

- $(\mathsf{PK}, \mathsf{SK}) \leftarrow \overline{\mathsf{Gen}}(1^\lambda)$: Choose $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{z}_0 \leftarrow D_{\mathbb{Z},r}^n$, $\mathbf{z}_1 \leftarrow D_{\mathbb{Z},r}^m$, and let $\mathbf{y} = \mathbf{z}_0 - \mathbf{A}\mathbf{z}_1 = [\mathbf{I}_n| - \mathbf{A}]\mathbf{z} \in \mathbb{Z}_q^n$ where $\mathbf{z} = [{\mathbf{z}_0}^t|{\mathbf{z}_1}^t]^t \in \mathbb{Z}^{n+m}$. The public key PK is $(\mathbf{A}, \mathbf{y})$ and the secret key SK is $\mathbf{z}_1$.

- $\mathbf{c}^t \leftarrow \overline{\mathsf{Enc}}(\mathbf{A}, \mathbf{y}, \mu)$: To encrypt a message $\mu \in \mathbb{Z}_p$, choose $\mathbf{x}_0 \leftarrow D^n_{\mathbb{Z},r}$, $\mathbf{x}_1 \leftarrow D^m_{\mathbb{Z},r}$ and $x' \leftarrow D_{\mathbb{Z},r}$. Output the ciphertext $\mathbf{c}^t = \mathbf{x}_0^t[\mathbf{A}|\mathbf{y}] + [\mathbf{x}_1^t|x'] + [\mathbf{0}|p \cdot \mu] \in \mathbb{Z}_q^{1\times(m+1)}$.
- $\mu \leftarrow \overline{\mathsf{Dec}}(\mathbf{z}_1, \mathbf{c})$: Compute $\mu' = \mathbf{c}^t \begin{bmatrix} \mathbf{z}_1 \\ 1 \end{bmatrix} \in \mathbb{Z}_q$. Output the $\mu \in \{0, \dots, p-1\} = \mathbb{Z}_p$ such that μ' is closest to $p \cdot \mu \mod q$.

Theorem 1. **([1]).** The above cryptosystem is d-KDM-CPA secure with respect to the set of affine functions over $\mathbb{Z}_p$ under the LWE assumption.

3 Security Model

In this section, we review the definition of revocable identity-based encryption (RIBE), and adapt the KDM security to the RIBE scheme. Since there are two kinds of secret keys for each user—the private key and the decryption key in the RIBE schemes, we consider our KDM security with respect to the private key and decryption key respectively.

An RIBE scheme has seven probabilistic polynomial-time (PPT) algorithms **Setup**, **PriKeyGen**, **KeyUpd**, **DecKeyGen**, **Enc**, **Dec** and **KeyRev** with associated message space $\mathcal{M}$, identity space $\mathcal{I}$, and time space $\mathcal{T}$. We assume that the size of $\mathcal{T}$ is a polynomial in the security parameter. There are three parties: key authority, sender and receiver. Key authority maintains a revocation list RL and state ST. Hereafter, an algorithm is called stateful if RL or ST needs updating for revocation.

- $(\mathsf{PP}, \mathsf{MK}, \mathsf{RL}, \mathsf{ST}) \leftarrow \mathbf{Setup}(1^n, N)$: Taking as input a security parameter n and a maximal number of users N, it outputs public parameters PP, a master secret key MK, a revocation list RL (initially empty) and a state ST.
- $(\mathsf{SK}_{\mathsf{id}}, \mathsf{ST}) \leftarrow \mathbf{PriKeyGen}(\mathsf{PP}, \mathsf{MK}, \mathsf{id}, \mathsf{ST})$: Taking as input public parameters PP, a master secret key MK, an identity $\mathsf{id} \in \mathcal{I}$ and a state ST, it outputs a private key $\mathsf{SK}_{\mathsf{id}}$ and an updated state ST.
- $\mathsf{KU}_{\mathsf{t}} \leftarrow \mathbf{KeyUpd}(\mathsf{PP}, \mathsf{MK}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$: Taking as input public parameters PP, a master secret key MK, a key update time $\mathsf{t} \in \mathcal{T}$, a revocation list RL and a state ST, it outputs an update key KU_{t}.
- $\mathsf{DK}_{\mathsf{id},\mathsf{t}}/\bot \leftarrow \mathbf{DecKeyGen}(\mathsf{PP}, \mathsf{SK}_{\mathsf{id}}, \mathsf{KU}_{\mathsf{t}})$: Taking as input public parameters PP, a private key $\mathsf{SK}_{\mathsf{id}}$ and an update key KU_{t}, it outputs a decryption key $\mathsf{DK}_{\mathsf{id},\mathsf{t}}$ or a special symbol $\bot$ indicating that id has been revoked.
- $\mathsf{CT}_{\mathsf{id},\mathsf{t}} \leftarrow \mathbf{Enc}(\mathsf{PP}, \mathsf{id}, \mathsf{t}, \mu)$: Taking as input public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$, an encryption time $\mathsf{t} \in \mathcal{T}$ and a message $\mu \in \mathcal{M}$, it outputs a ciphertext $\mathsf{CT}_{\mathsf{id},\mathsf{t}}$.
- $\mu \leftarrow \mathbf{Dec}(\mathsf{PP}, \mathsf{DK}_{\mathsf{id},\mathsf{t}}, \mathsf{CT}_{\mathsf{id},\mathsf{t}})$: Taking as input public parameters PP, a decryption key $\mathsf{DK}_{\mathsf{id},\mathsf{t}}$ and a ciphertext $\mathsf{CT}_{\mathsf{id},\mathsf{t}}$, it outputs a message $\mu \in \mathcal{M}$.
- $\mathsf{RL} \leftarrow \mathbf{KeyRev}(\mathsf{id}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$: Taking as input an identity to be revoked $\mathsf{id} \in \mathcal{I}$, a revocation time $\mathsf{t} \in \mathcal{T}$, a revocation list RL and a state ST, it outputs an updated revocation list RL.

