scientific reports

Check for updates

OPEN

An efficient lattice-based integrated revocable identity-based encryption

Haodong Huang[1], Juyan Li[1], Shujun Bi[1]✉ & Qi Yuan[2]

Revocable identity-based encryption (RIBE) enables data encryption without certificates and allows for the revocation of users, thereby offering a more streamlined and secure approach to dynamic member management. However, the existing revocation models lack strong scalability, rendering the RIBE scheme unsuitable for scenarios where the key generation center (KGC) experiences high workloads and users face heavy storage burdens. Therefore, this paper introduces an integrated revocation model that maintains both the workload for the KGC and the size of the secret keys at a constant level, while also relieving the encryptor of the burden of handling revocation information. By combining online and offline encryption, we construct an OO-IRIBE-EnDKER scheme from lattices, which possesses properties such as anonymity, decryption key exposure resistance (DKER), resistance to quantum computing attacks, and selective security. Finally, the effectiveness of the OO-IRIBE-EnDKER scheme is demonstrated through experimental results.

Keywords Lattice, RIBE, Anonymity, DKER

The digital supply chain represents an innovative approach that leverages digital tech nology, integrating big data and cloud computing to increase efficiency and foster sustainable growth for businesses[1]. Big data technology enables the collection, storage, pro cessing, and analysis of extensive supply chain data, improving understanding of market fluctuations, customer demands, product quality, and risks, resulting in more precise and quicker decision-making[2]. Moreover, cloud computing facilitates cross-departmental, cross-regional, and cross-platform data sharing and collaboration, reducing operational costs and enhancing efficiency. However, supply chain's digital transition implies that a sizable volume of sensitive data from businesses is uploaded to the cloud server, such as customer and supplier identity information, financial transactions, procurement details, production records, and more. Ensuring the security and confidentiality of this sensitive data has emerged as a paramount priority for businesses, commonly achieved through encryption.

Identity-based encryption (IBE)[3] not only inherits the advantages of public key cryptography, but also avoids the heavy management of PKI certificates. However, in the absence of a certificate revocation mechanism, the effective revocation of system users becomes a formidable challenge. An efficient user revocation method is crucial for achieving dynamic member management and access control to business data within the system. This not only contributes to ensuring real-time security and reliability of the system but also aids in maintaining the integrity of the system. Within the digital supply chain, we demonstrate the significance of revocable IBE (RIBE) schemes, as Fig. 1.

Boldyreva et al.[4] introduced a indirect revocation model by utilizing the framework of subset-cover, significantly minimizes the regular burden on the KGC's (Key Generation Center) workload to logarithmic levels. This construction has been widely adopted by subsequent schemes, more compact and efficient RIBE and revocable attribute-based encryption (RABE) were proposed[5–7]. However, devising a viable revocation model remains an ongoing challenge, especially in scenarios where the KGC experiences high workloads and the system users face heavy storage burdens.

To enhance the applicability of RIBE in practicalities, broader attack scenarios and privacy requisites need consideration. One common concern is the occurrence of events where decryption keys are exposed, frequently as a result of user error or outside assaults. To address this issue, Seo and Emura[8] proposed a notion in security termed as decryption key exposure resistance (DKER). DKER ensures the confidentiality of ciphertext in other time periods will not be damaged even if the decrypting key is exposed at any time. Afterwards, DKER has become a vital security requirement for RIBE and RABE schemes, prompting numerous subsequent works[9–11]. Wang et al.[12] presented a refined version of DKER in 2023, termed as Enhanced DKER (En-DKER), which provides

[1]School of Computer and Big Data, Heilongjiang University, Harbin 150080, China. [2]College of Telecommunication and Electronic Engineering, Qiqihar University, Qiqihar 161000, China. ✉email: bishujun@hlju.edu.cn

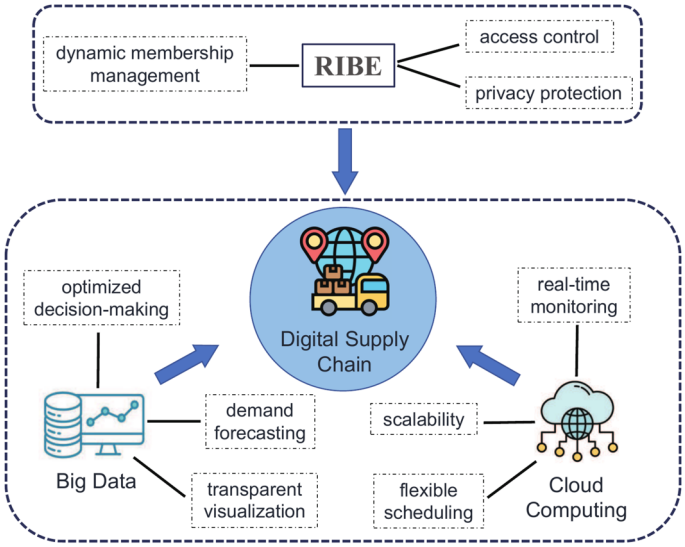


Fig. 1. Digital supply chain technology framework.

