mathematics

MDPI

Article

Revocable-Attribute-Based Encryption with En-DKER from Lattices

Qi Wang [1], Juyan Li [1], Zhedong Wang [2,3] and Yanfeng Zhu [1,*]

[1] College of Data Science and Technology, Heilongjiang University, Harbin 150080, China
[2] School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[3] State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
* Correspondence: 2001111@hlju.edu.cn

Abstract: Cloud computing offers abundant computing resources and scalable storage, but data leakage in the cloud storage environment is a common and critical concern due to inadequate protection measures. Revocable-attribute-based encryption (RABE) is introduced as an advanced form of identity-based encryption (IBE), which encrypts sensitive data while providing fine-grained access control and an effective user revocation mechanism. However, most existing RABE schemes are not resistant to quantum attacks and are limited in their application scenarios due to the revocation model. In this paper, we propose a RABE scheme constructed from lattices. Our scheme has several advantages, including a near-zero periodic workload for the key generation center (KGC), ensuring scalability as the number of users increases. Additionally, the encryptor is relieved from managing a revocation list. Moreover, our scheme guarantees the confidentiality and privacy of other ciphertexts even if the decryption key for a specific period is compromised. We validated the correctness of our scheme and demonstrated its security under the assumption of learning with errors (LWE), which is widely believed to be resistant to quantum attacks. Finally, we provide an application example of our RABE scheme in the electronic healthcare scenario.

Keywords: revocable-attribute-based encryption; enhanced decryption key exposure; lattice-based cryptography

MSC: 68P25; 81P94; 94A60

Citation: Wang, Q.; Li, J.; Wang, Z.; Zhu, Y. Revocable-Attribute-Based Encryption with En-DKER from Lattices. *Mathematics* **2023**, *11*, 4986. https://doi.org/10.3390/math11244986

Academic Editor: Antanas Cenys

Received: 20 November 2023
Revised: 14 December 2023
Accepted: 15 December 2023
Published: 17 December 2023

1. Introduction

Attribute-based encryption (ABE), introduced by Sahai and Waters [1], is regarded as an advanced variant of identity-based encryption (IBE). Its decryption process only becomes viable when the attributes meet the specified policy, thereby providing a cryptographic primitive for encryption with fine-grained access control. ABE manifests in two distinct forms: ciphertext-policy and key-policy. In ciphertext-policy ABE (CP-ABE) [2,3], ciphertexts are associated with access policies and keys are associated with attributes. Conversely, in key-policy ABE (KP-ABE) [4,5], ciphertexts are associated with attributes and keys are associated with access policies. In this paper, we focus our discussion on KP-ABE.

Over the years, ABE has evolved into a foundational cryptographic primitive, displaying vast potential applications. Researchers have proposed numerous enhanced and extended ABE schemes [4–8] to address essential facets such as expressiveness, efficiency, and security. Notably, ABE schemes resistant to quantum computers, especially those based on lattice cryptography, have received significant attention. The development of these quantum-resistant schemes addresses vital aspects while also presenting new challenges.

In many practical applications of ABE, an efficient revocation mechanism is crucial when users become malicious or their secret keys are compromised. Boneh and Franklin [9]

proposed a solution where the key generation center (KGC) periodically generates keys for all non-revoked users. However, this approach results in a periodic workload of $O(N-r)$ for the KGC, potentially becoming a bottleneck as the number of users grows, where N and r represent the maximum number of users and revoked users, respectively. Boldyreva et al. [10] introduced an indirect revocation model employing a binary tree structure and subset-cover framework, effectively reducing the periodic workload of the KGC to $O(r\log(N/r))$, a more scalable approach.

Following the work of Boldyreva et al. [10], Chen et al. [11] presented the first lattice-based indirect revocation IBE (RIBE) scheme. However, when extending this scheme to ABE, conflicts arise between fine-grained access control and the coarse-grained binary tree employed for user revocation, presenting challenges for security proofs. So is there a revocable-attribute-based encryption (RABE) from lattices that the encryptor does not need to manage the revocation list?

There have been a few exciting attempts towards addressing this problem [12–14]. However, these schemes adopt a direct revocation model proposed by Attrapadung and Imai [15] that eliminates the need for periodic key updates by both the KGC and users. Nevertheless, the encryptor must manage the revocation list and generate ciphertext that can only be decrypted by non-revoked users in specific scenarios.

In practical scenarios, the leakage of decryption keys from external attacks or user errors is frequently observed. Addressing this concern, Seo and Emura [16] introduced a significant security concept known as decryption key exposure resistance (DKER). DKER mandates that the exposure of decryption keys for any time period should not compromise the confidentiality of ciphertexts encrypted for distinct time periods within the context of RIBE schemes. By re-randomizing decryption keys, it is conceivable that the scheme can fulfill the DKER property. Several RABE schemes, relying on number theoretical assumptions, have been proposed to achieve DKER [17–19].

Nevertheless, the algebraic structure of lattices makes the re-randomization of a specific key challenging. This difficulty arises because, if a user generates a new decryption key that ensures correctness without possessing knowledge of the trapdoor, they would also have the capability to solve the Small Integer Solution (SIS) problem. So is there a RABE with DKER from lattices?

Katsumata et al. [20] proposed an approach to achieve the partial key re-randomization property from lattices and constructed the first lattice-based RIBE scheme with DKER. Their scheme adopts a two-level structure, where the first level incorporates [11] for revocation, while the second level relies on any lattice-based HIBE scheme [21,22] to fulfill the DKER property. However, this two-level structure cannot be extended to ABE. In ABE, multiple users may correspond to the same policy. Consequently, a revoked user can combine the decryption keys leaked by non-revoked users with the same policy to generate new decryption keys for other time periods.

1.1. Related Work

Qin et al. [23] proposed a server-aided revocation model, utilizing an untrusted server for periodic key updates instead of relying on the user. This innovative approach enables users to achieve arbitrary period decryption while maintaining only a constant-level secret key, thus significantly reducing the user's workload. Recently, Wang et al. [24] proposed a novel revocation model with a nearly negligible periodic workload for the KGC. Unlike direct revocation, this model eliminates the need for the encryptor to manage a revocation list. Additionally, they introduced a lattice basis delegation approach, enabling the delegation of sampling operations to an untrusted server. This approach significantly reduces the periodic workload associated with user decryption key generation.

Takayasu and Watanabe [25,26] integrated anonymity and DKER for the first time, constructing a RIBE scheme with bounded DKER (B-DKER) and anonymity. Anonymity, as defined by Boyen [27], guarantees that encrypted ciphertext must not reveal the recipient's identity. Simultaneously, B-DKER ensures the security of RIBE schemes under a

priori bounded exposure of decryption keys, representing a weak version of DKER. In a subsequent development, Wang et al. [24] introduced an enhanced form of DKER, named enhanced DKER (En-DKER). En-DKER extends the requirement by ensuring that the exposure of decryption keys in any time period cannot compromise the confidentiality and anonymity of ciphertexts in other time periods.

Wang et al. [28] and Yang et al. [29] proposed two revocable CP-ABE schemes under the learning with errors (LWE) assumption. Furthermore, Yang et al. [30] presented a revocable and multi-authority CP-ABE from the ring learning with errors (RLWE) assumption. Dong et al. [31] proposed a lattice-based RABE scheme with DKER. Huang et al. [32] proposed a multiple authorities CP-ABE scheme with DKER from lattices.

1.2. Technical Overview

Here, we provide a detailed analysis of the difficulties associated with the two open problems mentioned earlier in the introduction. Subsequently, we present the construction approach for our lattice-based RABE with the En-DKER scheme.

First, we define the symbols that may be used in the following discussions. $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{W}$ are matrices in $\mathbb{Z}_q^{n\times m}$, $\mathbf{T_A}$ is the trapdoor of the matrix $\mathbf{A}$, and $\mathbf{u}$ and $\mathbf{s}$ are random vectors in $\mathbb{Z}_q^n$. $\mathbf{B}_{ID}$ and $\mathbf{W}_t$ are random matrices of identity ID and time period t in $\mathbb{Z}_q^{n\times m}$ based on $\mathbf{B}$ and $\mathbf{W}$, respectively. In addition, the KGC manages a binary tree BT and randomly selects a particular leaf node η_{ID} for each identity ID. $\mathsf{Path}(\eta_{ID})$ and $\mathsf{KUNodes}(\mathsf{RL_t})$ are two node sets, where the former represents all nodes on the path from the leaf node η_{ID} to the root, and the latter represents the smallest nodes subset of non-revoked users in time period t. The detailed introduction of algorithm KUNodes is in Lemma 8. Assuming that an identity ID has not been revoked at time period t, there must be a node $\theta^* = \mathsf{Path}(\eta_{ID}) \cap \mathsf{KUNodes}(\mathsf{RL_t})$. For each node $\theta \in \mathsf{BT}$, select a uniformly random vector $\mathbf{u}_\theta$ in $\mathbb{Z}_q^n$.

We recall Chen et al.'s [11] RIBE scheme from lattices. As shown in Figure 1, the scheme consists of six algorithms: Setup, GenSK, KeyUp, GenDK, Enc, and Dec. The algorithm GenSK is run by the KGC to generate the secret key $\{\mathbf{sk}_{ID,\theta}\}_{\theta\in\mathsf{Path}(\eta_{ID})}$ for the identity ID. The KGC periodically runs the algorithm KeyUp, inputs the revocation list RL_t, and outputs and broadcasts the key update $\{\mathbf{ku}_{t,\theta}\}_{\theta\in\mathsf{KUNodes}(\mathsf{RL}_t)}$. If the user ID has not been revoked at time period t, he can generate the decryption key $\mathbf{dk}_{ID,t}$ by adding $\mathbf{sk}_{ID,\theta^*}$ and $\mathbf{ku}_{t,\theta^*}$ in a component-wise fashion. Conversely, if the user ID is revoked, there is no intersection node between the two node sets, $\mathbf{u}_\theta$ cannot be eliminated, and thus the decryption key $\mathbf{dk}_{ID,t}$ cannot be calculated.

$\mathsf{Setup} \to (\mathsf{PP}, \mathsf{MSK})$:	$\mathsf{PP} = (\mathbf{A}, \mathbf{B}, \mathbf{W}, \mathbf{u})$, $\mathsf{MSK} = \mathbf{T_A}$.
$\mathsf{GenSK} \to \{\mathbf{sk}_{ID,\theta}\}_{\theta\in\mathsf{Path}(\eta_{ID})}$:	s.t. $[\mathbf{A}\|\mathbf{B}_{ID}]\mathbf{sk}_{ID,\theta} = \mathbf{u}_\theta$.
$\mathsf{KeyUp} \to \{\mathbf{ku}_{t,\theta}\}_{\theta\in\mathsf{KUNodes}(\mathsf{RL}_t)}$:	s.t. $[\mathbf{A}\|\mathbf{W}_t]\mathbf{ku}_{t,\theta} = \mathbf{u} - \mathbf{u}_\theta$.
$\mathsf{GenDK} \to \mathbf{dk}_{ID,t}$:	s.t. $[\mathbf{A}\|\mathbf{B}_{ID}\|\mathbf{W}_t]\mathbf{dk}_{ID,t} = \mathbf{u}$.
$\mathsf{Enc} \to (c_0, \mathbf{c}_{ID,t})$:	$c_0 = \mathbf{s}^\top\mathbf{u} + \lfloor\frac{q}{2}\rfloor \cdot \mu + noise$,
	$\mathbf{c}_{ID,t} = \mathbf{s}^\top[\mathbf{A}\|\mathbf{B}_{ID}\|\mathbf{W}_t] + \mathbf{noise}$.

Figure 1. Chen et al.'s [11] RIBE scheme.

However, when extending Chen et al.'s [11] RIBE to RABE, conflicts arise between fine-grained access control and the coarse-grained binary tree employed for user revocation, presenting challenges for security proofs.

Specifically, in the security proof of [11], if the challenge identity ID^* is revoked, the adversary can still make secret key queries for ID^*. It should be noted that, in this case, the challenger cannot utilize SampleRight for generation. Instead, for each $\theta \in \mathsf{Path}(\eta_{ID^*})$, a random vector is chosen as the secret key $\mathbf{sk}_{ID^*,\theta}$, and $\mathbf{u}_\theta$ is assigned the value $\mathbf{sk}_{ID^*,\theta}$ multiplied by $[\mathbf{A}|\mathbf{B}_{ID^*}]$. However, in ABE schemes, there may be multiple policies that satisfy the challenge attribute set $\mathbf{x}^*$, and a policy may correspond to multiple users as well.

This means that there could be multiple revoked users who satisfy $\mathbf{x}^*$. When responding to the adversary's secret key queries using the same method, there will be overlapping node sets in $\mathsf{Path}(\eta_{ID})$, leading to conflicts in $\mathbf{u}_\theta$. Furthermore, if we set $\mathbf{u}_{ID,\theta}$ for each ID, the update key will be directly related to the ID, which will bring us back to the original scheme [9], where the KGC's period workload is $O(N-r)$.