We require the correctness condition holds that $\forall$ polynomially-bounded N, $\forall$ $(\mathsf{PP}, \mathsf{MK}) \leftarrow \mathrm{Setup}(1^n, N)$, $\forall$ $\mu \in \mathcal{M}$, $\forall$ $\mathsf{id} \in \mathcal{I}$, $\forall$ $\mathsf{t} \in \mathcal{T}$, all possible valid states ST and revocation lists RL, if identity id was not revoked before or at time t, for $(\mathsf{SK}_{\mathsf{id}}, \mathsf{ST}) \leftarrow \mathrm{PriKeyGen}(\mathsf{PP}, \mathsf{MK}, \mathsf{id}, \mathsf{ST})$, $\mathsf{KU}_{\mathsf{t}} \leftarrow \mathrm{KeyUpd}(\mathsf{PP}, \mathsf{MK}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$ and $\mathsf{DK}_{\mathsf{id},\mathsf{t}} \leftarrow \mathrm{DecKeyGen}(\mathsf{PP}, \mathsf{SK}_{\mathsf{id}}, \mathsf{KU}_{\mathsf{t}})$, we have $\Pr[\mathrm{Dec}(\mathsf{PP}, \mathsf{DK}_{\mathsf{id},\mathsf{t}}, \mathrm{Enc}(\mathsf{PP}, \mathsf{id}, \mathsf{t}, \mu)) \neq \mu] \leq negl(n)$.

Now we define the KDM security games in the RIBE. For simplicity, we only consider the selective chosen-identity attack model[4] in the single identity setting and take into account the key revocation and KDM security with respect to function family $\mathcal{F}$. We define the KDM security game with decryption key and private key respectively.

The KDM security game with the *decryption key* between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ is parameterized by some $\beta \in \{0, 1\}$ and proceeds as follows:

- **Initial**: The adversary first outputs the challenge identity id^* and time t^*, and also some information state it wants to preserve.
- **Setup**: The challenger runs $(\mathsf{PP}, \mathsf{MK}, \mathsf{RL}, \mathsf{ST}) \leftarrow \mathrm{Setup}(1^n, N)$, and the adversary $\mathcal{A}$ is given public parameters PP.
- **Query**: $\mathcal{A}$ may adaptively make a polynomial number of queries of the following oracles (the oracles share state):
  - **Extraction Queries**: $\mathcal{A}$ can query $\mathrm{PriKeyGen}(\cdot)$ for identity id, and gets a private key $\mathsf{SK}_{\mathsf{id}}$.
  - **Update Queries**: $\mathcal{A}$ can query $\mathrm{KeyUpd}(\cdot)$ for time t, and gets an update key KU_{t}.
  - **Revocation Queries**: $\mathcal{A}$ can query $\mathrm{KeyRev}(\cdot, \cdot)$ for identity id and time t, and gets an update RL.
  - **KDM-Encryption Queries**: $\mathcal{A}$ can make encryption queries of the form (f_0, f_1), where $f_0, f_1 \in \mathcal{F}$. If $\mathsf{DK}_{\mathsf{id}^*,\mathsf{t}^*} \neq \perp$, the challenger $\mathcal{C}$ computes $\mu \leftarrow f_\beta(\mathsf{DK}_{\mathsf{id}^*,\mathsf{t}^*})$ and $c \leftarrow \mathrm{Enc}(\mathsf{PP}, \mathsf{id}^*, \mathsf{t}^*, \mu)$, and responses a ciphertext $\mathsf{CT}_{\mathsf{id}^*,\mathsf{t}^*}$. If $\mathsf{DK}_{\mathsf{id}^*,\mathsf{t}^*} = \perp$ and $f_\beta = m_\beta$, a constant function in $\mathcal{M}$, $\mathcal{C}$ returns encryption of m_β, i.e.,$\mathsf{CT}_{\mathsf{id}^*,\mathsf{t}^*} \leftarrow \mathrm{Enc}(\mathsf{PP}, \mathsf{id}^*, \mathsf{t}^*, m_\beta)$. Otherwise, if $\mathsf{DK}_{\mathsf{id}^*,\mathsf{t}^*} = \perp$ and f_β is not a constant function in $\mathcal{M}$, then $\mathcal{C}$ returns the encryption of zero string, i.e., $\mathsf{CT}_{\mathsf{id}^*,\mathsf{t}^*} \leftarrow \mathrm{Enc}(\mathsf{PP}, \mathsf{id}^*, \mathsf{t}^*, \mathbf{0})$.
- **Guess**: The adversary outputs a bit β'. If $\beta' = \beta$, $\mathcal{A}$ succeeds.

The KDM security game with the *private key* between an adversary $\mathcal{A}$ and a challenger $\mathcal{C}$ is the same as above, except the KDM-Encryption queries. Such KDM-Encryption queries with the private key are as follows.

- **KDM-Encryption Queries**: $\mathcal{A}$ can make encryption queries of the form (f_0, f_1), where $f_0, f_1 \in \mathcal{F}$. The challenger $\mathcal{C}$ computes $\mu \leftarrow f_\beta(\mathsf{SK}_{\mathsf{id}^*})$ and $c \leftarrow \mathrm{Enc}(\mathsf{PP}, \mathsf{id}^*, \mathsf{t}^*, \mu)$, and responses a ciphertext $\mathsf{CT}_{\mathsf{id}^*,\mathsf{t}^*}$.

[4] The adaptive chosen-identity model is identical to the selective chosen-identity model, except the target identity and time are adaptively chosen by the adversary after seeing the public key.

We insist that KeyUpd$(\cdot)$ and KeyRev$(\cdot,\cdot)$ can be queried on time in a non-decreasing order of time. Besides, the following restrictions should always hold:

1. KeyRev$(\cdot,\cdot)$ cannot be queried at time t if KeyUpd$(\cdot)$ was queried on t.
2. If PriKeyGen$(\cdot)$ was queried on identity id^*, then KeyRev$(\mathsf{id}^*,\cdot)$ must be queried at time $\mathsf{t} \leq \mathsf{t}^*$. In other words, id^* must be revoked at time $\mathsf{t} \leq \mathsf{t}^*$.
3. If $\mathsf{t} \geq \mathsf{t}^*$ and ID^* is not revoked at t^*, then PriKeyGen(ID^*) cannot be queried at time t.