the protection of anonymity and confidentiality and ensures that even if the decryption key is exposed, neither properties will be compromised. Anonymity[13] is crucial. For instance, in financial transactions, encrypting and uploading transaction details to the cloud should not enable attackers to deduce buyers' identities from ciphertext, preventing real-time tracking and monitoring.

Ensuring the confidentiality and privacy of data in the post-quantum era has become an urgent issue. Regarding quantum computing attacks on RSA, a recent study[14] demonstrates that current quantum computers can compromise RSA-1000+. Study[15] confirms the acceleration effects of such attacks, while[16]strongly suggests the existence of polynomial-time complexity for these methods. Moreover[17], applied the hybrid quantum classical algorithm[14] to the lattice post-quantum cryptography and found some speedup, which requires a new consideration of the relationship between the lattice dimension and security. The cryptographic assumption of bilinear mapping, which is now the security basis of most RIBE schemes with DKER, which could be compromised within polynomial time by quantum computers[18]. At the same time, lattice-based cryptography with the property of resistance against quantum attacks is receiving more and more attention and research. Therefore, this paper mainly focus on constructing a RIBE scheme based on LWE, which can ensure more reliable security guarantees for data transmission and storage in the post-quantum era. We provide three main contributions:

- *A new revocation model* We present an integrated revocation model in which the encryptor is relieved from handling revocation information. This model offers a constant-level workload for the KGC and keeps users' secret keys at a constant size, which is well-suited for scenarios where the KGC experiences high workloads and the system users face heavy storage burdens.
- *A lattice-based integrated revocation IBE scheme* We construct a lattice-based online/offline integrated revocation IBE with En-DKER (OO-IRIBE-EnDKER) based on the integrated revocation model, which is IND-sRID-CPA secure under LWE.
- *Performance* We implement the OO-IRIBE-EnDKER scheme. Experimental data validates the advantages of the proposed integrated revocation model. Additionally, through the utilization of online/offline encryption techniques, the computational overhead of data owner is reduced.

Related works

Revocation model

Attrapadung et al.[19] considered that in certain specific scenarios, data owners have the right to control revocation list information, which is a direct revocation model. As a result of utilizing revocation lists, data owners have the ability to encrypt and produce ciphertexts accessible solely to users who are not revoked. Consequently, the necessity for periodic key updates is eliminated by this method, benefiting both users and KGC. Qin et al.[20] utilized a semi trusted server to perform key updates periodically for users, which is server-aided revocation model. The burden on the user is significantly reduced as this model, which enables arbitrary period decryption with just a secret key of constant level held by the user. Recently, Wang et al.[12] introduced a new revocation model which makes the KGC's periodic workload nearly insignificant and remains versatile across various scenarios. Table 1 presents the main differences between our model and existing models, where N = total number of users, r = the number of revoked users, $\alpha = O(logN)$, $\beta = O(r\log(N/r))$.

Revocation scheme

The RIBE from LWE was pioneered by Chen et al.[21], but this scheme does not consider DKER. In 2019, Katsumata et al.[22] divided the decryption key and ciphertext into two levels, and merged the RIBE scheme[21] with lattice-

Revocation model	The size of secret key	KGC's workload		RL managers
		Secret key	Periodic workload	
Indirect[4]	α	α	β	KGC
Wang et al.'s[12]	α	α	≈ 0	KGC
Direct[19]	α	α	–	Encryptor
Server-aided[20]	$O(1)$	$O(1)$	β	KGC
Integrated	$O(1)$	$O(1)$	≈ 0	KGC

Table 1. Model comparison.

based HIBE frameworks[23], realized the RIBE scheme with DKER from lattice. For improve the efficiency, Zhang et al.[24] constructed a server-aided RIBE, and Wang et al.[25] constructed two schemes, one with high efficiency and the other with high security.

However, anonymity is not maintained in these schemes in scenarios where decryption keys are leaked. Takayasu and Watanabe[26,27] constructed a RIBE scheme that incorporates bounded DERK along with anonymity features. In 2023, Wang et al.[12] proposed a RIBE with anonymity and DKER, which called En-DKER. Furthermore, they introduced a novel technique for delegating lattice basis operations, which allows for the assignment of sampling tasks to servers not trusted, significantly reduce the workload of user-generated decryption keys.