Chen et al.'s RIBE scheme from lattices [11] does not satisfy DKER. Specifically, if the decryption key $dk_{ID,t}$ in time period t is exposed, the adversary can use the key update $\mathbf{ku}_{t,\theta^*}$ to recover the secret key $\mathbf{sk}_{ID,\theta^*}$. As a result, the adversary can do whatever the user with the identity ID can do. Katsumata et al. [20] constructed the first RIBE scheme with DKER from lattices. As shown in Figure 2, $\bar{\mathbf{A}}$ is a matrix in $\mathbb{Z}_q^{n\times m}$, and $\mathbf{T}_{\bar{\mathbf{A}}}$ is the trapdoor of the matrix $\bar{\mathbf{A}}$. $\bar{\mathbf{s}}$ is a random vector in $\mathbb{Z}_q^n$. They divided the ciphertext and decryption key into two levels, where the first level incorporates [11] for revocation, while the second level relies on any lattice-based HIBE scheme [21,22] to fulfill the DKER property.

$$
\begin{array}{ll}
\mathsf{Setup} \to (\mathsf{PP}, \mathsf{MSK}): & \mathsf{PP} = (\mathbf{A}, \boxed{\bar{\mathbf{A}}}, \mathbf{B}, \mathbf{W}, \mathbf{u}),\ \mathsf{MSK} = (\mathbf{T}_{\mathbf{A}}, \boxed{\mathbf{T}_{\bar{\mathbf{A}}}}).\\
\mathsf{GenSK} \to \{\mathbf{sk}_{ID,\theta}\}_{\theta\in\mathsf{Path}(\eta_{ID})}: & \text{s.t. } [\mathbf{A}|\mathbf{B}_{ID}]\mathbf{sk}_{ID,\theta} = \mathbf{u}_\theta.\\
\mathsf{KeyUp} \to \{\mathbf{ku}_{t,\theta}\}_{\theta\in\mathsf{KUNodes}(\mathsf{RL}_t)}: & \text{s.t. } [\mathbf{A}|\mathbf{W}_t]\mathbf{ku}_{t,\theta} = \mathbf{u} - \mathbf{u}_\theta.\\
\mathsf{GenDK} \to (\mathbf{dk}_{ID,t}, \boxed{\overline{\mathbf{dk}}_{ID,t}}): & \text{s.t. } [\mathbf{A}|\mathbf{B}_{ID}|\mathbf{W}_t]\mathbf{dk}_{ID,t} = \mathbf{u}.\\
 & \text{s.t. } \boxed{[\bar{\mathbf{A}}|\mathbf{B}_{ID}|\mathbf{W}_t]\overline{\mathbf{dk}}_{ID,t} = \mathbf{u}}.\\
\mathsf{Enc} \to (c_0, \mathbf{c}_{ID,t}, \boxed{\bar{\mathbf{c}}_{ID,t}}): & c_0 = (\mathbf{s} + \boxed{\bar{\mathbf{s}}})^\top\mathbf{u} + \lfloor\tfrac{q}{2}\rfloor\cdot\mu + noise,\\
 & \mathbf{c}_{ID,t} = \mathbf{s}^\top[\mathbf{A}|\mathbf{B}_{ID}|\mathbf{W}_t] + \mathbf{noise},\\
 & \boxed{\bar{\mathbf{c}}_{ID,t} = \bar{\mathbf{s}}^\top[\bar{\mathbf{A}}|\mathbf{B}_{ID}|\mathbf{W}_t] + \mathbf{noise}}.
\end{array}
$$

Figure 2. Katsumata et al.'s [20] RIBE scheme with DKER.

However, this two-level structure cannot be extended to ABE. In ABE, multiple users may correspond to the same policy. Consequently, a revoked user can use his own partial secret key $\mathbf{T}_{[\bar{\mathbf{A}}|\mathbf{B}_{ID}]}$ and combine the decryption keys leaked by non-revoked users with the same policy to generate new decryption keys for other time periods. Interestingly, this issue also leads to the inability of [20] to guarantee anonymity in the event of decryption key leakage.

As shown in Figure 3, Wang et al. [24] constructed the first RIBE scheme with En-DKER from lattices. Luckily, their scheme provided a good solution approach. First, it associates the ciphertext with $\mathsf{KUNodes}(\mathsf{RL}_t)$ so that, when the challenger replies to the secret key query, it can be separated according to the access structure as well as whether the node belongs to the challenge nodes set $\mathsf{KUNodes}(\mathsf{RL}_t)^*$. This effectively solves the problem encountered when [11] is extended to ABE. Furthermore, unlike partial secret key re-randomization using a two-level structure in [20], Wang et al.'s scheme [24] achieved full secret key re-randomization. In this way, we can cleverly avoid the collusion problem encountered when extending [20] to ABE. By combining Wang et al.'s revocation model [24] with the BGG+14 [33], we propose the first RABE with En-DKER from lattices.

$$
\begin{array}{ll}
\mathsf{Setup} \to (\mathsf{PP}, \mathsf{MSK}): & \mathsf{PP} = (\mathbf{A}, \mathbf{B}, \mathbf{W}, \boxed{\{\overline{\mathbf{D}}_\theta\}_{\theta\in\mathsf{BT}}}, \mathbf{u}),\ \mathsf{MSK} = \mathbf{T}_{\mathbf{A}}.\\
\mathsf{GenSK} \to \{\mathbf{sk}_{ID,\theta}\}_{\theta\in\mathsf{Path}(\eta_{ID})}: & \text{s.t. } \boxed{[\mathbf{A}|\mathbf{B}_{ID}|\mathbf{D}_\theta]\mathbf{sk}_{ID,\theta} = \mathbf{G}}.\\
\boxed{\mathsf{NodesUp} \to \mathsf{KUNodes}(\mathsf{RL}_t)}. & \\
\mathsf{GenDK} \to \boxed{\mathbf{dk}_{ID,\theta^*,t}}: & \text{s.t. } \boxed{[\mathbf{A}|\mathbf{B}_{ID}|\mathbf{D}_{\theta^*}|\mathbf{W}_t]\mathbf{dk}_{ID,\theta^*,t} = \mathbf{u}}.\\
\mathsf{Enc} \to (c_0, \boxed{\{\mathbf{c}_{ID,\theta,t}\}_{\theta\in\mathsf{KUNodes}(\mathsf{RL}_t)}}): & c_0 = \mathbf{s}^\top\mathbf{u} + \lfloor\tfrac{q}{2}\rfloor\cdot\mu + noise,\\
 & \boxed{\mathbf{c}_{ID,\theta,t} = \mathbf{s}^\top[\mathbf{A}|\mathbf{B}_{ID}|\mathbf{D}_\theta|\mathbf{W}_t] + \mathbf{noise}}.
\end{array}
$$

Figure 3. Wang et al.'s [24] RIBE scheme with En-DKER.

1.3. Our Contributions

This paper makes the following contributions:

We extend the En-DKER property proposed by Wang et al. [24] in RIBE to RABE. Specifically, the leakage of any time period decryption keys should not compromise the confidentiality of ciphertexts from other time periods. At the same time, adversaries are unable to determine whether the attribute set of the ciphertext for the challenge time period satisfies a specific policy using keys from any other time periods or policies.

By combining Wang et al.'s revocation model [24] with the BGG+14 [33], we propose the first RABE with En-DKER from lattices. Our scheme cleverly avoids the security proof challenges faced when extending Chen et al.'s RIBE scheme [11] to RABE and the collusion issues encountered when extending Katsumata et al.'s RIBE with the DKER scheme [20] to ABE. It is noteworthy that our scheme retains the advantages of near-zero periodic workload for the KGC, and the encryptor does not need to manage a revocation list.

Finally, we validate the correctness and prove the security of our scheme under the LWE assumption.

2. Preliminaries

2.1. Notations

In this paper, we denote the underlying security parameter as λ. We use PPT to represent probabilistic polynomial time. We represent vectors with bold lowercase letters, e.g., $\mathbf{v}$, and matrices with uppercase letters, e.g., $\mathbf{A}$. By default, all vectors are considered column vectors. If n is a positive integer, $[n] = \{1, \ldots, n\}$. For a column vector $\mathbf{x} \in \mathbb{Z}_n$, $||\mathbf{x}||$ denotes the standard Euclidean norm. For a matrix $\mathbf{A} \in \mathbb{R}^{n \times m}$, $\widetilde{\mathbf{A}}$ is the Gram–Schmidt orthogonalization of $\mathbf{A}$, and $||\mathbf{A}||$ is the Euclidean norm of the longest column in $\mathbf{A}$.

The statistical distance between two distributions $\mathcal{D}$ and $\mathcal{D}'$ is denoted as $\mathsf{SD}(\mathcal{D}, \mathcal{D}')$. Two families of distributions $\mathcal{D} = \{\mathcal{D}_\lambda\}_{\lambda \in \mathbb{N}}$ and $\mathcal{D}' = \{\mathcal{D}'_\lambda\}_{\lambda \in \mathbb{N}}$ are considered statistically indistinguishable if there exists a negligible function $\mathsf{negl}(\cdot)$ such that $\mathsf{SD}(\mathcal{D}_\lambda, \mathcal{D}'_\lambda) \leq \mathsf{negl}(\lambda)$ for all $\lambda \in \mathbb{N}$. Here, $\mathsf{negl}(\cdot)$ is a function satisfying $\mathsf{negl}(\lambda) \leq \lambda^{-c}$ for every constant $c > 0$ and an integer N_c, where $\lambda > N_c$.

2.2. Useful Facts

Smudging. The given lemma, originally established in [34], asserts that adding large noise often "smudges out" any small values.

Lemma 1 (Smudging Lemma)**.** *Let B_1 and B_2 be two polynomials over the integers, and let $\mathcal{D} = \{\mathcal{D}_\lambda\}_\lambda$ be any B_1-bounded distribution family. Define $\mathcal{U} = \{\mathcal{U}_\lambda\}_\lambda$ as the uniform distribution over $[-B_2(\lambda), B_2(\lambda)]$. The families of distributions $\mathcal{D} + \mathcal{U}$ and $\mathcal{U}$ are statistically indistinguishable if there exists a negligible function $\mathsf{negl}(\cdot)$ such that for all $\lambda \in \mathbb{N}$, $B_1(\lambda)/B_2(\lambda) \leq \mathsf{negl}(\lambda)$.*

The definition of $\mathcal{B}$-Bounded is as follows.

Definition 1 ($\mathcal{B}$-Bounded)**.** *For a family of distributions $\mathcal{D} = \{\mathcal{D}_\lambda\}_{\lambda \in \mathbb{N}}$ over the integers and a bound $\mathcal{B} = \mathcal{B}(\lambda) > 0$, if for every $\lambda \in \mathbb{N}$ it holds that $Pr_{x \leftarrow \mathcal{D}_\lambda}[|x| \leq \mathcal{B}(\lambda)] = 1$, we say that $\mathcal{D}$ is $\mathcal{B}$-bounded.*

Leftover Hash Lemma. Here, we recall the leftover hash lemma from [21].

Lemma 2. *Suppose $m > (n+1)\log q + \omega(\log n)$. Then, the distribution $(\mathbf{A}, \mathbf{AR})$ is statistically indistinguishable from the distribution $(\mathbf{A}, \mathbf{B})$, where $\mathbf{A}$ and $\mathbf{B}$ are uniformly chosen matrices in $\mathbb{Z}_q^{n \times m}$, and $\mathbf{R}$ is a uniformly chosen matrix in $\{-1, 1\}^{m \times m}$. Simultaneously, $\mathsf{Pr}[||\mathbf{R}|| > 20\sqrt{m}] \leq \mathsf{negl}(m)$.*

Full-Rank Different Map. We need this tool to encode identities and time periods as matrices in $\mathbb{Z}_q^{n \times n}$.

Definition 2. *A function* $\mathsf{H} : \mathbb{Z}_q^n \to \mathbb{Z}_q^{n \times n}$ *is a full-rank different map if the matrix* $\mathsf{H}(\mathbf{u}) - \mathsf{H}(\mathbf{v}) \in \mathbb{Z}_q^{n \times n}$ *is full rank, for all distinct* $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$, *and* H *is computable in* $\mathcal{O}(n \log q)$.

2.3. Background on Lattices

Lattice. Let n, m, and q be positive integers. An m-dimensional lattice, denoted as $\mathcal{L}$, is a discrete subgroup within $\mathbb{R}^m$. Consider $\mathcal{L}_q^{\perp}(\mathbf{A})$, the q-ary lattice defined as $\{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{0} \text{ in } \mathbb{Z}_q\}$, where $\mathbf{A}$ is a matrix in $\mathbb{Z}_q^{n \times m}$. For any $\mathbf{u}$ in $\mathbb{Z}_q^n$, let $\mathcal{L}_q^{\mathbf{u}}(\mathbf{A})$ denote the coset $\{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{u} \text{ in } \mathbb{Z}_q\}$.