We say that a scheme has KDM security with the decryption key/private key against selective chosen-identity and chosen-plaintext attacks (KDM-sID-CPA) with respect to $\mathcal{F}$, if the advantage of any PPT adversary $\mathcal{A}$ is bounded by a negligible function $negl(n)$, i.e. $Adv(\mathcal{A}) = |\Pr[\mathcal{A} \text{ succeeds}] - \frac{1}{2}| \leq negl(n)$.

4 KDM Security for RIBE with the Private Key

In this section, we give a generic construction of KDM-secure RIBE with the private key from a KDM-secure IBE and a RIBE scheme. Let k.Π = (k.Setup, k.PriKeyGen, k.Enc, k.Dec) be a KDM-secure IBE scheme with identity space $\mathsf{k}.\mathcal{I}$ and message space $\mathsf{k}.\mathcal{M}$. Let r.Π = (r.Setup, r.PriKeyGen, r.KeyUpd, r.DecKeyGen, r.Enc, r.Dec, KeyRev) be an RIBE scheme with identity space $\mathsf{r}.\mathcal{I}$, time space $\mathsf{r}.\mathcal{T}$ and message space $\mathsf{r}.\mathcal{M}$. We assume $\mathsf{k}.\mathcal{I} = \mathsf{r}.\mathcal{I}, \mathsf{k}.\mathcal{M} = \mathsf{r}.\mathcal{M}$.

Our KDM-secure RIBE Π = (Setup, PriKeyGen, KeyUpd, DecKeyGen, Enc, Dec, KeyRev) with identity space $\mathcal{I}$, message space $\mathcal{M}$ and time space $\mathcal{T}$. Assuming $\mathcal{I} = \mathsf{k}.\mathcal{I} = \mathsf{r}.\mathcal{I}, \mathcal{M} = \mathsf{k}.\mathcal{M} = \mathsf{r}.\mathcal{M}, \mathcal{T} = \mathsf{r}.\mathcal{T}$, our construction is as follows.

- $(\mathsf{PP}, \mathsf{MK}, \mathsf{RL}, \mathsf{ST}) \leftarrow$ Setup$(1^n, N)$: Taking as input a security parameter n and a maximal number of users N, run $(\mathsf{k.PP}, \mathsf{k.MK}) \leftarrow$ k.Setup(1^n) and $(\mathsf{r.PP}, \mathsf{r.MK}) \leftarrow$ r.Setup$(1^n, N)$. It outputs public parameters PP=(k.PP,r.PP), a master secret key MK=(k.MK,r.MK), a revocation list RL (initially empty) and a state ST.
- $(\mathsf{SK_{id}}, \mathsf{ST}) \leftarrow$ PriKeyGen$(\mathsf{PP}, \mathsf{MK}, \mathsf{id}, \mathsf{ST})$: Taking as input public parameters PP, a master secret key MK, an identity $\mathsf{id} \in \mathcal{I}$ and a state ST, run $\mathsf{k.SK_{id}} \leftarrow$ k.PriKeyGen$(\mathsf{k.PP}, \mathsf{k.MK}, \mathsf{id})$ and $\mathsf{r.SK_{id}} \leftarrow$ r.PriKeyGen$(\mathsf{r.PP}, \mathsf{r.MK}, \mathsf{id}, \mathsf{ST})$. It outputs a private key $\mathsf{SK_{id}} = (\mathsf{k.SK_{id}}, \mathsf{r.SK_{id}})$ and an updated state ST.
- $\mathsf{KU_t} \leftarrow$ KeyUpd$(\mathsf{PP}, \mathsf{MK}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$: Taking as input public parameters PP, a master secret key MK, a key update time $\mathsf{t} \in \mathcal{T}$, a revocation list RL and a state ST, run $\mathsf{r.KU_t} \leftarrow$ r.KeyUpd$(\mathsf{r.PP}, \mathsf{r.MK}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$. it outputs an update key $\mathsf{KU_t} = \mathsf{r.KU_t}$.
- $\mathsf{DK_{id,t}}/\perp \leftarrow$ DecKeyGen$(\mathsf{PP}, \mathsf{SK_{id}}, \mathsf{KU_t})$: Taking as input public parameters PP, a private key $\mathsf{SK_{id}}$ and an update key $\mathsf{KU_t}$, run $\mathsf{r.DK_{id,t}} \leftarrow$ r.DeyKeyGen$(\mathsf{r.PP}, \mathsf{r.SK_{id}}, \mathsf{r.KU_t})$. It outputs a decryption key $\mathsf{DK_{id,t}} = (\mathsf{k.SK_{id}}, \mathsf{r.DK_{id,t}})$ or a special symbol $\perp$ if $\mathsf{r.DK_{id,t}} = \perp$ indicating that id has been revoked.