In other public-key encryption schemes such as Attribute-Based Encryption (ABE), revocable encryption also constitutes a critical research focus. Guo et al.[28]. proposed a blockchain-aided ABE scheme that eliminates key escrow through two-party computation and allows efficient user revocation with minimal overhead through group key updates. Li et al.[29] proposed a collusion-resistant CP-ABE scheme with efficient attribute revocation using attribute groups. Chen et al.[30] proposed a revocable attribute-based encryption scheme that securely delegates revocation to cloud servers while ensuring data integrity and full security.

Online/offline

Guo et al.[31] pioneered online/offline for the encryption process. In this model, the intensive computational work is handled offline, thereby lessening the online computational load for users. Liu et al.[32] further constructed a more efficient online/offline IBE scheme. Lai et al.[33] introduced a semi-generic transformation for deriving online/offline encryption from traditional IBE. This transformation explores a notably more efficient variant. Cui et al.[34] introduced attribute-based keyword search by adopting online/offline in mobile cloud environments. This integration is designed to decrease computational costs for both online and local calculations, catering to the needs of mobile users. Recently, Zuo et al.[35] proposed an LWE-based identity-based online/offline encryption scheme with offline precomputation, achieving 65-80% faster online encryption and quantum-resistant CPA security under the standard model.

Forward and backward secrecy

Regarding forward security and backward security, different cryptographic schemes have distinct definitions. For instance, in searchable encryption[36], forward security ensures that newly updated entries cannot be linked to previous search results, while backward security guarantees that search queries should not leak matching entries after their deletion. For revocable encryption, the definitions of forward and backward security are as follows: only systems supporting both forward secrecy and backward secrecy can prevent revoked users from accessing sensitive data[37]. Forward security is inherently provided in revocable encryption-once a user is revoked, they can no longer access subsequently encrypted data. However, to the best of our knowledge, existing lattice-based revocable identity-based encryption schemes have yet to achieve backward security, which remains an open challenge requiring resolution in future research.

Motivation

The construction approach of integrated revocation as follow. Firstly, we analyze in detail the several existing revocation models. For better analysis and comparison, we provide their flowcharts as shown in Fig. 2, where solid lines represent public channels published to the cloud server, while dotted lines represent secure private channels. $\mathrm{Path}(\eta_{\mathrm{ID}})$ and $\mathrm{KUNodes}(\mathrm{RL_t})$ denote two distinct sets of nodes. $\mathrm{Path}(\eta_{\mathrm{ID}})$ encompasses whole nodes from leaf node η_{ID} to the root, $\mathrm{KUNodes}(\mathrm{RL_t})$ represents the minimum ancestor set of user nodes that have not been revoked at time t[38].

By comparing Fig. 2a and b, we can clearly see that direct revocation model[19] can only applies to scenarios where the data owner has the authority to manage the revocation list RL_t. In addition, besides being restricted to limited scenarios, this model is also only applicable to fine-grained revocable encryption schemes. By observing Fig. 2c, we found that although users in Qin et al.'s server-aided revocation model[20] do not need to periodically update the key, the workload the KGC still grows logarithmically. As illustrated in Fig. 2d, Wang et al.[12] discovered that $\mathrm{KUNodes}(\mathrm{RL_t})$ reveals no information about the revocation list. This is due to the adversary's inability to associate individual leaf nodes with specific users. Within their models of revocation, the KGC is responsible for the regular generates and broadcasts of the $\mathrm{KUNodes}(\mathrm{RL_t})$ set, which is a negligible workload.

However, in the mentioned revocation models, the workload for the KGC both grow logarithmically with the amount of system users N. The rationale behind this stems from incorporating binary trees into their