Discrete Gaussians. For any parameter $\sigma > 0$, the discrete Gaussian distribution is defined $\rho_{\mathcal{L},\sigma}(\mathbf{x}) = \rho_\sigma(\mathbf{x})/\rho_\sigma(\mathcal{L})$, where $\rho_\sigma(\mathbf{x}) = \exp(-\pi\|\mathbf{x}\|^2/\sigma^2)$ and $\rho_\sigma(\mathcal{L}) = \sum_{\mathbf{x} \in \mathcal{L}} \rho_\sigma(\mathbf{x})$.
The following lemmas represent crucial properties of the discrete Gaussian distribution [35].

Lemma 3. *For positive integers* n, m, q *with* $m > n$, $q > 2$, *and a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, *there exists a negligible function* $\mathsf{negl}(\cdot)$ *such that* $\mathsf{Pr}[||\mathbf{x}|| > \sigma\sqrt{m} : \mathbf{x} \leftarrow \mathcal{D}_{\mathcal{L}_q^{\perp}(\mathbf{A}),\sigma}] \leq \mathsf{negl}(n)$ *when* $\sigma = \tilde{\Omega}(n)$.

Lemma 4. *For positive integers* n, m, q *with* $m > 2n \log q$, *and given* $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$ *and* $\mathbf{e} \leftarrow \mathcal{D}_{\mathbb{Z}^m,\sigma}$, *the distribution of* $\mathbf{u} = \mathbf{A}\mathbf{e} \bmod q$ *is statistically close to the uniform distribution over* $\mathbb{Z}_q^n$.

Trapdoor Generators. The ensuing lemma outlines properties of algorithms designed for generating short bases of lattices.

Lemma 5. *[36–38] For integers* n, m, $q > 0$. *There exist* PPT *algorithms with the following properties:*

- $\mathsf{TrapGen}(1^n, 1^m, q) \to (\mathbf{A}, \mathbf{T}_\mathbf{A})$: *On inputting* n, m, q, *output a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *and its trapdoor* $\mathbf{T}_\mathbf{A} \in \mathbb{Z}^{m \times m}$, *satisfying* $||\mathbf{T}_\mathbf{A}|| \leq O(n \log q)$.
- *There exists a gadget matrix* $\mathbf{G}$, *which is a full-rank matrix in* $\mathbb{Z}_q^{n \times m}$ *and has a publicly known trapdoor* $\mathbf{T}_\mathbf{G}$ *with* $||\widetilde{\mathbf{T}_\mathbf{G}}|| \leq \sqrt{5}$.

Sampling Algorithms. We review some sampling algorithms from [36–38].

Lemma 6. *Let* n, m, *and* q *be positive integers. We have the following* PPT *algorithms:*

- $\mathsf{SamplePre}(\mathbf{A}, \mathbf{T}_\mathbf{A}, \sigma, \mathbf{u}) \to \mathbf{s}$: *Given a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *with trapdoor* $\mathbf{T}_\mathbf{A}$, *a vector* $\mathbf{u} \in \mathbb{Z}_q^n$, *and a parameter* $\sigma \geq ||\widetilde{\mathbf{T}_\mathbf{A}}|| \cdot \omega(\sqrt{\log m})$, *output a vector* $\mathbf{s} \in \mathbb{Z}_q^m$ *satisfying* $\mathbf{A} \cdot \mathbf{s}^\top = \mathbf{u}^\top$ *and* $||\mathbf{s}|| \leq \sqrt{m}\sigma$.
- $\mathsf{SampleLeft}(\mathbf{A}, \mathbf{M}, \mathbf{T}_\mathbf{A}, \sigma, \mathbf{u}) \to \mathbf{s}$: *Given a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ *with trapdoor* $\mathbf{T}_\mathbf{A}$, *a matrix* $\mathbf{M} \in \mathbb{Z}_q^{n \times m_0}$, *a vector* $\mathbf{u} \in \mathbb{Z}_q^n$, *and a parameter* $\sigma \geq ||\widetilde{\mathbf{T}_\mathbf{A}}|| \cdot \omega(\sqrt{\log(m + m_0)})$, *output a vector* $\mathbf{s} \in \mathbb{Z}_q^{m+m_0}$ *distributed statistically close to* $\mathcal{D}_{\mathcal{L}_q^{\mathbf{u}}([\mathbf{A}|\mathbf{M}]),\sigma}$.
- $\mathsf{SampleRight}(\mathbf{A}, \mathbf{G}, \mathbf{R}, \mathbf{T}_\mathbf{G}, \sigma, \mathbf{u}) \to \mathbf{s}$: *Given a matrix* $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, *the gadget matrix* $\mathbf{G}$ *with trapdoor* $\mathbf{T}_\mathbf{G}$, *a uniform random matrix* $\mathbf{R} \leftarrow \{-1, 1\}^{m \times m}$, *a vector* $\mathbf{u} \in \mathbb{Z}_q^n$, *and a parameter* $\sigma \geq ||\widetilde{\mathbf{T}_\mathbf{G}}|| \cdot \sqrt{m} \cdot \omega(\sqrt{\log m})$, *output a vector* $\mathbf{s} \in \mathbb{Z}_q^{2m}$ *distributed statistically close to* $\mathcal{D}_{\mathcal{L}_q^{\mathbf{u}}([\mathbf{A}|\mathbf{A}\mathbf{R}+\mathbf{G}]),\sigma}$.

Hardness Assumption. The security of our revocable ABE scheme is reduced to the learning with errors (LWE) assumption.

Assumption 1 (Learning with Errors [39])**.** *Let* n, m, q *be positive integers, and a parameter* $\sigma \in \mathbb{R}$; *for any PPT adversary* $\mathcal{A}$, *there exists a negligible function* $\mathsf{negl}(\cdot)$ *that satisfies*

$$|\mathsf{Pr}[\mathcal{A}(\mathbf{A}, \mathbf{s}^\top\mathbf{A} + \mathbf{e}) = 1] - \mathsf{Pr}[\mathcal{A}(\mathbf{A}, \mathbf{b}) = 1]| \leq \mathsf{negl}(\lambda),$$

where $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{b} \leftarrow \mathbb{Z}_q^n$, *and* $\mathbf{e} \leftarrow \chi_{\mathsf{LWE}}^m$.

Here, we set χ_{LWE} is a B_{LWE}-bounded distribution. Moreover, Peikert [40] proved that, if $B_{\mathsf{LWE}} \geq \omega(\log n) \cdot \sqrt{n}$, the hardness of the LWE assumption is equivalent to the worst-case GapSVP_γ with parameter $\gamma = 2^{\Omega(n^\varepsilon)}$.

Lattice Evaluation. Here, we review some algorithms that implement the key-homomorphic features from [33,41].

Lemma 7. *Let n, m, and q be positive integers. For any matrices $\mathbf{B}_1, \ldots, \mathbf{B}_\ell \in \mathbb{Z}_q^{n\times m}$, any attribute sets $\mathbf{x} \in \{0,1\}^\ell$, and any Boolean circuit $f : \mathbf{x} \to \{0,1\}$ of depth $\leq d$, set $\mathbf{c}_i = \mathbf{s}^\top(\mathbf{B}_i + x_i\mathbf{G}) + \mathbf{e}_i$, where $i \in [\ell]$, $\mathbf{s} \in \mathbb{Z}_q^n$, and $\mathbf{e}_i \leftarrow \chi_{\mathsf{LWE}}^m$, there exist algorithms $(\mathsf{Eval}_{\mathsf{pk}}, \mathsf{Eval}_{\mathsf{ct}}, \mathsf{Eval}_{\mathsf{sim}})$ with the following properties:*

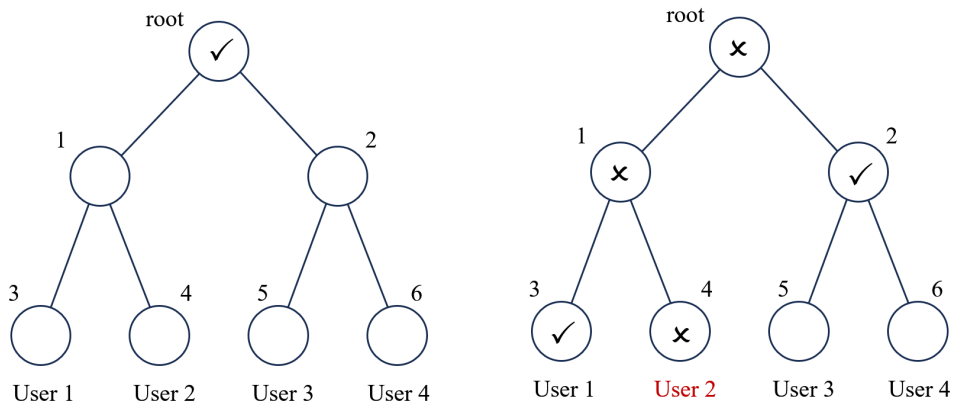
- $\mathsf{Eval}_{\mathsf{pk}}(f, (\mathbf{B}_1, \ldots, \mathbf{B}_\ell)) \to \mathbf{B}_f$*: Given a Boolean circuit f and ℓ matrices $(\mathbf{B}_1, \ldots, \mathbf{B}_\ell)$, output the matrix $\mathbf{B}_f$.*
- $\mathsf{Eval}_{\mathsf{ct}}(f, \{(\mathbf{B}_i, x_i, \mathbf{c}_i)\}_{i\in[\ell]}) \to \mathbf{c}_f$*: For a Boolean circuit f, ℓ matrices $(\mathbf{B}_1, \ldots, \mathbf{B}_\ell)$, an attribute set $\mathbf{x}$, and ℓ vectors $(\mathbf{c}_1, \ldots, \mathbf{c}_\ell)$, output $\mathbf{c}_f$. Here, $\mathbf{c}_f = \mathbf{s}^\top(\mathbf{B}_f + f(\mathbf{x})\mathbf{G}) + \mathbf{e}_f$, where $\mathbf{B}_f = \mathsf{Eval}_{\mathsf{pk}}(f, (\mathbf{B}_1, \ldots, \mathbf{B}_\ell))$, and $\|\mathbf{e}_f\| \leq \mathcal{B}\sqrt{m} \cdot (m+1)^d$ with almost negligible probability.*
- $\mathsf{Eval}_{\mathsf{sim}}(f, \{(\mathbf{S}_i, x_i^*)\}_{i\in[\ell]}, \mathbf{A}) \to \mathbf{S}_f$*: Given a Boolean circuit f, ℓ matrices $\mathbf{S}_1, \ldots, \mathbf{S}_\ell \in \mathbb{Z}_q^{m\times m}$, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and an attribute set $\mathbf{x}^*$, output $\mathbf{S}_f$. Ensure $\mathbf{AS}_f - f(\mathbf{x}^*)\mathbf{G} = \mathbf{B}_f$, where $\mathbf{B}_f = \mathsf{Eval}_{\mathsf{pk}}(f, (\mathbf{AS}_1 - x_1^*\mathbf{G}, \ldots, \mathbf{AS}_\ell - x_\ell^*\mathbf{G}))$. If $\mathbf{S}_1, \ldots, \mathbf{S}_\ell \in \{-1, 1\}^{m\times m}$, then $\|\mathbf{S}_f\| \leq 20\sqrt{m} \cdot (m+1)^d$ with almost negligible probability.*

2.4. The Complete Subtree Method

The Complete Subtree (CS) method, introduced by Naor et al. [42], is utilized in indirect revocation schemes to alleviate the periodic workload of the KGC. In this approach, the system constructs a complete binary tree BT. For a non-leaf node $\theta \in \mathsf{BT}$, θ_l and θ_r denote the left and right child nodes of θ, and η denotes the leaf node in BT. $\mathsf{Path}(\eta)$ represents the set of nodes on the path from η to the root.

Lemma 8 (KUNodes)**.** *On inputting the revocation list RL_t for time period t, the* KUNodes *algorithm follows these steps: initializes two empty sets X and Y; adds $\mathsf{Path}(\eta)$ to X for each $\eta \in \mathsf{RL}_t$; for each $\theta \in X$, adds θ_l to Y if $\theta_l \notin X$, and adds θ_r to Y if $\theta_r \notin X$; if Y remains empty, adds* root *to Y; finally, outputs Y, which is the smallest subset of nodes representing non-revoked users during time period t.*

In Figure 4a, there are no revoked users and $\mathsf{KUNodes} = \{\text{root}\}$. However, in Figure 4b, User 2 has been revoked and $\mathsf{KUNodes} = \{2, 3\}$. For a non-revoked user, the node set $\mathsf{Path}(\text{User})$ must have an intersection with the node set KUNodes. For example, in Figure 4b, we have $\mathsf{Path}(\text{User } 1) = \{\text{root}, 1, 3\}$ and $\mathsf{KUNodes} \cap \mathsf{Path}(\text{User } 1) = 3$.