- $\mathsf{CT}_{\mathsf{id,t}} \leftarrow \mathrm{Enc}(\mathsf{PP}, \mathsf{id}, \mathsf{t}, \mu)$: Taking as input public parameters PP, an identity $\mathsf{id} \in \mathcal{I}$, an encryption time $\mathsf{t} \in \mathcal{T}$ and a message $\mu \in \mathcal{M}$, sample a uniform pair $(\mathsf{k}.\mu, \mathsf{r}.\mu) \in \mathcal{M}^2$ such that $\mu = \mathsf{k}.\mu + \mathsf{r}.\mu$. Run $\mathsf{k.CT} \leftarrow \mathrm{k.Enc}(\mathsf{k.PP}, \mathsf{id}, \mathsf{k}.\mu)$ and $\mathsf{r.CT} \leftarrow \mathrm{r.Enc}(\mathsf{r.PP}, \mathsf{id}, \mathsf{t}, \mathsf{r}.\mu)$. It outputs a ciphertext $\mathsf{CT}_{\mathsf{id,t}} = (\mathsf{k.CT}, \mathsf{r.CT})$.
- $\mu \leftarrow \mathrm{Dec}(\mathsf{PP}, \mathsf{DK}_{\mathsf{id,t}}, \mathsf{CT}_{\mathsf{id,t}})$: Taking as input public parameters PP, a decryption key $\mathsf{DK}_{\mathsf{id,t}}$ and a ciphertext $\mathsf{CT}_{\mathsf{id,t}}$, run $\mathsf{k}.\mu \leftarrow \mathrm{k.Dec}(\mathsf{k.PP}, \mathsf{k.SK}_{\mathsf{id}}, \mathsf{k.CT})$ and $\mathsf{r}.\mu \leftarrow \mathrm{r.Dec}(\mathsf{r.PP}, \mathsf{r.DK}_{\mathsf{id,t}}, \mathsf{r.CT})$. If $\mathsf{k}.\mu = \perp$ or $\mathsf{r}.\mu = \perp$, it output $\perp$. Otherwise, it outputs a message $\mu = \mathsf{k}.\mu + \mathsf{r}.\mu \in \mathcal{M}$.
- $\mathsf{RL} \leftarrow \mathrm{KeyRev}(\mathsf{id}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$: Taking as input an identity to be revoked $\mathsf{id} \in \mathcal{I}$, a revocation time $\mathsf{t} \in \mathcal{T}$, a revocation list RL and a state ST, run $\mathsf{r.RL} \leftarrow \mathrm{r.KeyRev}(\mathsf{id}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$. It outputs an updated revocation list RL=$\mathsf{r.RL}$.

The correctness of our scheme Π relies on the correctness of each building block, i.e., k.Π and r.Π. The security of Π is given as follows.

Theorem 2. Assuming the IBE scheme k.Π is KDM-sID-CPA secure (resp. KDM-ID-CPA) with the private key with respect to the affine functions $\mathcal{F}$ and the RIBE scheme r.Π is IND-sID-CPA secure (resp. IND-ID-CPA), then the scheme Π is KDM-sID-CPA secure (resp. KDM-ID-CPA) with the private key with respect to $\mathcal{F}$.

Proof. (Sketch) Since the proofs for the selective chosen-identity model and the adaptive chosen-identity model are the same, we only consider the proof in the selective chosen-identity model. Let id^* and t^* be the target identity and time. Denote Q the number of extraction queries issued by the adversary $\mathcal{A}$. For $1 \leq i \leq Q$, let $\mathsf{SK}_{\mathsf{id}_i}$ denote the queried private key on identity id_i. For simplicity, we divide $\mathcal{A}$ into two types:

- Type I : for $\forall i \in [Q]$, $\mathsf{SK}_{\mathsf{id}^*} \neq \mathsf{SK}_{\mathsf{id}_i}$. That means, $\mathcal{A}$ does not issue the extraction query on id^*.
- Type II : for some $i \in [Q]$, $\mathsf{SK}_{\mathsf{id}^*} = \mathsf{SK}_{\mathsf{id}_i}$. That means, $\mathcal{A}$ learns the private key $\mathsf{SK}_{\mathsf{id}^*}$ by the extraction query, but id^* is revoked at t^*.

Combining the Lemmas 5 and 6, the advantage of $\mathcal{A}$ is negligible. □

Lemma 5. If $\mathcal{A}$ is a successful adversary of Type I, there exists a PPT simulator $\mathcal{B}$ attacking the underlying KDM-IBE scheme with non-negligible probability.

Lemma 6. If $\mathcal{A}$ is a successful adversary of Type II, there exists a PPT simulator $\mathcal{B}$ attacking the underlying RIBE scheme with non-negligible probability.

Remark 1. Especially, our RIBE construction Π is even d-KDM-secure if the underlying IBE scheme k.Π is d-KDM secure, where d is the private key clique size.

5 KDM Security for RIBE with the Decryption Key

In this section, we present a concrete construction for KDM-secure RIBE with the decryption key in the selective chosen-identity model.

5.1 Our KDM-RIBE Scheme

In our construction, we use the instance of [1] to deal with user's identity and another IBE instance to handle the time. As in [1], we use an additive group $\mathbb{G} = \mathbb{Z}_q^n$ and a ring $R = \mathbb{Z}_q[x]/(F(x))$, where $F(x)$ is a monic and irreducible polynomial with degree n and $\mathbb{G}$ is an R-module[5]. Let p be the smallest prime divisor of q, and we define $U = \{u_0 = 0, u_1, u_2, \dots\} \subseteq R$ as the set consisting of all the polynomials having coefficients in $\mathbb{Z}_p$, which makes $|U| = p^n \geq 2^n$ and $u_i - u_j$ a unit for any $i \neq j$. (See detailed discussion in [1].)

Suppose identity id and time t are encoded into $U \backslash \{0\}$ respectively and our RIBE scheme from lattices is described below.