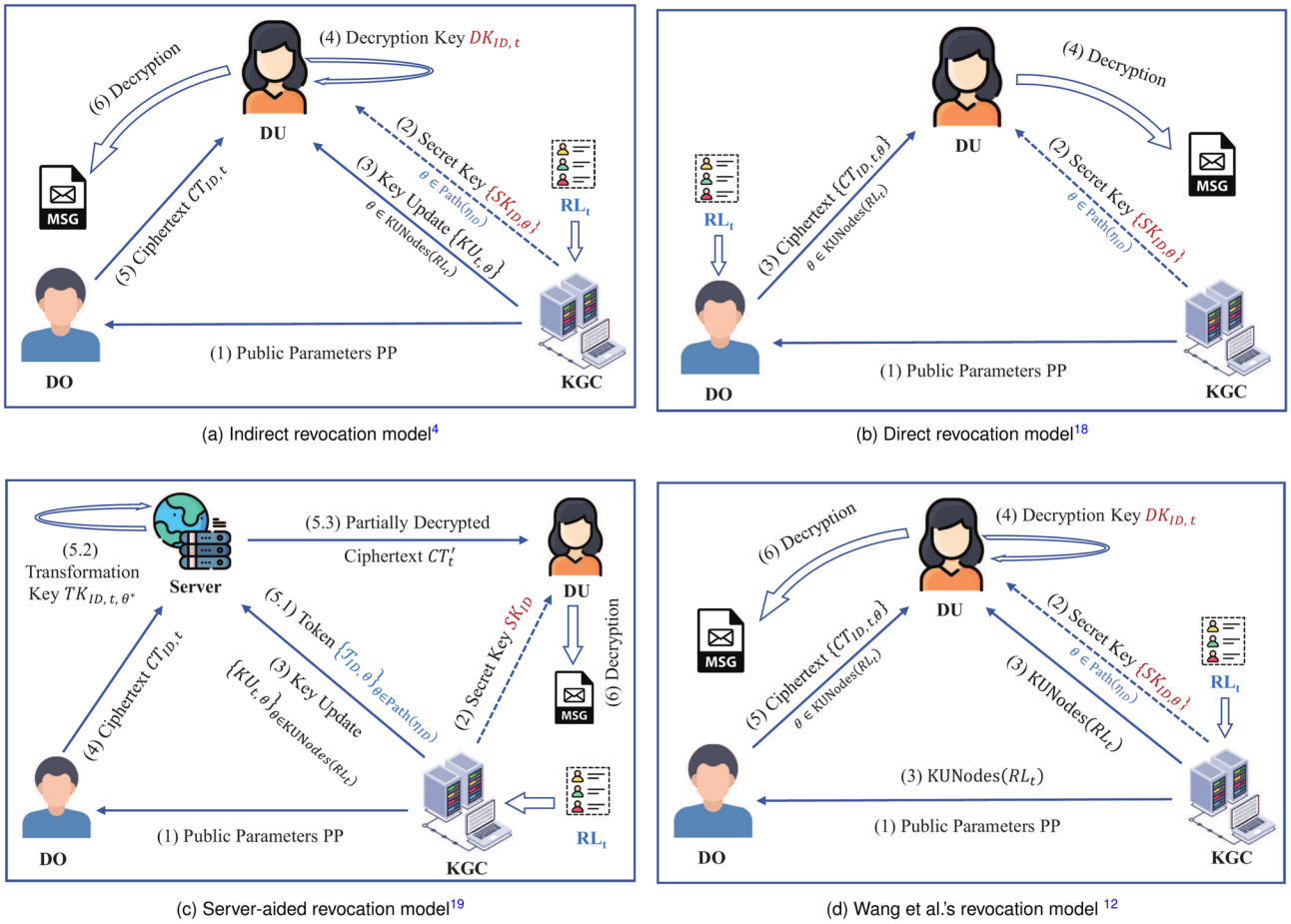


Fig. 2. Four current revocation models.

indirect revocation model design, targeting a reduction in the KGC's periodic workload from a linear scale to a logarithmic one[4]. But this change simultaneously elevates the size of users' secret keys from a constant level to a logarithmic one.

Surprisingly, we found that the binary tree structure may not be necessary. In Wang et al.'s revocation model[12], the KGC's periodic workload is already almost negligible, and the revocation list is managed by the KGC, making the application scenarios unrestricted. Based on this model, we made further improvements by no longer utilizing a binary tree structure and instead having the KGC manage a number list NL containing N numbers. Each user is randomly associated with one of these numbers and the KGC updates the set NRno_t in each period, which represents all users who have not been revoked. In consequence, the KGC's workload is now solely determined by the assigned number and user identity, with no dependence on the binary tree's depth. This ensures that all of the KGC's workload is $O(1)$. Additionally, only the KGC knows the correspondence between users and numbers. Furthermore, our lattice based RIBE scheme can similarly have the En-DKER property, since the advantages of[12] are exploited. Additionally, by utilizing the approach proposed in[12] to delegate a lattice basis, significantly reduce the workload of user-generated decryption keys.