(**a**) No user has been revoked (**b**) Only User 2 has been revoked

Figure 4. A graphical description of the KUNodes algorithm.

3. The Notion of Revocable ABE with En-DKER

3.1. Syntax and Correctness

Let $\mathcal{ID}$ be an identity space, $\mathcal{M}$ be a message space, $\mathcal{X}$ be an attribute space, $\mathcal{T}$ be a time period space, and $\mathcal{F}$ be a sequence of sets of functions, namely $\mathcal{F} = \{f : \mathcal{X}^\ell \to \{0,1\}\}$. Our revocable ABE scheme consists of six algorithms (**Setup**, **GenSK**, **NodesUp**, **GenDK**, **Enc**, **Dec**), defined as follows:

- **Setup**$(1^\lambda) \to (\mathsf{PP}, \mathsf{MSK})$: Executed by the KGC, this algorithm takes as input a security parameter λ. It produces public parameters PP and a master secret key MSK.
- **GenSK**$(\mathsf{PP}, \mathsf{MSK}, ID, f) \to \mathsf{SK}_{ID,f}$: Executed by the KGC, this algorithm takes as input the public parameters PP, the master secret key MSK, an identity $ID \in \mathcal{ID}$, and a policy function $f \in \mathcal{F}$. It produces a secret key $\mathsf{SK}_{ID,f}$.
- **NodesUp**$(\mathsf{BT}, t, \mathsf{RL}_t) \to \mathsf{KUNodes}(\mathsf{RL}_t)$: Executed by the KGC, this algorithm takes as input the binary tree BT, a time period $t \in \mathcal{T}$, and the revocation list RL_t for the time period t. It produces and broadcasts a node set $\mathsf{KUNodes}(\mathsf{RL}_t)$.
- **GenDK**$(\mathsf{PP}, \mathsf{SK}_{ID,f}, \mathsf{KUNodes}(\mathsf{RL}_t)) \to \mathsf{DK}_{ID,f,t}$: Executed by the receiver, this algorithm takes as input the public parameters PP, the secret key $\mathsf{SK}_{ID,f}$, and the node set $\mathsf{KUNodes}(\mathsf{RL}_t)$. It produces a decryption key $\mathsf{DK}_{ID,f,t}$.
- **Enc**$(\mathsf{PP}, \mathbf{x}, \mathsf{KUNodes}(\mathsf{RL}_t), \mu) \to \mathsf{CT}_{\mathbf{x},t}$: Executed by the sender, this algorithm takes as input the public parameters PP, an attribute set $\mathbf{x} \in \mathcal{X}^l$, the node set $\mathsf{KUNodes}(\mathsf{RL}_t)$, and a message $\mu \in \mathcal{M}$. It produces a ciphertext $\mathsf{CT}_{\mathbf{x},t}$.
- **Dec**$(\mathsf{CT}_{\mathbf{x},t}, \mathsf{DK}_{ID,f,t}) \to \mu'$: Executed by the receiver, this algorithm takes as input the ciphertext $\mathsf{CT}_{\mathbf{x},t}$ and the decryption key $\mathsf{DK}_{ID,f,t}$. It produces a message $\mu' \in \mathcal{M}$.

Correctness. A revocable ABE scheme is correct if, for all $\lambda \in \mathbb{N}$, $ID \in \mathcal{ID}$, $t \in \mathcal{T}$, $\mu \in \mathcal{M}$, $\mathbf{x} \in \mathcal{X}^\ell$, and $f \in \mathcal{F}$ that satisfy $f(\mathbf{x}) = 0$, it holds that

$$\Pr\left[\mu' = \mu \;\middle|\; \begin{array}{c} (\mathsf{PP}, \mathsf{MSK}) \leftarrow \mathsf{Setup}(1^\lambda) \\ \mathsf{SK}_{ID,f} \leftarrow \mathsf{GenSK}(\mathsf{PP}, \mathsf{MSK}, ID, f) \\ \mathsf{KUNodes}(\mathsf{RL}_t) \leftarrow \mathsf{NodesUp}(\mathsf{BT}, t, \mathsf{RL}_t) \\ \mathsf{DK}_{ID,f,t} \leftarrow \mathsf{GenDK}(\mathsf{PP}, \mathsf{SK}_{ID,f}, \mathsf{KUNodes}(\mathsf{RL}_t)) \\ \mathsf{CT}_{\mathbf{x},t} \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathbf{x}, t, \mathsf{KUNodes}(\mathsf{RL}_t), \mu) \\ \mu' \leftarrow \mathsf{Dec}(\mathsf{CT}_{\mathbf{x},t}, \mathsf{DK}_{ID,f,t}) \end{array}\right] = 1 - \mathsf{negl}(\lambda).$$

3.2. Security Model of Revocable ABE with En-DKER

We first extend the En-DKER property proposed by Wang et al. [24] in RIBE to RABE. Specifically, the En-DKER property of the RABE scheme, in addition to possessing the features of DKER, also satisfies that adversaries are unable to determine whether the attribute set of the ciphertext for the challenge time period satisfies a specific policy using keys from any other time periods or policies, which is analogous to the anonymity property of the IBE scheme.

Then, we provide the formal definition of selective security via a game between an adversary $\mathcal{A}$ and the challenger $\mathcal{C}$. Set a global variable $t_{cu} \in \mathcal{T}$ with an initial value of 1 to facilitate the generation of the decryption key $\mathsf{DK}_{ID,f,t}$ of any time period queried by $\mathcal{A}$. This is particularly useful as the revocation list RL is dynamically updated following the time period t.

Initialize: $\mathcal{C}$ establishes a binary tree BT. $\mathcal{A}$ sets the challenge attribute sets $\mathbf{x}^{(0)}$ and $\mathbf{x}^{(1)}$, the challenge time period t^*, and the challenge node set $\mathsf{KUNodes}(\mathsf{RL}_{t^*})^*$.

Setup Phase: $\mathcal{C}$ executes the Setup algorithm, providing the public parameters PP to $\mathcal{A}$.

Query Phase: $\mathcal{A}$ adaptively makes the following queries to $\mathcal{C}$:

1. $\mathcal{A}$ sets $\mathcal{Q}_0 = \{ID\}$ for user registration queries. $\mathcal{C}$ randomly selects an unassigned leaf node η_{ID} for ID. (At the conclusion of the query, $\mathcal{C}$ acquires $\mathsf{RL}^*_{t^*}$ based on $\mathsf{KUNodes}(\mathsf{RL}_{t^*})^*$ and BT.)
2. $\mathcal{A}$ sets $\mathcal{Q}_1 = \{ID, f\}$ for the secret key queries; $\mathcal{C}$ replies with the corresponding secret key $\mathsf{SK}_{ID,f} \leftarrow \mathsf{GenSK}(\mathsf{PP}, \mathsf{MSK}, ID, f)$. This is subject to the constraint $ID \in \mathcal{Q}_0$; if $f(\mathbf{x}^{(0)}) = 0$ or $f(\mathbf{x}^{(1)}) = 0$, $ID \in \mathsf{RL}^*_{t^*}$.
3. Let $t_{cu} = 1$, and loop through the following steps:
   (a) $\mathcal{A}$ sets $\mathcal{Q}_2 = \{(ID, f, t_{cu})\}$ for the decryption key queries; $\mathcal{C}$ replies with the decryption key $\mathsf{DK}_{ID,f,t_{cu}} \leftarrow \mathsf{GenDK}(\mathsf{PP}, \mathsf{SK}_{ID,f}, \mathsf{KUNodes}(\mathsf{RL}_{t_{cu}}))$. This is subject to the constraint $ID \in \mathcal{Q}_0$; $ID \notin \mathsf{RL}_{t_{cu}}$; if $t_{cu} = t^*$, $f(\mathbf{x}^{(0)}) \neq 0$ and $f(\mathbf{x}^{(1)}) \neq 0$.
   (b) $\mathcal{A}$ sets $\mathcal{Q}_3 = \{(ID, t_{cu})\}$ for revocation queries, $\mathcal{C}$ adds ID to the revocation list RL and updates $\mathsf{RL}_{t_{cu}+1} = \mathsf{RL}$. Then, $\mathcal{C}$ sent $\mathsf{KUNodes}(\mathsf{RL}_{t_{cu}+1})$ to $\mathcal{A}$. This is subject to the constraint $ID \in \mathcal{Q}_0$; $\mathsf{RL}_{t^*} = \mathsf{RL}^*_{t^*}$.
   (c) $t_{cu} = t_{cu} + 1$.

Challenge Phase: $\mathcal{A}$ sets challenge plaintexts $\mu^{(0)}$ and $\mu^{(1)}$. $\mathcal{C}$ randomly chooses a bit $b \leftarrow \{0,1\}$ and replies with the ciphertext $\mathsf{CT}_{\mathbf{x}^{(b)},t^*} \leftarrow \mathsf{Enc}(\mathsf{PP}, \mathbf{x}^{(b)}, t^*, \mathsf{KUNodes}(\mathsf{RL}_{t^*})^*, \mu^{(b)})$.

Guess: $\mathcal{A}$ outputs a guess b' of b and succeeds if $b' = b$. The advantage of $\mathcal{A}$ is defined as

$$\mathsf{Adv}^{\mathsf{SEL\text{-}En\text{-}CPA}}_{\mathsf{RABE},\mathcal{A}}(\lambda) = |\mathsf{Pr}[b = b'] - 1/2|.$$

Definition 3. *A revocable ABE with En-DKER scheme is selectively secure if, for any PPT adversaries* $\mathcal{A}$, $\mathsf{Adv}^{\mathsf{SEL\text{-}En\text{-}CPA}}_{\mathsf{RABE},\mathcal{A}}(\lambda)$ *is at most negligible.*

4. Revocable ABE with En-DKER from Lattices

4.1. Our Construction

In our scheme, we set the message space $\mathcal{M} = \{0,1\}$, the identity space $\mathcal{ID} \subset \mathbb{Z}_q^n \setminus \{\mathbf{0}_n\}$, the attribute space $\mathcal{X} = \{0,1\}$, a sequence of sets of functions $\mathcal{F} = f : \{0,1\}^l \to \{0,1\}$, and the time period space $\mathcal{T} \subset \mathbb{Z}_q^n$. For any $B \in \mathbb{N}$, let $\mathcal{U}_B$ denote the uniform distribution on $\mathbb{Z} \cap [-B, B]$. $\mathsf{H}(\cdot)$ is a full-rank different map defined in Definition 2 and $\mathbf{G}$ is a gadget matrix defined in Lemma 5.

To ensure the decryption algorithm outputs $\perp$ with almost negligible probability when $f(\mathbf{x}) = 1$, we follow the approach of [12,13] and set an encoding function $\mathsf{encode} : \{0,1\} \to \{0,1\}^k$ with $k = \omega(\log \lambda)$. For each $\mu \in \{0,1\}$, we define $\mathsf{encode}(\mu) = (\mu, 0, \ldots, 0) \in \{0,1\}^k$. In addition, our system parameters satisfy the following constraints:

- For sampling: $m > 2n \log q$ and $\sigma > \sqrt{m} \cdot \omega(\sqrt{m})$.

- For correctness: $k = \omega(\log \lambda)$, $O((m+1)^d(m^{5/2}\sigma + m^{3/2}\mathsf{B}_{\mathsf{big}})) < q/4B_{\mathsf{LWE}}$.
- For security: $n = O(\lambda)$, $\chi_{\mathsf{LWE}} = \mathcal{U}_{B_{\mathsf{LWE}}}$, where $B_{\mathsf{LWE}} \geq \omega(\log n) \cdot \sqrt{n}$.
- For smudging: $\chi_{\mathsf{big}} = \mathcal{U}_{B_{\mathsf{big}}}$, where $B_{\mathsf{big}} > (m\sigma^2+1)2^{\lambda+1}$.

Now, we describe our revocable ABE with En-DKER from lattices construction.

Setup$(1^\lambda) \to (\mathsf{PP}, \mathsf{MSK})$: On inputting a security parameter λ, the detailed process is as follows:

1. Run the algorithm $\mathsf{TrapGen}(1^n, 1^m, q)$ to generate $(\mathbf{A}, \mathbf{T}_\mathbf{A})$, where $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.
2. Choose random matrices $\{\mathbf{B}_i\}_{i\in[\ell]}$, $\mathbf{W}$ in $\mathbb{Z}_q^{n\times m}$, and a random matrix $\mathbf{U}$ in $\mathbb{Z}_q^{n\times k}$.
3. Build a binary tree BT with at least N leaf nodes. For each node $\theta \in \mathsf{BT}$, select a random matrix $\mathbf{D}_\theta$ in $\mathbb{Z}_q^{n\times m}$.
4. Output $\mathsf{PP} = \{\mathbf{A}, \{\mathbf{B}_i\}_{i\in[\ell]}, \mathbf{W}, \mathbf{U}, \{\mathbf{D}_\theta\}_{\theta\in\mathsf{BT}}\}$, $\mathsf{MSK} = \{\mathbf{T}_\mathbf{A}, \mathsf{BT}\}$.