- $(\mathsf{PP}, \mathsf{MK}, \mathsf{RL}, \mathsf{ST}) \leftarrow$ **Setup**$(1^n, N)$: On input a security parameter n and a maximal number N of users, perform the following steps:
  1. Sample $\mathbf{R}_1, \mathbf{R}_2 \leftarrow D^{m \times w}_{\mathbb{Z}, \omega(\sqrt{\log n})}$, choose uniformly random $\mathbf{A} \xleftarrow{r} \mathbb{Z}_q^{n \times m}$, $\mathbf{y} \xleftarrow{r} \mathbb{Z}_q^n$ and let $\widetilde{\mathbf{A}}_1 = \mathbf{A}\mathbf{R}_1, \widetilde{\mathbf{A}}_2 = \mathbf{A}\mathbf{R}_2 \in \mathbb{Z}_q^{n \times w}$.
  2. Let RL be an empty set and BT be a binary-tree with at least N leaf nodes, and set ST:=BT.
  3. Output RL, ST, public parameters $\mathsf{PP} = (\mathbf{A}, \widetilde{\mathbf{A}}_1, \widetilde{\mathbf{A}}_2, \mathbf{y})$ and a master secret key $\mathsf{MK} = \{\mathbf{R}_1, \mathbf{R}_2\}$.
- $(\mathsf{SK}_{\mathsf{id}}, \mathsf{ST}) \leftarrow$ **PriKeyGen**$(\mathsf{PP}, \mathsf{MK}, \mathsf{id}, \mathsf{ST})$: On input public parameters PP, a master secret key MK, an identity $\mathsf{id} \in U \backslash \{0\}$ and a state ST, it picks an unassigned leaf node v from BT and stores id in that node. It then performs the following steps:
  1. For any $\theta \in \mathsf{Path}(v)$, if $\mathbf{y}_{\theta,1}, \mathbf{y}_{\theta,2}$ are undefined, pick $\mathbf{y}_{\theta,1} \xleftarrow{r} \mathbb{Z}_q^n$, set $\mathbf{y}_{\theta,2} := \mathbf{y} - \mathbf{y}_{\theta,1}$ and store them in the node θ. Set $\mathbf{A}_{\mathsf{id}} := [\mathbf{A} | (\mathsf{id})\mathbf{G} - \widetilde{\mathbf{A}}_1]$. Sample $\mathbf{z}_0 \leftarrow D^n_{\mathbb{Z},r}$, $\mathbf{e}_{\theta,1} \leftarrow D_{\Lambda^{\perp}_{\mathbf{z}_0 - \mathbf{y}_{\theta,1}}(\mathbf{A}_{\mathsf{id}}), r}$ so that $\mathbf{z}_0 - \mathbf{A}_{\mathsf{id}}\mathbf{e}_{\theta,1} = \mathbf{y}_{\theta,1}$.
  2. Output $\mathsf{SK}_{\mathsf{id}} := \{(\theta, \mathbf{e}_{\theta,1})\}_{\theta \in \mathsf{Path}(v)}$.
- $\mathsf{KU}_{\mathsf{t}} \leftarrow$ **KeyUpd**$(\mathsf{PP}, \mathsf{MK}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$: On input public parameters PP, a master secret key MK, a time $\mathsf{t} \in U \backslash \{0\}$, a revocation list RL and a state ST, it performs the following steps:
  1. For any $\theta \in \mathsf{KUNodes}(\mathsf{BT}, \mathsf{RL}, \mathsf{t})$[6], if $\mathbf{y}_{\theta,1}, \mathbf{y}_{\theta,2}$ are undefined, pick $\mathbf{y}_{\theta,1} \xleftarrow{r} \mathbb{Z}_q^n$, set $\mathbf{y}_{\theta,2} := \mathbf{y} - \mathbf{y}_{\theta,1}$ and store them in the node θ. Set $\mathbf{A}_{\mathsf{t}} := [\mathbf{A} | \mathsf{t}\mathbf{G} - \widetilde{\mathbf{A}}_2]$. Sample $\mathbf{e}_{\theta,2} \leftarrow D_{\Lambda^{\perp}_{-\mathbf{y}_{\theta,2}}(\mathbf{A}_{\mathsf{t}}), r}$, so that $-\mathbf{A}_{\mathsf{t}}\mathbf{e}_{\theta,2} = \mathbf{y}_{\theta,2}$.
  2. Output $\mathsf{KU}_{\mathsf{t}} := \{(\theta, \mathbf{e}_{\theta,2})\}_{\theta \in \mathsf{KUNodes}(\mathsf{BT}, \mathsf{RL}, \mathsf{t})}$.
- $\mathsf{DK}_{\mathsf{id},\mathsf{t}}/\perp \leftarrow$ **DecKeyGen**$(\mathsf{PP}, \mathsf{SK}_{\mathsf{id}}, \mathsf{KU}_{\mathsf{t}})$: On input public parameters PP, a private key $\mathsf{SK}_{\mathsf{id}} := \{(i, \mathbf{e}_{i,1})\}_{i \in \mathsf{I}}$ and update key $\mathsf{KU}_{\mathsf{t}} := \{(j, \mathbf{e}_{j,2})\}_{j \in \mathsf{J}}$ for some sets of nodes I and J, it runs the following steps:

[5] Scalar Multiplication $R \times \mathbb{G} \rightarrow \mathbb{G}$ is defined by identifying each $\mathbf{a} = (a_0, \cdots, a_{n-1})^t \in \mathbb{G}$ with the polynomial $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in R$, multiplying in R, and then mapping back to $\mathbb{G}$.

[6] Due to limit page, we omit the description of $\mathsf{KUNodes}$. Refer to the concrete algorithm in [4]. It takes as input a binary-tree BT, a revocation list RL and time t, and outputs a set of nodes.

1. $\forall(i, \mathbf{e}_{i,1}) \in \mathsf{SK}_{\mathsf{id}}$, $\forall(j, \mathbf{e}_{j,2}) \in \mathsf{KU}_{\mathsf{t}}$, if $\exists(i,j)$ s.t. $i = j$, $\mathsf{DK}_{\mathsf{id},\mathsf{t}} \leftarrow (\mathbf{e}_{i,1}, \mathbf{e}_{j,2})$, else if $\mathsf{SK}_{\mathsf{id}}$ and KU_{t} do not have any node in common, $\mathsf{DK}_{\mathsf{id},\mathsf{t}} \leftarrow \perp$.
2. Output $\mathsf{DK}_{\mathsf{id},\mathsf{t}} := \{(\mathbf{e}_{i,1}, \mathbf{e}_{i,2})\}_{i \in \mathsf{I} \cap \mathsf{J}}$.