Preliminaries

For column vector $\mathbf{x}$, let $||\mathbf{x}|| = \sqrt{\sum_i x_i^2}$. For matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, let $||\mathbf{A}|| = max\{||\mathbf{x_i}||\}_{i \in [m]}$, where $\mathbf{x_i}$ is the column of $\mathbf{A}$. Let $\mathscr{L}_q^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m | \mathbf{Ax} = \mathbf{0} \bmod q\}$, $\mathscr{L}_q^{\mathbf{u}}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m | \mathbf{Ax} = \mathbf{u} \bmod q\}$, where $\mathbf{u} \in \mathbb{Z}_q^n$, $\widetilde{\mathbf{A}}$ be the Gram–Schmidt orthogonalization of $\mathbf{A}$. Let $\rho_\sigma(\mathbf{x}) = \exp(-\pi||x||^2/\sigma^2)$, $\rho_\sigma(\mathscr{L}) = \sum_{\mathbf{x} \in \mathscr{L}} \rho_\sigma(\mathbf{x})$, then discrete gaussian distribution $\rho_{\mathscr{L},\sigma}(\mathbf{x}) = \rho_\sigma(\mathbf{x})/\rho_\sigma(\mathscr{L})$, where $\sigma > 0$. Let $[n] = \{1, \ldots, n\}$.

Lemma 1 [39] *When* $\sigma = \tilde{\Omega}(n)$ *and* $\mathbf{x} \leftarrow \mathscr{D}_{\mathscr{L}_q^{\perp}(\mathbf{A}),\sigma}$, $\Pr[||\mathbf{x}|| \geq \sigma\sqrt{m}] < \epsilon$ *holds, where* $n > 0, q > 2, m > n$, $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$.

Lemma 2 [39] *The distribution between uniform distribution over* $\mathbb{Z}_q^n$ *and* $\mathbf{Ae}$ *is statistically close, where* $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$, $\mathbf{e} \leftarrow \mathscr{D}_{\mathbb{Z}^m,\sigma}$, $n > 0, m > 2n \log q, q > 2$.

Lemma 3 [40–42] *Let* $q \geq 2, n > 0, m \geq 2n\lceil \log q \rceil$, *there exist the following PPT algorithms.*

- *The algorithm* $\mathrm{TrapGen}(1^n, 1^m, q)$ *with a full rank matrix* $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ *and trapdoor* $\mathbf{T_A} \in \mathbb{Z}^{m\times m}$ *as output, where* $\mathbf{AT_A} = 0$, $||\mathbf{T_A}|| \leq O(n\log q)$, *and the distribution between uniform distribution over* $\mathbb{Z}_q^{n\times m}$ *and* $\mathbf{A}$ *is statistically close. Furthermore, There are publicly matrix* $\mathbf{G} \in \mathbb{Z}_q^{n\times m}$ *and its trapdoor* $\mathbf{T_G}$, *where* $||\widetilde{\mathbf{T_G}}|| \leq \sqrt{5}$.
- *The algorithm* $\mathrm{SamplePre}(\mathbf{A}, \mathbf{T_A}, \sigma, \mathbf{u})$ *with* $\mathbf{s} \in \mathbb{Z}_q^m$ *as output, where* $\mathbf{As} = \mathbf{u} \in \mathbb{Z}_q^n$, $\sigma \geq ||\widetilde{\mathbf{T_A}}|| \cdot \omega(\sqrt{\log m})$, *The distribution* $\mathbf{s}$ *and* $\mathscr{D}_{\mathscr{L}_q^{\mathbf{u}}(\mathbf{A}),\sigma}$ *are statistically close.*
- *The algorithm* $\mathrm{SampleLeft}(\mathbf{A}, \mathbf{M}, \mathbf{T_A}, \sigma, \mathbf{u})$ *with* $\mathbf{s} \in \mathbb{Z}_q^{m+m_0}$ *as output, where* $[\mathbf{A}|\mathbf{M}]\mathbf{s} = \mathbf{u} \in \mathbb{Z}_q^n$, $\mathbf{M} \in \mathbb{Z}_q^{n\times m_0}$, $\sigma \geq ||\widetilde{\mathbf{T_A}}|| \cdot \omega(\sqrt{\log(m+m_0)})$. *The distribution* $\mathbf{s}$ *and* $\mathscr{D}_{\mathscr{L}_q^{\mathbf{u}}([\mathbf{A}|\mathbf{M}]),\sigma}$ *are statistically close.*
- *The algorithm* $\mathrm{SampleRight}(\mathbf{A}, \mathbf{G}, t, \mathbf{R}, \mathbf{T_G}, \sigma, \mathbf{u})$ *with* $\mathbf{s} \in \mathbb{Z}_q^{2m}$ *as output, where* $[\mathbf{A}|\mathbf{AR} + t\mathbf{G}]\mathbf{s} = \mathbf{u} \in \mathbb{Z}_q^n$, $t \in \mathbb{Z}^*$, $\mathbf{R} \leftarrow \{-1, 1\}^{m\times m}$, $\sigma \geq ||\widetilde{\mathbf{T_G}}|| \cdot \sqrt{m} \cdot \omega(\sqrt{\log m})$. *The distribution* $\mathbf{s}$ *and* $\mathscr{D}_{\mathscr{L}_q^{\mathbf{u}}([\mathbf{A}|\mathbf{AR}+t\mathbf{G}]),\sigma}$ *are statistically close.*

The LWE assumption[43]. If $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^m$, $\gamma \leftarrow \mathbb{Z}_q^n$, and $e \leftarrow \mathscr{D}_{\mathbb{Z}^n,\sigma}$, then $(\mathbf{A}, \mathbf{As} + e)$ and $(\mathbf{A}, \gamma)$ are computationally indistinguishable.