GenSK$(\mathsf{PP}, \mathsf{MSK}, ID, f) \to \mathsf{SK}_{ID,f}$: On inputting the public parameters PP, the master secret key MSK, an identity $ID \in \mathcal{ID}$, and a policy function $f \in \mathcal{F}$, the detailed process is as follows:

1. If ID belongs to a newly registered user in the system, then randomly pick an unassigned leaf node η_{ID} from BT and store ID in it.
2. Compute $\mathbf{B}_f = \mathsf{Eval}_{\mathsf{pk}}(f, (\mathbf{B}_1, \ldots, \mathbf{B}_\ell))$.
3. For each $\theta \in \mathsf{Path}(\eta_{ID})$, generate $\mathbf{K}_{ID,f,\theta} \in \mathbb{Z}_q^{3m\times m}$, satisfying $[\mathbf{A}|\mathbf{B}_f|\mathbf{D}_\theta]\mathbf{K}_{ID,f,\theta} = \mathbf{G}$.
   (a) Choose a random matrix $\mathbf{K}'_{ID,f}$ in $\mathcal{D}_{\mathbb{Z},\sigma}^{2m\times m}$ and set $\mathbf{Z}_{ID,f} = [\mathbf{A}|\mathbf{B}_f]\mathbf{K}'_{ID,f} \in \mathbb{Z}_q^{m\times m}$.
   (b) Sample $\mathbf{K}''_{ID,f,\theta} \leftarrow \mathsf{SampleLeft}(\mathbf{A}, \mathbf{D}_\theta, \mathbf{T}_\mathbf{A}, \sigma, \mathbf{G} - \mathbf{Z}_{ID,f})$.
   (c) Divide $\mathbf{K}'_{ID,f}$ and $\mathbf{K}''_{ID,f,\theta}$ into two parts, $\mathbf{K}'_{1,ID,f}$, $\mathbf{K}'_{2,ID,f}$ and $\mathbf{K}''_{1,ID,f,\theta}$, $\mathbf{K}''_{2,ID,f,\theta}$ with m rows per part. Then, generate

$$\mathbf{K}_{ID,f,\theta} = \left[\begin{array}{c|c|c} \left(\mathbf{K}'_{1,ID,f} + \mathbf{K}''_{1,ID,f,\theta}\right)^\top & \left(\mathbf{K}'_{2,ID,f}\right)^\top & \left(\mathbf{K}''_{2,ID,f,\theta}\right)^\top \end{array} \right]^\top.$$

4. Output $\mathsf{SK}_{ID,f} = \{\mathbf{K}_{ID,f,\theta}\}_{\theta\in\mathsf{Path}(\eta_{ID})}$.

NodesUp$(\mathsf{BT}, t, \mathsf{RL}_t) \to \mathsf{KUNodes}(\mathsf{RL}_t)$: On inputting the binary tree BT, a time period $t \in \mathcal{T}$, and the revocation list RL_t for the time period t, the KGC generates and broadcasts a set $\mathsf{KUNodes}(\mathsf{RL}_t)$ for the time period t.

GenDK$(\mathsf{PP}, \mathsf{SK}_{ID,f}, \mathsf{KUNodes}(\mathsf{RL}_t)) \to \mathsf{DK}_{ID,f,t}$: On inputting the public parameters PP, the secret key $\mathsf{SK}_{ID,f}$, and the node set $\mathsf{KUNodes}(\mathsf{RL}_t)$, the detailed process is as follows:

1. Set $\theta^* = \mathsf{Path}(\eta_{ID}) \cap \mathsf{KUNodes}(\mathsf{RL}_t)$. If $\theta^* = \emptyset$, outputs $\perp$. Otherwise, continue the following steps.
2. Compute $\mathbf{W}_t = \mathbf{W} + \mathsf{H}(t)\mathbf{G}$.
3. Generate $\mathbf{DK}_{ID,f,t} \in \mathbb{Z}_q^{4m\times k}$, satisfying $[\mathbf{A}|\mathbf{B}_f|\mathbf{D}_{\theta^*}|\mathbf{W}_t]\mathbf{DK}_{ID,f,t} = \mathbf{U}$.
   (a) Choose a random matrix $\widetilde{\mathbf{K}}_{ID,f,t} \in \chi_{\mathsf{big}}^{4m\times k}$. Set $\mathbf{H}_{ID,f,t} = [\mathbf{A}|\mathbf{B}_f|\mathbf{D}_{\theta^*}|\mathbf{W}_t]\widetilde{\mathbf{K}}_{ID,f,t}$ and send to the server.
   (b) The server samples $\widetilde{\mathbf{K}'}_{ID,f,t} \leftarrow \mathsf{SamplePre}(\mathbf{G}, \mathbf{T}_\mathbf{G}, \sigma, \mathbf{U} - \mathbf{H}_{ID,f,t})$ and sends to the user.
   (c) Compute $\widetilde{\mathbf{K}''}_{ID,f,t} = \mathbf{K}_{f,\theta^*}\widetilde{\mathbf{K}'}_{ID,f,t}$, satisfying $[\mathbf{A}|\mathbf{B}_f|\mathbf{D}_{\theta^*}]\widetilde{\mathbf{K}''}_{ID,f,t} = \mathbf{U} - \mathbf{H}_{ID,f,t}$, where $\widetilde{\mathbf{K}''}_{ID,f,t} \in \mathbb{Z}_q^{3m\times k}$.
   (d) Divide $\widetilde{\mathbf{K}}_{ID,f,t}$ into four parts: $\widetilde{\mathbf{K}}_{1,ID,f,t}$, $\widetilde{\mathbf{K}}_{2,ID,f,t}$, $\widetilde{\mathbf{K}}_{3,ID,f,t}$, $\widetilde{\mathbf{K}}_{4,ID,f,t}$, and $\widetilde{\mathbf{K}''}_{ID,f,t}$ into three parts: $\widetilde{\mathbf{K}''}_{1,ID,f,t}$, $\widetilde{\mathbf{K}''}_{2,ID,f,t}$, $\widetilde{\mathbf{K}''}_{3,ID,f,t}$, with m rows per part. Then, generate

$$\mathbf{DK}_{ID,f,t} = \left[\begin{array}{c|c} \begin{pmatrix} \widetilde{\mathbf{K}}_{1,ID,f,t} + \widetilde{\mathbf{K}''}_{1,ID,f,t} \\ \widetilde{\mathbf{K}}_{2,ID,f,t} + \widetilde{\mathbf{K}''}_{2,ID,f,t} \end{pmatrix}^\top & \begin{pmatrix} \widetilde{\mathbf{K}}_{3,ID,f,t} + \widetilde{\mathbf{K}''}_{3,ID,f,t} \\ \widetilde{\mathbf{K}}_{4,ID,f,t} \end{pmatrix}^\top \end{array} \right]^\top.$$

4. Output $\mathsf{DK}_{ID,f,t} = \mathbf{DK}_{ID,f,t}$.

Enc$(\mathsf{PP}, \mathbf{x}, \mathsf{KUNodes}(\mathsf{RL}_t), \mu) \to \mathsf{CT}_{\mathbf{x},t}$: On inputting the public parameters PP, an attribute set $\mathbf{x} = \{x_1, \ldots, x_\ell\} \in \mathcal{X}^\ell$, the node set $\mathsf{KUNodes}(\mathsf{RL}_t)$, and a message $\mu \in \mathcal{M}$, the detailed process is as follows:

1. Choose a random vector $\mathbf{s}$ in $\mathbb{Z}_q^n$.
2. Choose random matrices $\mathbf{R}_i$, $\mathbf{S}_\theta$, and $\mathbf{V}$ in $\{-1, 1\}^{m \times m}$, where $i \in [\ell], \theta \in \mathsf{KUNodes}(\mathsf{RL}_t)$.
3. Choose noise $\mathbf{e} \leftarrow \chi_{\mathsf{LWE}}^k$ and a noise vector $\mathbf{e}' \leftarrow \chi_{\mathsf{LWE}}^m$.
4. Generate $\mathsf{CT}_{\mathbf{x},t} = \{\mathbf{c}_{in}, \{\mathbf{c}_i\}_{i\in[\ell]}, \{\mathbf{c}_\theta\}_{\theta\in\mathsf{KUNodes}(\mathsf{RL}_t)}, \mathbf{c}_t, \mathbf{c}_{out}\}$, where

$$\begin{aligned} & \mathbf{c}_{out} = \mathbf{s}^\top \mathbf{U} + \left\lfloor \tfrac{q}{2} \right\rfloor \cdot \mathsf{encode}(\mu) + \mathbf{e} \in \mathbb{Z}_q^k, \\ & \mathbf{c}_{in} = \mathbf{s}^\top \mathbf{A} + \mathbf{e}' \in \mathbb{Z}_q^m, \\ & \mathbf{c}_t = \mathbf{s}^\top \mathbf{W}_t + \mathbf{e}' \mathbf{V} \in \mathbb{Z}_q^m, \\ i \in [\ell]: \quad & \mathbf{c}_i = \mathbf{s}^\top (\mathbf{B}_i + x_i \mathbf{G}) + \mathbf{e}' \mathbf{R}_i \in \mathbb{Z}_q^m, \\ \theta \in \mathsf{KUNodes}(\mathsf{RL}_t): \quad & \mathbf{c}_\theta = \mathbf{s}^\top \mathbf{D}_\theta + \mathbf{e}' \mathbf{S}_\theta \in \mathbb{Z}_q^m. \end{aligned}$$

5. Output $\mathsf{CT}_{\mathbf{x},t}$.

Dec$(\mathsf{CT}_{\mathbf{x},t}, \mathsf{DK}_{ID,f,t}) \to \mu'$: On inputting the ciphertext $\mathsf{CT}_{\mathbf{x},t}$ and the decryption key $\mathsf{DK}_{ID,f,t}$, the detailed process is as follows:

1. If $f(\mathbf{x}) = 1$, outputs $\perp$. Otherwise, continue the following steps.
2. Compute $\mathbf{c}_f = \mathsf{Eval}_{\mathsf{ct}}(f, \{(x_i, \mathbf{B}_i, \mathbf{c}_i)\}_{i=1}^\ell) \in \mathbb{Z}_q^m$.
3. Compute $\mathbf{c}' = \mathbf{c}_{out} - [\mathbf{c}_{in} | \mathbf{c}_f | \mathbf{c}_{\theta^*} | \mathbf{c}_t] \mathbf{DK}_{ID,f,t} \in \mathbb{Z}_q^k$.
4. Output μ' by computing $\mathsf{encode}(\mu') = \lfloor \frac{q}{2} \cdot \mathbf{c}' \rceil$.

Correctness. We analyze the correctness of the scheme.