- $\mathsf{CT}_{\mathsf{id},\mathsf{t}} \leftarrow \mathbf{Enc}(\mathsf{PP}, \mathsf{id}, \mathsf{t}, \mu)$: On input public parameters PP, an identity $\mathsf{id} \in U \backslash \{0\}$, a time $\mathsf{t} \in U \backslash \{0\}$, and a message $\mu \in \mathbb{Z}_p$:
  1. Set $\mathbf{F}_{\mathsf{id},\mathsf{t}} := [\mathbf{A}|(\mathsf{id})\mathbf{G} - \widetilde{\mathbf{A}}_1|\mathsf{t}\mathbf{G} - \widetilde{\mathbf{A}}_2] \in \mathbb{Z}_q^{n \times (m+2w)}$.
  2. Choose $\mathbf{x}_0 \leftarrow D^n_{\mathbb{Z},r}$, $\mathbf{x}_1^{(1)} \leftarrow D^m_{\mathbb{Z},r}$, $\mathbf{x}_1^{(2)} \leftarrow D^w_{\mathbb{Z},\gamma}, \mathbf{x}_2^{(2)} \leftarrow D^w_{\mathbb{Z},\gamma}$, $x_2 \leftarrow D_{\mathbb{Z},\gamma}$, and set $\mathbf{x}_1^t := [(\mathbf{x}_1^{(1)})^t|(\mathbf{x}_1^{(2)})^t|(\mathbf{x}_2^{(2)})^t] \in \mathbb{Z}_q^{1 \times (m+2w)}$.
  3. Compute $c_0 \leftarrow \mathbf{x}_0^t \mathbf{y} + x_2 + p \cdot \mu \in \mathbb{Z}_q$, $\mathbf{c}_1 \leftarrow \mathbf{x}_0^t \mathbf{F}_{\mathsf{id},\mathsf{t}} + \mathbf{x}_1^t \in \mathbb{Z}_q^{1 \times (m+2w)}$.
  4. Output the ciphertext $\mathsf{CT}_{\mathsf{id},\mathsf{t}} := (c_0, \mathbf{c}_1) \in \mathbb{Z}_q \times \mathbb{Z}_q^{1 \times (m+2w)}$.
- $m \leftarrow \mathbf{Dec}(\mathsf{PP}, \mathsf{DK}_{\mathsf{id},\mathsf{t}}, \mathsf{CT}_{\mathsf{id},\mathsf{t}})$: On input public parameters PP, a decryption key $\mathsf{DK}_{\mathsf{id},\mathsf{t}} := (\mathbf{e}_1, \mathbf{e}_2)$, and a ciphertext $\mathsf{CT}_{\mathsf{id},\mathsf{t}} := (c_0, \mathbf{c}_1)$, it runs the following steps:
  1. Parse $\mathbf{c}_1$ as $[\mathbf{c}_{1,0}|\mathbf{c}_{1,1}|\mathbf{c}_{1,2}] \in \mathbb{Z}_q^{1 \times m} \times \mathbb{Z}_q^{1 \times w} \times \mathbb{Z}_q^{1 \times w}$.
  2. Compute $\mu' \leftarrow c_0 + [\mathbf{c}_{1,0}|\mathbf{c}_{1,1}]\mathbf{e}_1 + [\mathbf{c}_{1,0}|\mathbf{c}_{1,2}]\mathbf{e}_2$.
  3. Output $\mu \in \mathbb{Z}_p$ s.t. μ' is closest to $p \cdot \mu \bmod q$.
- $\mathsf{RL} \leftarrow \mathbf{KeyRev}(\mathsf{id}, \mathsf{t}, \mathsf{RL}, \mathsf{ST})$: On input an identity id, a time t, a revocation list RL and a state ST, the algorithm adds $(\mathsf{id}, \mathsf{t})$ to RL for all nodes associated with identity id and returns RL.

5.2 Correctness and Security

We can set the parameters as follows: $m = \Theta(n \log q)$, Gaussian parameter r needs to be large enough for Gaussian sampling i.e. $r \geq \max\{s_1(\mathbf{R}_1), s_1(\mathbf{R}_2)\} \cdot \omega(\sqrt{\log n}) = O(\sqrt{m} + \sqrt{w}) \cdot \omega(\sqrt{\log n})^2 = O(\sqrt{m}) \cdot \omega(\sqrt{\log n})^2$. On the other hand, the hardness of LWE requires $r \geq 2\sqrt{n}$. For the security proof, we need $\gamma' \geq O(m) \cdot r^2 \cdot \omega(\sqrt{\log n})$ and let $\gamma = \sqrt{r^2 + 2\gamma'^2}$, $p = \gamma \cdot poly(n)$ for a sufficiently large $poly(n)$ term to ensure correctness and modulus $q = p^2$. Now we prove the correctness.

$$\begin{aligned}\mu' &= c_0 + [\mathbf{c}_{1,0}|\mathbf{c}_{1,1}]\mathbf{e}_1 + [\mathbf{c}_{1,0}|\mathbf{c}_{1,2}]\mathbf{e}_2 \\ &= p \cdot \mu + \mathbf{x}_0^t \mathbf{z}_0 + x_2 + [(\mathbf{x}_1^{(1)})^t|(\mathbf{x}_1^{(2)})^t]\mathbf{e}_1 + [(\mathbf{x}_1^{(1)})^t|(\mathbf{x}_2^{(2)})^t]\mathbf{e}_2.\end{aligned}$$

Thus, the decryption is correct if the error term $|\mathbf{x}_0^t \mathbf{z}_0 + x_2 + [(\mathbf{x}_1^{(1)})^t|(\mathbf{x}_1^{(2)})^t]\mathbf{e}_1 + [(\mathbf{x}_1^{(1)})^t|(\mathbf{x}_2^{(2)})^t]\mathbf{e}_2| < \frac{p}{2}$. By the Cauchy-Schwartz equality and Lemma 2, it holds except with negligible probability.

Theorem 3. The above RIBE scheme is KDM-sID-CPA secure with the decryption key with respect to the affine functions over $\mathbb{Z}_p$ under the above parameters under the LWE assumption.