Definition 1 If $Pr_{x\leftarrow\mathscr{D}_\lambda}[|x| \leq \mathscr{B}(\lambda)] = 1 - \epsilon$, then the distribution $\mathscr{D}_\lambda$ is called B-bounded.

Lemma 4 [44] *Let* B_1 *and* B_2 *be integer polynomials of* λ. *Consider two distribution families:* $\mathscr{D}$, *which is* B_1 *-bounded, and the uniform distribution* $\mathscr{U}$ *over* $[-B_2, B_2]$. *If* $|B_1/B_2| \leq \mathrm{negl}(\lambda)$, *then* $\mathscr{D} + \mathscr{U}$ *is statistically close to* $\mathscr{U}$.

Lemma 5 [23] *If* $\omega(\log n) + (\log q)(n+1) < m$, *then* $(\mathbf{A}, \mathbf{AX})$ *and* $(\mathbf{A}, \mathbf{U})$ *are statistically indistinguishable, where* $\mathbf{A}, \mathbf{U} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{x} \leftarrow \{-1, 1\}^{m\times m}$.

Definition 2 For any different $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_q^n$, we have $(\mathrm{H}(\mathbf{u}) - \mathrm{H}(\mathbf{v})) \in \mathbb{Z}_q^{n\times n}$ is non singular, then H is called a full-rank different map.

System architecture and definitions

The proposed integrated revocation model and the definition of the OO-IRIBE-EnDKER are introduced in section Integrated revocation mode, the security definition for the OO-IRIBE-EnDKER is provided insection Security.

Integrated revocation model

Figure 3 illustrates our system model, which consists of three entities: data user (DU), data owner (DO) and KGC.

- KGC: Responsible for generating public parameters PP, generating secret keys $\mathrm{SK}_{\mathrm{ID},no_{\mathrm{ID}}}$ for users, managing the revocation list RL_t and publicly releasing a number set NRno_t for time t. In our system, the KGC is fully trusted.
- DO: Encrypts and shares data with recipient (DU) by leveraging PP and NRno_t. DO is also fully trusted.
- DU: Uses secret key $\mathrm{SK}_{\mathrm{ID},no_{\mathrm{ID}}}$ to get the decryption key $\mathrm{DK}_{\mathrm{ID},t}$. DU is an entity that intends to access encrypted data. DU is semi-trusted, as malicious DU may intentionally leak partial or modified decryption keys. To reduce the computational overhead for DU in generating decryption keys, our system will incorporate the Cloud Service Provider (CSP). However, CSP is not related to our proposed integrated undo model, so we no longer represent that individual in Fig. 3. CSP assists DU in generating decryption keys. The CSP operates

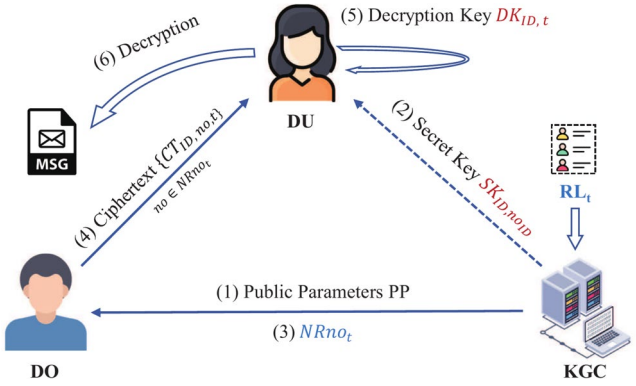


Fig. 3. Ours integrated revocation model.

under a semi-honest model, meaning it faithfully executes authorized requests and refrains from data leakage, yet actively attempts to infer maximal information from both operational procedures and resultant outputs.

There are seven algorithms in the OO-IRIBE-EnDKER scheme.