1. When $f(\mathbf{x}) = 1$, the probability of the last $k-1$ coordinates being 0 is $2^{-(k-1)} = 2^{-\omega(\log \lambda)}$, which is negligible in λ. Consequently, the decryption algorithm outputs $\perp$ with all but negligible probability.
2. When $f(\mathbf{x}) = 0$, according to the correctness of the $\mathsf{Eval}_{\mathsf{ct}}$ algorithm, we have $\mathbf{c}_f = \mathbf{s}^\top \mathbf{B}_f + \mathbf{e}' \mathbf{R}_f$. Therefore,

$$\begin{aligned} \mathbf{c}' &= \mathbf{c}_{out} - [\mathbf{c}_{in} | \mathbf{c}_f | \mathbf{c}_{\theta^*} | \mathbf{c}_t] \mathbf{DK}_{ID,f,t} \\ &= \mathbf{s}^\top \mathbf{U} + \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathsf{encode}(\mu) - \mathbf{s}^\top [\mathbf{A} | \mathbf{B}_f | \mathbf{D}_{\theta^*} | \mathbf{W}_t] \mathbf{DK}_{ID,f,t} + \mathbf{noise} \\ &= \left\lfloor \frac{q}{2} \right\rfloor \cdot \mathsf{encode}(\mu) + \mathbf{noise}, \end{aligned}$$

where

$$\begin{aligned} \mathbf{noise} &= \mathbf{e} - \mathbf{e}'^\top [\mathbf{I}_m | \mathbf{R}_f | \mathbf{S}_{\theta^*} | \mathbf{V}] \mathbf{DK}_{ID,f,t} \\ &= \mathbf{e} - \mathbf{e}'^\top [\mathbf{I}_m | \mathbf{R}_f | \mathbf{S}_{\theta^*} | \mathbf{V}] \begin{bmatrix} \widetilde{\mathbf{K}}_{1,ID,f,t} + \mathbf{K}'_{1,ID,f} \widetilde{\mathbf{K}'}_{ID,f,t} + \mathbf{K}''_{1,ID,f,\theta^*} \widetilde{\mathbf{K}'}_{ID,f,t} \\ \widetilde{\mathbf{K}}_{2,ID,f,t} + \mathbf{K}'_{2,ID,f} \widetilde{\mathbf{K}'}_{ID,f,t} \\ \widetilde{\mathbf{K}}_{3,ID,f,t} + \mathbf{K}''_{2,ID,f,\theta^*} \widetilde{\mathbf{K}'}_{ID,f,t} \\ \widetilde{\mathbf{K}}_{4,ID,f,t} \end{bmatrix}. \end{aligned}$$

Correctness now follows since **noise** is small and should not affect $\lfloor \frac{q}{2} \rfloor \cdot \mathsf{encode}(\mu)$. Moreover, the following inequalities hold except with negligible probability:

- From Lemma 2, we have $||\mathbf{S}||$ and $||\mathbf{V}_{\theta^*}|| \leq 20\sqrt{m}$.
- From Lemma 7, we have $||\mathbf{R}_f|| \leq 20\sqrt{m} \cdot (m+1)^d$.
- Because $\mathbf{e} \leftarrow \chi_{\mathsf{LWE}}^k$ and $\mathbf{e}' \leftarrow \chi_{\mathsf{LWE}}^m$, we have $||\mathbf{e}|| \leq B_{\mathsf{LWE}}\sqrt{k}$ and $||\mathbf{e}'|| \leq B_{\mathsf{LWE}}\sqrt{m}$.

$$\begin{aligned}||\mathbf{noise}|| &= ||\mathbf{e} - \mathbf{e'}^{\top}[\mathbf{I}_m|\mathbf{R}|\mathbf{S}_{\theta^*}|\mathbf{V}]\mathbf{DK}_{ID,f,t}|| \\ &\leq ||\mathbf{e}|| + ||\mathbf{e'}^{\top}|| \cdot ||[\mathbf{I}_m|\mathbf{R}|\mathbf{S}_{\theta^*}|\mathbf{V}]\mathbf{DK}_{ID,f,t}|| \\ &\leq O(B_{\mathsf{LWE}}(m+1)^d(m^{5/2}\sigma + m^{3/2}\mathsf{B}_{\mathsf{big}})) < q/4,\end{aligned}$$

and we can obtain μ by computing $\mathsf{encode}(\mu) = \lfloor \frac{q}{2} \cdot \mathbf{c}' \rceil$.

4.2. Security Proof

We show that our RABE construction is secure in the following theorem:

Theorem 1. *Our proposed RABE scheme with En-DKER is* IND-CPA *secure under the assumption that the* LWE *problem is hard.*

Proof. We consider a sequence of games, and the change between each successive game is only by a negligible amount $\mathsf{negl}_x(\lambda)$. Let $\mathcal{P}_{\mathcal{A},x}(\lambda)$ be the function that represents the probability of the adversary $\mathcal{A}$ correctly guessing the challenge bit b in $\mathsf{Game}_x^{(b)}$. The first game is the original IND-CPA secure game for our RABE scheme, so the advantage of $\mathcal{A}$ is $\mathsf{Adv}^{\mathsf{SEL\text{-}En\text{-}CPA}}_{\mathsf{RABE},\mathcal{A}}(\lambda) = |\mathcal{P}_{\mathcal{A},0}(\lambda) - 1/2|$. The final hybrid is one where the ciphertext is independent with the bit b, and the advantage of the adversary $\mathcal{A}$ is zero, so the advantage of $\mathcal{A}$ is $\mathcal{P}_{\mathcal{A},4}(\lambda) = 1/2$. So, for all $\lambda \in \mathbb{N}$, we have $\mathsf{Adv}^{\mathsf{SEL\text{-}En\text{-}CPA}}_{\mathsf{RABE},\mathcal{A}}(\lambda) \leq \sum_{x\in[4]} |\mathcal{P}_{\mathcal{A},x-1}(\lambda) - \mathcal{P}_{\mathcal{A},x}(\lambda)| \leq \sum_{x\in[4]} \mathsf{negl}_x(\lambda)$. □

The Series of Games. Let $\mathcal{A}$ be the adversary in the security definition of the RABE with En-DKER and adhere to the security model defined in Section 3.2. We consider the following series of games.

$\mathbf{Game}_0^{(b)}$: This is the original IND-CPA secure game for our RABE scheme, and $\mathcal{B}$ chooses a random bit $b \leftarrow \{0,1\}$.

$\mathbf{Game}_1^{(b)}$: In this game, we change the generation way of matrices $\{\mathbf{B}_i\}_{i\in[\ell]}$, $\{\mathbf{D}_\theta\}_{\theta\in\mathsf{BT}}$, and $\mathbf{W}$.

1. Choose random matrices $\mathbf{R}_i^*$, $\mathbf{S}_\theta^*$, and $\mathbf{V}^*$ in $\{-1,1\}^{m\times m}$, where $i \in [\ell]$ and $\theta \in \mathsf{BT}$.
2. For each $i \in [\ell]$, $\theta \in \mathsf{BT}$, we set $\mathbf{B}_i = \mathbf{A}\mathbf{R}_i^* - x_i^{(b)}\mathbf{G}$, $\mathbf{W} = \mathbf{A}\mathbf{V}^* - \mathsf{H}(t^*)\mathbf{G}$,

$$\mathbf{D}_\theta = \begin{cases} \mathbf{A}\mathbf{S}_\theta^*, & \text{if } \theta \in \mathsf{KUNodes}(\mathsf{RL}_{t^*})^* \\ \mathbf{A}\mathbf{S}_\theta^* + \mathbf{G}, & \text{otherwise} \end{cases}.$$

We show that $\mathsf{Game}_0^{(b)}$ is statistically indistinguishable from $\mathsf{Game}_1^{(b)}$. By Lemma 2, $(\mathbf{A}, \mathbf{A}\mathbf{R}_i^*, \mathbf{A}\mathbf{S}_\theta^*, \mathbf{A}\mathbf{V}^*)$ is statistically close to $(\mathbf{A}, \mathbf{B}_i, \mathbf{D}_\theta, \mathbf{W})$, where $\mathbf{B}_i, \mathbf{D}_\theta, \mathbf{W}$ are the independently random matrices in $\mathbb{Z}_q^{n\times m}$, $i \in [\ell]$ and $\theta \in \mathsf{BT}$. Moreover, the difference between $(\mathbf{A}\mathbf{R}_i^*, \mathbf{A}\mathbf{S}_\theta^*, \mathbf{A}\mathbf{V}^*)$ and $(\mathbf{A}\mathbf{R}_i^* - x_i^{(b)}\mathbf{G}, \mathbf{A}\mathbf{S}_\theta^* + \mathbf{G}, \mathbf{A}\mathbf{V}^* - \mathsf{H}(t^*)\mathbf{G})$ is merely syntactic. So, there exists a negligible function $\mathsf{negl}_1(\cdot)$ satisfying $|\mathcal{P}_{\mathcal{A},0}(\lambda) - \mathcal{P}_{\mathcal{A},1}(\lambda)| \leq \mathsf{negl}_1(\lambda)$ for any adversary $\mathcal{A}$.

$\mathbf{Game}_2^{(b)}$: In this game, we change the generation way of the secret key $\mathsf{SK}_{ID,f}$ for secret key query of (ID, f), mainly divided into the following three cases:

- **Case 1**: $f(\mathbf{x}^{(b)}) = 0$. In this case, the user ID must have been revoked before the challenge time period t^*, i.e. $\mathsf{Path}(\eta_{ID}) \cap \mathsf{KUNodes}(\mathsf{RL}_{t^*})^* = \emptyset$, as per the secret key query restriction in the security model. So, for each $\theta \in \mathsf{Path}(\eta_{ID})$, $\mathbf{D}_\theta = \mathbf{A}\mathbf{S}_\theta^* + \mathbf{G}$.
  1. Perform operation 3.(a) in algorithm GenSK.
  2. Sample $\mathbf{K}''_{ID,f,\theta} \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{S}_\theta^*, \mathbf{G}, \mathbf{T}_\mathbf{G}, \sigma, \mathbf{G} - \mathbf{Z}_{ID,f})$.
- **Case 2**: $f(\mathbf{x}^{(b)}) \neq 0$ and $ID \notin \mathsf{RL}_{t^*}$. In this case, $\mathbf{D}_{\theta^*} = \mathbf{A}\mathbf{S}_{\theta^*}^*$, where $\theta^* = \mathsf{Path}(\eta_{ID}) \cap \mathsf{KUNodes}(\mathsf{RL}_{t^*})$. So, the challenger cannot use $\mathbf{G}$ and algorithm SampleRight to sample

$\mathbf{K}''_{ID,f,\theta^*}$. Furthermore, $\mathbf{Z}_{ID,f}$ can only be randomly selected once, so we need to use the SampleRight algorithm to sample $\mathbf{K}'_{ID,f}$.

1. Sample $\mathbf{K}''_{ID,f,\theta^*} \leftarrow \mathcal{D}^{2m\times m}_{\mathbb{Z},\sigma}$ and set $\mathbf{Z}_{ID,f} = [\mathbf{A}|\mathbf{D}_{\theta^*}]\mathbf{K}''_{ID,f,\theta^*}$.
2. For other nodes $\theta \in \mathsf{Path}(\eta_{ID})$ and $\theta \neq \theta^*$, the challenger computes $\mathbf{K}''_{ID,f,\theta} \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{S}^*_\theta, \mathbf{G}, \mathbf{T}_\mathbf{G}, \sigma, \mathbf{Z}_{ID,f})$.
3. Compute $\mathbf{R}^*_f = \mathsf{Eval}_{\mathsf{sim}}\left(f, \{(x^{(b)}_i, \mathbf{R}^*_i)\}^{\ell}_{i=1}, \mathbf{A}\right)$ and obtain a low-norm matrix $\mathbf{R}^*_f \in \mathbb{Z}^{m\times m}_q$ such that $\mathbf{A}\mathbf{R}^*_f - f(\mathbf{x}^{(b)})\mathbf{G} = \mathbf{B}_f$. By the definition, we have $\mathbf{R}^*_f \leq 20\sqrt{m}\cdot(m+1)^d$. Moreover, $\sigma = \sqrt{5}\cdot(1+||\mathbf{R}^*_f||)\cdot\omega(\sqrt{\log m})$ as needed for algorithm SampleRight.
4. Sample $\mathbf{K}'_{ID,f} \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{R}^*_f, -f(\mathbf{x}^{(b)})\mathbf{G}, \mathbf{T}_\mathbf{G}, \sigma, \mathbf{G} - \mathbf{Z}_{ID,f})$.

- **Case 3**: $f(\mathbf{x}^{(b)}) \neq 0$ and $ID \in \mathsf{RL}_{t^*}$. In this case, $\mathsf{Path}(\eta_{ID}) \cap \mathsf{KUNodes}(\mathsf{RL}_{t^*}) = \emptyset$, and $\mathbf{D}_\theta = \mathbf{A}\mathbf{S}^*_\theta + \mathbf{G}$, for each $\theta \in \mathsf{Path}(\eta_{ID})$.
  1. Perform the operation 3.(a) in algorithm **GenSK**.
  2. Sample $\mathbf{K}''_{ID,f,\theta} \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{S}^*_\theta, \mathbf{G}, \mathbf{T}_\mathbf{G}, \sigma, \mathbf{G} - \mathbf{Z}_{ID,f})$.

We show that $\mathsf{Game}^{(b)}_1$ is statistically indistinguishable from $\mathsf{Game}^{(b)}_2$. By Lemma 6 , $\mathbf{K}'_{ID,f}$ and $\mathbf{K}''_{ID,f,\theta}$ sampled via algorithm SampleLeft and algorithm SampleRight are statistically close to randomly chosen in $\mathcal{D}^{2m\times m}_{\mathbb{Z},\sigma}$. Moreover, $\mathbf{Z}_{ID,f} = [\mathbf{A}|\mathbf{B}_f]\mathbf{K}'_{ID,f}$ and $\mathbf{Z}_{ID,f} = [\mathbf{A}|\mathbf{D}_{\theta^*}]\mathbf{K}''_{ID,f,\theta^*}$ are statistically indistinguishable from a random matrix selected in $\mathbb{Z}^{n\times 2m}_q$. So, there exists a negligible function $\mathsf{negl}_2(\cdot)$ satisfying $|\mathcal{P}_{\mathcal{A},1}(\lambda) - \mathcal{P}_{\mathcal{A},2}(\lambda)| \leq \mathsf{negl}_2(\lambda)$ for any adversary $\mathcal{A}$.