Remark 2. Our scheme is only 1-KDM-sID-CPA secure and it seems hard to prove the d-KDM using our proof strategy. In our simulation of $\mathsf{Type\ I}$, we generate the public parameter $\mathbf{y}$ by setting $\mathbf{y} = \mathbf{y}_{\mathsf{id}^*} + \mathbf{y}_{\mathsf{t}^*}$ with $\mathbf{y}_{\mathsf{id}^*}$ obtained from the challenger and $\mathbf{y}_{\mathsf{t}^*}$ from our computation. However, when considering the d-KDM security, it needs $\mathbf{y}_{\mathsf{id}_1^*}, \cdots, \mathbf{y}_{\mathsf{id}_d^*}$ for the different private keys, which seems hard for us to generate the $\mathbf{y}$, thus making our proof fail.

6 KDM Security for IBE

In this section, we present an efficient KDM-ID-CPA secure IBE scheme in the random oracle model, which can be used as a component of our generic construction of KDM-secure RIBE in Sect. 4.

6.1 KDM-IBE Scheme

The plaintext space is $\mathbb{Z}_p$. The secret key clique size of scheme is d, the parameter $w = n\lceil \log q \rceil$, and the random oracle is $H : U\backslash\{0\} \to \mathbb{Z}_q^n$, where $U\backslash\{0\}$ is the identity space defined as before. The concrete construction is as follows:

- $(\mathsf{PP}, \mathsf{MSK}) \leftarrow$ **Setup**$(1^n, d)$: On input the security parameter n and secret key clique size d, perform the following steps:
  1. Sample $\mathbf{R} \leftarrow D^{m\times w}_{\mathbb{Z},\omega(\sqrt{\log n})}$. Choose a uniform random matrix $\mathbf{A} \xleftarrow{r} \mathbb{Z}_q^{n\times m}$, and let $\widetilde{\mathbf{A}} = -\mathbf{A}\mathbf{R} \in \mathbb{Z}_q^{n\times w}$.
  2. The public parameters is $\mathsf{PP} = \{\mathbf{A}, \widetilde{\mathbf{A}}\}$. The master secret key is $\mathsf{MSK} = \mathbf{R}$.
- $\mathsf{SK}_{\mathsf{id}} \leftarrow$ **Ext**$(\mathsf{PP}, \mathsf{MSK}, \mathsf{id})$: On input the public parameters PP, identity $\mathsf{id} \in U\backslash\{0\}$, and master secret key MSK, it performs the following steps:
  1. Set $\mathbf{A}_{\mathsf{id}} = [\mathbf{A}|(\mathsf{id})\mathbf{G} + \widetilde{\mathbf{A}}] \in \mathbb{Z}_q^{n\times(m+w)}$ and $\mathbf{y}_{\mathsf{id}} = H(\mathsf{id}) \in \mathbb{Z}_q^n$.
  2. Sample $\mathbf{z}_0 \leftarrow D^n_{\mathbb{Z},r}$, $\mathbf{z}_1 \leftarrow D^{m+w}_{\Lambda^{\perp}_{\mathbf{z}_0 - \mathbf{y}_{\mathsf{id}}}(\mathbf{A}_{\mathsf{id}}),\sigma}$ such that $\mathbf{y}_{\mathsf{id}} = \mathbf{z}_0 - \mathbf{A}_{\mathsf{id}}\mathbf{z}_1$.
  3. Output $\mathsf{SK}_{\mathsf{id}} := \mathbf{z}_1$.
- $\mathsf{CT} \leftarrow$ **Enc**$(\mathsf{PP}, \mathsf{id}, \mu)$: On input the public parameters PP, identity $\mathsf{id} \in U\backslash\{0\}$ and message $\mu \in \mathbb{Z}_p$, perform the following steps:
  1. Let $\mathbf{A}_{\mathsf{id}} = [\mathbf{A}|(\mathsf{id})\mathbf{G} + \widetilde{\mathbf{A}}]$ and $\mathbf{y}_{\mathsf{id}} = H(\mathsf{id}) \in \mathbb{Z}_q^n$.
  2. Choose $\mathbf{x}_0 \leftarrow D^n_{\mathbb{Z},r}, \mathbf{x}_1 \leftarrow D^{m+w}_{\mathbb{Z},r}$ and $x_2 \leftarrow D_{\mathbb{Z},r}$. Compute $\mathbf{c}^t = \mathbf{x}_0^t[\mathbf{A}_{\mathsf{id}}|\mathbf{y}_{\mathsf{id}}] + [\mathbf{x}_1^t|x_2] + [\mathbf{0}|p\cdot\mu] \in \mathbb{Z}_q^{1\times(m+w+1)}$.
  3. Output $\mathsf{CT} := \mathbf{c}^t$.
- $\mu \leftarrow$ **Dec**$(\mathsf{PP}, \mathsf{SK}_{\mathsf{id}}, \mathsf{CT})$: On input the public parameters PP, private key $\mathsf{SK}_{\mathsf{id}}$ and ciphertext CT, perform the following steps:
  1. Compute $\mu' = \mathbf{c}^t \begin{bmatrix}\mathbf{z}_1\\ 1\end{bmatrix} \in \mathbb{Z}_q$.
  2. Output the $\mu \in \{0,\ldots,p-1\} = \mathbb{Z}_p$ such that μ' is closest to $p\cdot\mu \mod q$.

By Lemma 2, we set $m = \Theta(n\log q)$, and Gaussian parameter $r \geq 2\sqrt{n}$ to satisfy the reductions from LWE to worst-case lattice problems [17] and $\sigma \geq s_1(\mathbf{R})\cdot\omega(\sqrt{\log n}) \geq O(\sqrt{m})\cdot\omega(\sqrt{\log n})^2$ and set $\sigma = r\cdot O(\sqrt{m+\omega})\cdot\omega(\sqrt{\log n})$. For correctness, we let message space size $p \geq \sigma^2(n+m+w)\cdot\omega(\sqrt{\log n})$ and $q = p^2$.

6.2 Security of KDM-IBE Scheme

We analyze the security in both the classical random oracle and quantum random oracle model.