(1) $\mathbf{Setup}(1^\lambda, N) \rightarrow \{\mathrm{PP}, \mathrm{MSK}\}$. For given security parameter λ and number of system users N, KGC produces PP and MSK as output, where MSK that contains a number list NL with N numbers.
(2) $\mathbf{GenSK}(\mathrm{PP}, \mathrm{ID}, \mathrm{MSK}) \rightarrow \mathrm{SK}_{\mathrm{ID}}$. For given PP, $\mathrm{ID} \in \mathscr{I}\mathscr{D}$(user identity sapce) and MSK, KGC produces ID's secret key $\mathrm{SK}_{\mathrm{ID}}$ as output, where the user identity ID is randomly associated with one number no_{ID} from NL, and only the KGC knows the correspondence between users and numbers.
(3) $\mathbf{NumUp}(\mathrm{PP}, \mathrm{MSK}, \mathrm{NL}, t, \mathrm{RL}_t) \rightarrow \mathrm{NRno}_t$. For given PP, MSK, NL, a revocation list RL_t at time t, KGC produces a number set NRno_t as output, which represents the users who have not been revoked at time t.
(4) $\mathbf{GenDK}(\mathrm{PP}, t, \mathrm{SK}_{\mathrm{ID}}) \rightarrow \mathrm{DK}_{\mathrm{ID},t}$. For given PP, t, $\mathrm{SK}_{\mathrm{ID}}$, DU produces a decryption key $\mathrm{DK}_{\mathrm{ID},t}$ as output.
(5) $\mathbf{Offline.Enc}(\mathrm{PP}, t, \mathrm{NRno}_t) \rightarrow \mathrm{IT}$. For given PP, t, NRno_t, DO produces an intermediate ciphertext IT as output.
(6) $\mathbf{Online.Enc}(\mathrm{PP}, \mathrm{ID}, \mathrm{IT}, \mu) \rightarrow \mathrm{CT}_{\mathrm{ID},t}$. For given PP, ID, IT, and plaintext μ, DO produces the ciphertext $\mathrm{CT}_{\mathrm{ID},t}$ as output.
(7) $\mathbf{Dec}(\mathrm{CT}_{\mathrm{ID},t}, \mathrm{DK}_{\mathrm{ID},t}) \rightarrow \mu'$. For given $\mathrm{CT}_{\mathrm{ID},t}$, $\mathrm{DK}_{\mathrm{ID},t}$, DU produces message μ'.

Security

The security model for OO-IRIBE-EnDKER is established through the game between adversary $\mathscr{A}$ and challenger $\mathscr{C}$.

Initialize: $\mathscr{A}$ sends the identities $\mathrm{ID}^{(i)}, i = 1, 2$, time t^* and number set NRno_t^* to $\mathscr{C}$.
Setup Phase: $\mathscr{C}$ performs **Setup** and outputs PP.
Learning Phase: The following oracle can be adaptive access polynomials by $\mathscr{A}$.

1. The number list NL establishment oracle $\mathscr{O}_{\mathscr{N}\mathscr{L}}$: $\mathscr{A}$ initiates with the query $\mathscr{Q}_0 = \{\mathrm{ID}\}$, and $\mathscr{C}$ randomly selects an unassigned number no_{ID} for the ID. Upon completing the query, $\mathscr{C}$ returns " NL has been established" to $\mathscr{A}$.

In the following queries, we assume that the $no_{\mathrm{ID}} \in \mathrm{NL}$ corresponding to the ID has already been established.