Game$^{(b)}_3$: In this game, we change the generation way of the decryption key $\mathsf{DK}_{ID,f,t}$ for decryption key query of (ID, f, t), when $f(\mathbf{x}^{(b)}) = 0$, $ID \notin \mathsf{RL}_{t^*}$ and $t \neq t^*$.

1. Sample $\widehat{\mathbf{K}}_t \leftarrow \mathsf{SampleRight}(\mathbf{A}, \mathbf{V}^*, (\mathsf{H}(t) - \mathsf{H}(t^*))\mathbf{G}, \mathbf{T}_\mathbf{G}, \sigma, \mathbf{G})$.
2. Perform the operation 2.(a) and 2.(b) in algorithm GenDK to generate $\widetilde{\mathbf{K}}_{ID,f,t}$ and $\widetilde{\mathbf{K}'}_{ID,f,t}$.
3. Compute $\widehat{\mathbf{K}}''_{ID,f,t} = \widehat{\mathbf{K}}_t\widetilde{\mathbf{K}'}_{ID,f,t}$, satisfying $[\mathbf{A}|\mathbf{W}_t]\widehat{\mathbf{K}}''_{ID,f,t} = \mathbf{U} - \mathbf{H}_{ID,f,t}$.
4. Divide $\widehat{\mathbf{K}}''_{ID,f,t}$ into two parts: $\widehat{\mathbf{K}}''_{1,ID,f,t}$ and $\widehat{\mathbf{K}}''_{2,ID,f,t}$, with m rows per part. Set

$$\widehat{\mathbf{DK}}_{ID,f,t} = \left[\begin{array}{c|c} \begin{pmatrix} \widetilde{\mathbf{K}}_{1,ID,f,t} + \widehat{\mathbf{K}}''_{1,ID,f,t} \\ \widetilde{\mathbf{K}}_{2,ID,f,t} \end{pmatrix}^\top & \begin{pmatrix} \widetilde{\mathbf{K}}_{3,ID,f,t} \\ \widetilde{\mathbf{K}}_{4,ID,f,t} + \widehat{\mathbf{K}}''_{2,ID,f,t} \end{pmatrix}^\top \end{array}\right]^\top \in \mathbb{Z}^{4m\times k}_q.$$

We show that $\mathsf{Game}^{(b)}_2$ is statistically indistinguishable from $\mathsf{Game}^{(b)}_3$. Recall in $\mathsf{Game}^{(b)}_2$

$$\mathbf{DK}_{ID,f,t} = \left[\begin{array}{c|c} \begin{pmatrix} \widetilde{\mathbf{K}}_{1,ID,f,t} + \widetilde{\mathbf{K}''}_{1,ID,f,t} \\ \widetilde{\mathbf{K}}_{2,ID,f,t} + \widetilde{\mathbf{K}''}_{2,ID,f,t} \end{pmatrix}^\top & \begin{pmatrix} \widetilde{\mathbf{K}}_{3,ID,f,t} + \widetilde{\mathbf{K}''}_{3,ID,f,t} \\ \widetilde{\mathbf{K}}_{4,ID,f,t} \end{pmatrix}^\top \end{array}\right]^\top.$$

By the triangle inequality for statistical distance and Lemma 1, when $B_{\mathsf{big}} > (m\sigma^2 + 1)2^{\lambda+1}$, there exists a negligible function $\mathsf{negl}_{smudge}(\cdot)$ for all $\lambda \in \mathbb{N}$,

$$\begin{aligned} &\mathsf{SD}(\widetilde{\mathbf{K}}_{1,ID,f,t} + \widetilde{\mathbf{K}''}_{1,ID,f,t}, \widetilde{\mathbf{K}}_{1,ID,f,t} + \widehat{\mathbf{K}}''_{1,ID,f,t}) \\ &\leq \mathsf{SD}(\widetilde{\mathbf{K}}_{1,ID,f,t} + \widetilde{\mathbf{K}''}_{1,ID,f,t}, \widetilde{\mathbf{K}}_{1,ID,f,t}) + \mathsf{SD}(\widetilde{\mathbf{K}}_{1,ID,f,t}, \widetilde{\mathbf{K}}_{1,ID,f,t} + \widehat{\mathbf{K}}''_{1,ID,f,t}) \\ &\leq mk\cdot\mathsf{negl}_{smudge}(\cdot) + mk\cdot\mathsf{negl}_{smudge}(\cdot) \\ &= 2mk\cdot\mathsf{negl}_{smudge}(\cdot). \end{aligned}$$

In the remaining $3m$ rows, each m row's statistical distance is equal to $mk \cdot \mathsf{negl}_{smudge}(\cdot)$. So, in the adversary's view,

$$|\mathcal{P}_{\mathcal{A},2}(\lambda) - \mathcal{P}_{\mathcal{A},3}(\lambda)| \leq 5mk \cdot \mathsf{negl}_{smudge}(\cdot).$$

$\mathbf{Game}_4^{(b)}$: In this game, we change the generation way of the matrix $\mathbf{A}$ and the ciphertexts.

1. Choose a random matrix $\mathbf{A}$ in $\mathbb{Z}_q^{n\times m}$.
2. Choose $\mathbf{c}_{out}^* \leftarrow \mathbb{Z}_q^k$ and $\mathbf{c}_{in}^*, \mathbf{c}_i^*, \mathbf{c}_\theta^*, \mathbf{c}_{t^*}^* \leftarrow \mathbb{Z}_q^m$, where $\theta \in \mathsf{KUNodes}(\mathsf{RL}_{t^*})^*$ and $i \in [\ell]$.

It remains to be shown that $\mathsf{Game}_3^{(b)}$ and $\mathsf{Game}_4^{(b)}$ are computationally indistinguishable under the hardness of the LWE problem. If there exists a non-negligible function $\delta(\cdot)$ such that $|\mathcal{P}_{\mathcal{A},3}(\lambda) - \mathcal{P}_{\mathcal{A},4}(\lambda)| \geq \delta(\cdot)$, we can also construct an LWE algorithm $\mathcal{B}$ under $\mathcal{A}$ such that $\mathsf{Adv}_{\mathcal{B}}^{\mathsf{LWE}}(\lambda) \geq \delta(\lambda)$ for all $\lambda \in \mathbb{N}$.

LWE Instance: $\mathcal{B}$ begins by obtaining an $\mathsf{LWE}_{n,q,\sigma}$ challenger of two random matrices $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, $\mathbf{U} \in \mathbb{Z}_q^{n\times k}$ and two vectors $\mathbf{c} \in \mathbb{Z}_q^k$, $\mathbf{c}' \in \mathbb{Z}_q^m$, where $\mathbf{c} \in \mathbb{Z}_q^k$ and $\mathbf{c}' \in \mathbb{Z}_q^m$ are either random or $\mathbf{c}' = \mathbf{s}^\top \mathbf{A} + \mathbf{e}'$ and $\mathbf{c} = \mathbf{s}^\top \mathbf{U} + \mathbf{e}$ for some random vector $\mathbf{s} \in \mathbb{Z}_q^n$ and $\mathbf{e} \leftarrow \chi_{\mathsf{LWE}}^k$, $\mathbf{e}' \leftarrow \chi_{\mathsf{LWE}}^m$.

Public Parameters: $\mathcal{A}$ sets the challenge attributes $\mathbf{x}^{(0)}$ and $\mathbf{x}^{(1)}$, time period t^*, and node set $\mathsf{KUNodes}(\mathsf{RL}_{t^*})^*$. Then, $\mathcal{B}$ sets the public parameters PP as in $\mathsf{Game}_3^{(b)}$: Uniformly random matrices $\mathbf{R}_i^*$, $\mathbf{S}_\theta^*$, and $\mathbf{V}^*$ in $\{-1,1\}^{m\times m}$, $\mathbf{B}_i = \mathbf{A}\mathbf{R}_i^* + x_i^{(b)}\mathbf{G}$, $\mathbf{W} = \mathbf{A}\mathbf{V}^* - \mathsf{H}(t^*)\mathbf{G}$,

$$\mathbf{D}_\theta = \begin{cases} \mathbf{A}\mathbf{S}_\theta^*, & \text{if } \theta \in \mathsf{KUNodes}(\mathsf{RL}_{t^*})^* \\ \mathbf{A}\mathbf{S}_\theta^* + \mathbf{G}, & \text{otherwise} \end{cases},$$

where $i \in [\ell]$ and $\theta \in \mathsf{BT}$.

Query Phase: $\mathcal{B}$ answers $\mathcal{A}$'s user registration, secret key, decryption key, and revocation queries as in $\mathsf{Game}_3^{(b)}$.

Challenge Phase: $\mathcal{A}$ sets two messages $\mu^{(0)}$, $\mu^{(1)} \in \{0,1\}$. $\mathcal{B}$ computes $\mathbf{c}_{in}^* = \mathbf{c}'$, $\mathbf{c}_i^* = \mathbf{c}'\mathbf{R}_i^*$, $\mathbf{c}_\theta^* = \mathbf{c}'\mathbf{S}_\theta^*$, and $\mathbf{c}_{t^*}^* = \mathbf{c}'\mathbf{V}^*$, $\mathbf{c}_{out}^* = \mathbf{c} + \mathsf{encode}(\mu^{(b)}) \cdot \lfloor \frac{q}{2} \rfloor$, where $i \in [\ell]$ and $\theta \in \mathsf{KUNodes}(\mathsf{RL}_{t^*})^*$.

When the LWE challenge is pseudorandom,

$$\begin{aligned}
&\mathbf{c}_{out}^* = \mathbf{c} + \mathsf{encode}(\mu^{(b)}) \cdot \lfloor \tfrac{q}{2} \rfloor = \mathbf{s}^\top \mathbf{U} + \mathsf{encode}(\mu^{(b)}) \cdot \lfloor \tfrac{q}{2} \rfloor + \mathbf{e}, \\
&\mathbf{c}_{in}^* = \mathbf{c} = \mathbf{s}^\top \mathbf{A} + \mathbf{e}', \\
&\mathbf{c}_{t^*}^* = \mathbf{s}^\top (\mathbf{A}\mathbf{V}^* - \mathsf{H}(t^*)\mathbf{G} + \mathsf{H}(t^*)\mathbf{G}) + \mathbf{e}'\mathbf{V}^* = \mathbf{s}^\top \mathbf{W}_t + \mathbf{e}'\mathbf{V}^*, \\
i \in [\ell]: \quad &\mathbf{c}_i^* = \mathbf{s}^\top (\mathbf{A}\mathbf{R}_i^* - x_i^{(b)}\mathbf{G} + x_i^{(b)}\mathbf{G}) + \mathbf{e}'\mathbf{R}_i^* = \mathbf{s}^\top (\mathbf{B}_i + x_i^{(b)}\mathbf{G}) + \mathbf{e}'\mathbf{R}_i^*, \\
\theta \in \mathsf{KUNodes}(\mathsf{RL}_{t^*})^*: \quad &\mathbf{c}_\theta^* = (\mathbf{s}^\top \mathbf{A} + \mathbf{e}')\mathbf{S}_\theta^* = \mathbf{s}^\top \mathbf{D}_\theta + \mathbf{e}'\mathbf{S}_\theta^*,
\end{aligned}$$

the ciphertexts are distributed exactly as in $\mathsf{Game}_3^{(b)}$. When the LWE challenge is random, the ciphertexts are distributed exactly as in $\mathsf{Game}_4^{(b)}$.

Guess: $\mathcal{A}$ outputs a guess b' of b. Then, $\mathcal{B}$ outputs $\mathcal{A}$'s guess as the answer to the $\mathsf{LWE}_{n,q,\sigma}$ challenge it is trying to solve.

Note that, when the LWE challenge is pseudorandom, $\mathcal{A}$'s view is as in $\mathsf{Game}_3^{(b)}$; when the LWE challenge is random, $\mathcal{A}$'s view is as in $\mathsf{Game}_4^{(b)}$. So, if the LWE assumption holds, there exists a negligible function $\mathsf{negl}_4(\cdot)$, satisfying $|\mathcal{P}_{\mathcal{A},3}(\lambda) - \mathcal{P}_{\mathcal{A},4}(\lambda)| \leq \mathsf{negl}_4(\lambda)$.

5. Application in Practice

In this section, we provide an application example of our RABE scheme with En-DKER in the electronic healthcare scenario.

As shown in Figure 5, the system primarily consists of three entities: KGC, patient, and doctor. The KGC is responsible for generating secret keys for system users and periodically publishing a set of nodes representing the non-revoked users. As the data owner, the patient encrypts their electronic medical record (EMR) and shares with attending physicians. Additionally, doctors can periodically generate their decryption keys, and only doctors who satisfy the access policy and have not been revoked can decrypt and access the EMR information of the patient.