Theorem 4. The IBE system described above is d-KDM-ID-CPA secure with the affine functions over $\mathbb{Z}_p$ for the arbitrary constant d in the classical random oracle model under the LWE assumption.

In the quantum random oracle model (QROM), similar to [22], replacing the random oracle with a semi-constant distribution SC_λ[7], we can get the 1-KDM security in the QROM. However, when extending to the d-KDM security in the QROM, such technique fails. The main obstacle is how to embed d challenges simultaneously. When plugging d challenges to the random oracle queries like [22], the adversary may detect its non-randomness. In details, we can define a d-leveled semi-constant distribution $\mathsf{SC}_{d,\lambda}$, which makes d patches with d constant values with some probability and others are random values. By Corollary 4.3 in [22], there is at most a distance $\frac{8}{3}d{q_H}^4\lambda^2$ between $\mathsf{SC}_{d,\lambda}$ and the true random oracle. However, in the security proof, compared to the adversary's advantage $O(\lambda^d)$, this distance seems too large. Thus, it makes the original proof strategy fail. Besides, Katsumata et al. [13] provided a tighter security reduction for GPV-IBE in QROM by programming the random oracle the same way for all identities. However, it seems not easy to apply their techniques to our setting. We leave the d-KDM security in the quantum world as the further work.

Acknowledgement. The authors would like to thank the anonymous reviewers for their valuable comments. This work was supported in part by National Natural Science Foundation of China (Nos. 61632020, 61472416, 61772520), Key Research Project of Zhejiang Province (No. 2017C01062), Fundamental Theory and Cutting-Edge Technology Research Program of Institute of Information Engineering, CAS (No. Y7Z0321102).

References

1. Alperin-Sheriff, J., Peikert, C.: Circular and KDM security for identity-based encryption. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 334–352. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_20
2. Applebaum, B., Cash, D., Peikert, C., Sahai, A.: Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 595–618. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03356-8_35

[7] The definition of semi-constant distribution in [22] plays an essential role in the security proof of GPV IBE in the QROM, which makes a random value inserted into a small but significant fraction of oracle inputs. When replacing the oracle with the semi-constant distribution, the adversary can use the challenge with significant probability, which cannot be detected by the quantum adversary.

3. Black, J., Rogaway, P., Shrimpton, T.: Encryption-scheme security in the presence of key-dependent messages. In: Nyberg, K., Heys, H. (eds.) SAC 2002. LNCS, vol. 2595, pp. 62–75. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-36492-7_6
4. Boldyreva, A., Goyal, V., Kumar, A.: Identity-based encryption with efficient revocation. In: Ning, P., Syverson, P.E., Jha, S. (eds.) CCS 2008. ACM, New York (2008)
5. 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). https://doi.org/10.1007/3-540-44647-8_13
6. Boneh, D., Halevi, S., Hamburg, M., Ostrovsky, R.: Circular-secure encryption from decision Diffie-Hellman. In: Wagner, D. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 108–125. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-85174-5_7
7. Brakerski, Z., Goldwasser, S., Kalai, Y.T.: Black-box circular-secure encryption beyond affine functions. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 201–218. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19571-6_13
8. Chen, J., Lim, H.W., Ling, S., Wang, H., Nguyen, K.: Revocable identity-based encryption from lattices. In: Susilo, W., Mu, Y., Seberry, J. (eds.) ACISP 2012. LNCS, vol. 7372, pp. 390–403. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31448-3_29
9. Chen, Y., Zhang, J., Deng, Y., Chang, J.: KDM security for identity-based encryption: Constructions and separations. IACR Cryptology ePrint Archive 2016, 1020 (2016). http://eprint.iacr.org/2016/1020
10. Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. In: Dwork, C. (ed.) Proceedings of the 40th Annual ACM Symposium on Theory of Computing, pp. 197–206. ACM (2008)
11. Katsumata, S., Matsuda, T., Takayasu, A.: Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. IACR Cryptology ePrint Archive 2018, 420 (2018). https://eprint.iacr.org/2018/420
12. Katsumata, S., Yamada, S.: Partitioning via non-linear polynomial functions: more compact IBEs from ideal lattices and bilinear maps. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part II. LNCS, vol. 10032, pp. 682–712. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53890-6_23
13. Katsumata, S., Yamada, S., Yamakawa, T.: Tighter security proofs for GPV-IBE in the quantum random oracle model. IACR Cryptology ePrint Archive 2018, 451 (2018). https://eprint.iacr.org/2018/451
14. Kitagawa, F., Tanaka, K.: Key dependent message security and receiver selective opening security for identity-based encryption. In: Abdalla, M., Dahab, R. (eds.) PKC 2018. LNCS, vol. 10769, pp. 32–61. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-76578-5_2
15. Micciancio, D., Peikert, C.: Trapdoors for lattices: simpler, tighter, faster, smaller. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 700–718. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29011-4_41
16. Micciancio, D., Regev, O.: Worst-case to average-case reductions based on gaussian measures. In: 45th Symposium on Foundations of Computer Science (FOCS 2004), pp. 372–381. IEEE Computer Society (2004)
17. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) Proceedings of the 37th Annual ACM Symposium on Theory of Computing, pp. 84–93. ACM (2005)

18. Seo, J.H., Emura, K.: Revocable identity-based encryption revisited: security model and construction. In: Kurosawa, K., Hanaoka, G. (eds.) PKC 2013. LNCS, vol. 7778, pp. 216–234. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-36362-7_14

19. Shamir, A.: Identity-based cryptosystems and signature schemes. In: Blakley, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 47–53. Springer, Heidelberg (1985). https://doi.org/10.1007/3-540-39568-7_5

20. Takayasu, A., Watanabe, Y.: Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In: Pieprzyk, J., Suriadi, S. (eds.) ACISP 2017. LNCS, vol. 10342, pp. 184–204. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60055-0_10

21. 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). https://doi.org/10.1007/978-3-662-49387-8_7

22. Zhandry, M.: Secure identity-based encryption in the quantum random oracle model. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 758–775. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_44