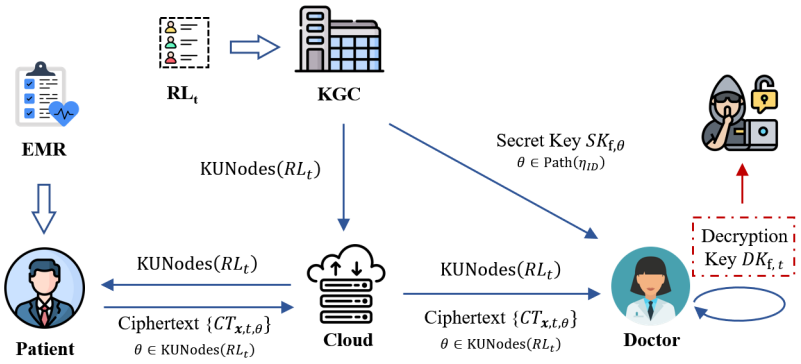


Figure 5. Electronic medical application.

Our scheme also satisfies the En-DKER property, ensuring that the leakage of decryption keys from any time period should not compromise the confidentiality of ciphertexts from other time periods. Additionally, adversaries cannot determine whether the attribute set of ciphertext for the challenge time period satisfies a specific policy using keys from any other time periods or policies.

6. Conclusions

To enhance the practicality of the lattice-based RABE scheme, we extend the En-DKER property from RIBE to RABE. This extension ensures that the leakage of any time period decryption keys should not compromise the confidentiality of ciphertexts from other time periods. Additionally, adversaries are unable to determine whether the attribute set of the ciphertext for the challenge time period satisfies a specific policy using keys from any other time periods or policies. Building upon the BGG+14 scheme, we then construct the first RABE with En-DKER from lattices. Our scheme retains advantages such as near-zero periodic workload for the KGC, and the encryptor is relieved from managing a revocation list. Finally, we validate the correctness and prove the security of our scheme under the LWE assumption.

However, this scheme is based on the LWE assumption, which requires complex inverse algorithms and matrix multiplication for trapdoor generation, making it unsuitable for practical applications. In the future, we plan to extend the approach to the ring LWE assumption, aiming to develop a more advantageous scheme that addresses the computational complexity and storage requirements.

Author Contributions: Methodology, Q.W.; validation, J.L. and Z.W.; formal analysis, Y.Z.; writing—original draft preparation, Q.W.; writing—review and editing, Z.W. and Y.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are contained within the article.

Acknowledgments: The authors are thankful to the anonymous referees for their helpful comments.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Sahai, A.; Waters, B. Fuzzy identity-based encryption. In Proceedings of the Advances in Cryptology–EUROCRYPT 2005: 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Aarhus, Denmark, 22–26 May 2005; Proceedings 24; Springer: Berlin/Heidelberg, Germany, 2005; pp. 457–473.
2. Bethencourt, J.; Sahai, A.; Waters, B. Ciphertext-policy attribute-based encryption. In Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP'07), Oakland, CA, USA, 20–23 May 2007; IEEE: Piscataway Township, NJ, USA, 2007; pp. 321–334.
3. Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization. In Proceedings of the International Workshop on Public Key Cryptography, Taormina, Italy, 6–9 March 2011; Springer: Berlin/Heidelberg, Germany, 2011; pp. 53–70.
4. Attrapadung, N.; Libert, B.; De Panafieu, E. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In Proceedings of the Public Key Cryptography–PKC 2011: 14th International Conference on Practice and Theory in Public Key Cryptography, Taormina, Italy, 6–9 March 2011; Proceedings 14; Springer: Berlin/Heidelberg, Germany, 2011; pp. 90–108.
5. Hohenberger, S.; Waters, B. Attribute-based encryption with fast decryption. In Proceedings of the Public-Key Cryptography–PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, 26 February–1 March 2013; Proceedings 16; Springer: Berlin/Heidelberg, Germany, 2013; pp. 162–179.
6. Goyal, V.; Pandey, O.; Sahai, A.; Waters, B. Attribute-based encryption for fine-grained access control of encrypted data. In Proceedings of the 13th ACM Conference on Computer and Communications Security, Taormina, Italy, 6–9 March 2006; pp. 89–98.
7. Lewko, A.; Waters, B. New proof methods for attribute-based encryption: Achieving full security through selective techniques. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 180–198.
8. Itkis, G.; Shen, E.; Varia, M.; Wilson, D.; Yerukhimovich, A. Bounded-collusion attribute-based encryption from minimal assumptions. In Proceedings of the Public-Key Cryptography–PKC 2017: 20th IACR International Conference on Practice and Theory in Public-Key Cryptography, Amsterdam, The Netherlands, 28–31 March 2017; Proceedings, Part II 20; Springer: Berlin/Heidelberg, Germany, 2017; pp. 67–87.
9. Boneh, D.; Franklin, M. Identity-based encryption from the Weil pairing. *SIAM J. Comput.* **2003**, *32*, 586–615. [CrossRef]
10. Boldyreva, A.; Goyal, V.; Kumar, V. Identity-based encryption with efficient revocation. In Proceedings of the 15th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 27–31 October 2008; pp. 417–426.
11. Chen, J.; Lim, H.W.; Ling, S.; Wang, H.; Nguyen, K. Revocable identity-based encryption from lattices. In Proceedings of the Information Security and Privacy: 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, 9–11 July 2012; Proceedings 17; Springer: Berlin/Heidelberg, Germany, 2012; pp. 390–403.
12. Luo, F.; Al-Kuwari, S.; Wang, H.; Wang, F.; Chen, K. Revocable attribute-based encryption from standard lattices. *Comput. Stand. Interfaces* **2023**, *84*, 103698. [CrossRef]
13. Ling, S.; Nguyen, K.; Wang, H.; Zhang, J. Revocable predicate encryption from lattices. In Proceedings of the Provable Security: 11th International Conference, ProvSec 2017, Xi'an, China, 23–25 October 2017; Proceedings 11; Springer: Berlin/Heidelberg, Germany, 2017; pp. 305–326.
14. Meng, F. Directly Revocable Ciphertext-Policy Attribute-Based Encryption from Lattices. Cryptology ePrint Archive, Paper 2020/940, 2020. Available online: https://eprint.iacr.org/2020/940 (accessed on 31 July 2020).
15. Attrapadung, N.; Imai, H. Attribute-based encryption supporting direct/indirect revocation modes. In Proceedings of the Cryptography and Coding: 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, 15–17 December 2009; Proceedings 12; Springer: Berlin/Heidelberg, Germany, 2009; pp. 278–300.
16. Seo, J.H.; Emura, K. Revocable identity-based encryption revisited: Security model and construction. In Proceedings of the Public-Key Cryptography–PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, 26 February–1 March 2013; Proceedings 16; Springer: Berlin/Heidelberg, Germany, 2013; pp. 216–234.
17. Qin, B.; Zhao, Q.; Zheng, D.; Cui, H. (Dual) server-aided revocable attribute-based encryption with decryption key exposure resistance. *Inf. Sci.* **2019**, *490*, 74–92. [CrossRef]
18. Cheng, L.; Meng, F. Server-aided revocable attribute-based encryption revised: Multi-user setting and fully secure. In Proceedings of the Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, 4–8 October 2021; Proceedings, Part II 26; Springer: Berlin/Heidelberg, Germany, 2021; pp. 192–212.
19. Xu, S.; Yang, G.; Mu, Y. Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. *Inf. Sci.* **2019**, *479*, 116–134. [CrossRef]
20. Katsumata, S.; Matsuda, T.; Takayasu, A. Lattice-Based Revocable (Hierarchical) IBE with Decryption Key Exposure Resistance. In Proceedings of the Public-Key Cryptography–PKC 2019: 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, 14–17 April 2019; Proceedings, Part II 22; Springer: Berlin/Heidelberg, Germany, 2019; pp. 441–471.
21. Agrawal, S.; Boneh, D.; Boyen, X. Efficient lattice (h) ibe in the standard model. In Proceedings of the Eurocrypt, Nice, Frence, 30 May–3 June 2010; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6110, pp. 553–572.
22. Cash, D.; Hofheinz, D.; Kiltz, E.; Peikert, C. Bonsai trees, or how to delegate a lattice basis. *J. Cryptol.* **2012**, *25*, 601–639. [CrossRef]

23. Qin, B.; Deng, R.H.; Li, Y.; Liu, S. Server-aided revocable identity-based encryption. In Proceedings of the Computer Security–ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, 21–25 September 2015; Proceedings, Part I 20; Springer: Berlin/Heidelberg, Germany, 2015; pp. 286–304.
24. Wang, Q.; Huang, H.; Li, J.; Yuan, Q. Revocable IBE with En-DKER from Lattices: A Novel Approach for Lattice Basis Delegation. Cryptology ePrint Archive, Paper 2023/1028, 2023. Available online: https://eprint.iacr.org/2023/1028 (accessed on 3 July 2023).
25. Takayasu, A.; Watanabe, Y. Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In Proceedings of the Information Security and Privacy: 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, 3–5 July 2017; Proceedings, Part I 22; Springer: Berlin/Heidelberg, Germany, 2017; pp. 184–204.
26. Takayasu, A.; Watanabe, Y. Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more. *Theor. Comput. Sci.* **2021**, *849*, 64–98. [CrossRef]
27. Boyen, X.; Waters, B. Anonymous hierarchical identity-based encryption (without random oracles). In Proceedings of the Advances in Cryptology-CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2006; Proceedings 26; Springer: Berlin/Heidelberg, Germany, 2006; pp. 290–307.
28. Wang, S.; Zhang, X.; Zhang, Y. Efficient revocable and grantable attribute-based encryption from lattices with fine-grained access control. *IET Inf. Secur.* **2018**, *12*, 141–149. [CrossRef]
29. Yang, K.; Wu, G.; Dong, C.; Fu, X.; Li, F.; Wu, T. Attribute Based Encryption with Efficient Revocation from Lattices. *Int. J. Netw. Secur.* **2020**, *22*, 161–170.
30. Yang, Y.; Sun, J.; Liu, Z.; Qiao, Y. Practical revocable and multi-authority CP-ABE scheme from RLWE for Cloud Computing. *J. Inf. Secur. Appl.* **2022**, *65*, 103108. [CrossRef]
31. Dong, X.; Hu, Y.; Wang, B.; Liu, M.; Gao, W. Lattice-based revocable attribute-based encryption with decryption key exposure resistance. *IET Inf. Secur.* **2021**, *15*, 428–441. [CrossRef]
32. Huang, B.; Gao, J.; Li, X. Efficient lattice-based revocable attribute-based encryption against decryption key exposure for cloud file sharing. *J. Cloud Comput.* **2023**, *12*, 1–15. [CrossRef] [PubMed]
33. Boneh, D.; Gentry, C.; Gorbunov, S.; Halevi, S.; Nikolaenko, V.; Segev, G.; Vaikuntanathan, V.; Vinayagamurthy, D. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In Proceedings of the Advances in Cryptology–EUROCRYPT 2014: 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014; Proceedings 33; Springer: Berlin/Heidelberg, Germany, 2014; pp. 533–556.
34. Asharov, G.; Jain, A.; López-Alt, A.; Tromer, E.; Vaikuntanathan, V.; Wichs, D. Multiparty computation with low communication, computation and interaction via threshold FHE. In Proceedings of the Advances in Cryptology–EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012; Proceedings 31; Springer: Berlin/Heidelberg, Germany, 2012; pp. 483–501.
35. 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, Victoria, BC, Canada, 17–20 May 2008; pp. 197–206.
36. Micciancio, D.; Peikert, C. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In Proceedings of the Eurocrypt, Cambridge, UK, 15–19 April 2012; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 700–718.
37. Ajtai, M. Generating hard instances of the short basis problem. In Proceedings of the Automata, Languages and Programming: 26th International Colloquium, ICALP'99 Prague, Czech Republic, 11–15 July 1999; Proceedings 26; Springer: Berlin/Heidelberg, Germany, 1999; pp. 1–9.
38. Alwen, J.; Peikert, C. Generating shorter bases for hard random lattices. *Theory Comput. Syst.* **2011**, *48*, 535–553. [CrossRef]
39. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM (JACM)* **2009**, *56*, 1–40. [CrossRef]
40. Peikert, C. Public-key cryptosystems from the worst-case shortest vector problem. In Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing, Bethesda, MD, USA, 31 May–2 June 2009; pp. 333–342.
41. Gorbunov, S.; Vaikuntanathan, V.; Wee, H. Predicate encryption for circuits from LWE. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 503–523.
42. Naor, D.; Naor, M.; Lotspiech, J. Revocation and tracing schemes for stateless receivers. In Proceedings of the Advances in Cryptology—CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2001; Proceedings 21; Springer: Berlin/Heidelberg, Germany, 2001; pp. 41–62.