2. Secret key oracle $\mathscr{O}_{\mathscr{S}\mathscr{K}}$: $\mathscr{A}$ initiates with the query $\mathscr{Q}_1 = \{\mathrm{ID}\}$. If $\mathrm{ID} \in \{\mathrm{ID}^{(i)}\}_{i=0,1}$; or $\mathrm{ID} \in \mathrm{RL}_{t^*}^*$, then $\mathscr{C}$ returns $\perp$. Otherwise, $\mathscr{C}$ returns $\mathrm{SK}_{\mathrm{ID}}$.
3. Decryption key oracle $\mathscr{O}_{\mathscr{D}\mathscr{K}}$: $\mathscr{A}$ initiates with the query $\mathscr{Q}_2 = \{(\mathrm{ID}, t_{cu})\}$. If (1)$\mathrm{ID} \in \mathrm{RL}_{t_{cu}}$; or (2) $t_{cu} = t^*$, $\mathrm{ID} \in \{\mathrm{ID}^{(i)}\}_{i=0,1}$; or (3) global variable $t_{cu+1} \geq t_{cu}$, then $\mathscr{C}$ returns $\perp$. Otherwise, $\mathscr{C}$ returns $\mathrm{DK}_{\mathrm{ID},t}$.
4. Revocation oracle $\mathscr{O}_{\mathscr{R}\mathscr{L}}$: $\mathscr{A}$ initiates with the query $\mathscr{Q}_3 = \{(\mathrm{ID}, t_{cu})\}$. $\mathscr{C}$ obtains $\mathrm{RL}_{t_{cu}+1}$ by updating $\mathrm{RL}_{t_{cu}}$, where $\mathrm{ID} \in \mathrm{RL}_{t_{cu}+1}$, $\mathrm{RL}_{t_{cu}} \subseteq \mathrm{RL}_{t_{cu}+1}$, $t_{cu+1} \geq t_{cu}$, calculates and returns NRno_t to $\mathscr{A}$, where $\{\mathrm{ID}^{(i)}\}_{i=0,1} \subseteq \mathscr{Q}_3$ or $\{\mathrm{ID}^{(i)}\}_{i=0,1} \nsubseteq \mathscr{Q}_3$.**Challenge Phase**: $\mathscr{A}$ sends plaintexts $\mu^{(i)}$ to $\mathscr{C}$, $i = 0, 1$. $\mathscr{C}$ chooses $b \leftarrow \{0, 1\}$, computes $\mathrm{IT}^* \leftarrow \mathsf{Offline.Enc}(\mathrm{PP}, t^*, \mathrm{NRno}_t^*)$, $\mathrm{CT}_{\mathrm{ID}^{(b)},t^*} \leftarrow \mathsf{Online.Enc}(\mathrm{PP}, \mathrm{ID}^{(b)}, \mathrm{IT}^*, \mu^{(b)})$, and returns $\mathrm{CT}_{\mathrm{ID}^{(b)},t^*}$.

Guess: $\mathscr{A}$ outputs the guess bit b'.

Let $\mathrm{Adv}_{\mathrm{RIBE},\mathscr{A}}^{\mathsf{SEL\text{-}\ En\text{-}\ CPA}}(\lambda) = |\Pr[b = b'] - 1/2|$ be the advantage of adversar $\mathscr{A}$ winning the game. If $\mathrm{Adv}_{\mathrm{RIBE},\mathscr{A}}^{\mathsf{SEL\text{-}\ En\text{-}\ CPA}}(\lambda) < \epsilon$, then then OO-IRIBE-EnDKER scheme is IND-sRID-CPA secure.

In addition, we classify adversaries' strategies into two categories:

1. If $\{\mathrm{ID}^{(0)}, \mathrm{ID}^{(1)}\} \subseteq \mathrm{RL}_{t^*}$, then $\mathscr{A}$ can query for $\mathscr{O}_{\mathscr{S}\mathscr{K}}$ and $\mathscr{O}_{\mathscr{D}\mathscr{K}}$ for $t \neq t^*$.
2. If $\{\mathrm{ID}^{(0)}, \mathrm{ID}^{(1)}\} \nsubseteq \mathrm{RL}_{t^*}$, then $\mathscr{A}$ can only query for $\mathscr{O}_{\mathscr{D}\mathscr{K}}$ for $t \neq t^*$.

The OO-IRIBE-EnDKER scheme

We present the OO-IRIBE-EnDKER scheme, show the correctness of the prososed shceme, and prove the security.

Construction

1. $\mathbf{Setup}(1^\lambda, N) \rightarrow \{\mathrm{MSK}, \mathrm{PP}\}$. For given total number of user N and security parameter λ, KGC selects a modulus q for LWE and determine dimensions n and m, gets $(\mathbf{A}, \mathbf{T_A})$ by running TrapGen, chooses $\mathbf{B}, \mathbf{W} \leftarrow \mathbb{Z}_q^{n \times m}$, $\{\mathbf{u}_i\}_{i \in [l]} \leftarrow \mathbb{Z}_q^n$, constructs a list NL consisting of at least N numbers. Then, for every no in NL, choose $\mathbf{D}_{no} \leftarrow \mathbb{Z}_q^{n \times m}$. At last, KGC keeps $\mathrm{MSK} = \{\mathbf{T_A}, \mathrm{NL}\}$ and outputs $\mathrm{PP} = \{\mathbf{A}, \{\mathbf{u}_i\}_{i \in [l]}, \mathbf{B}, \{\mathbf{D}_{no}\}_{no \in \mathrm{NL}}, \mathbf{W}\}$.

2. $\mathbf{GenSK}(\mathrm{PP}, \mathrm{ID}, \mathrm{MSK}) \rightarrow \mathrm{SK}_{\mathrm{ID}}$. For given $\mathrm{PP}, \mathrm{ID}, \mathrm{MSK}$, KGC chooses number $no_{\mathrm{ID}} \leftarrow \mathrm{NL}$ that hasn't been allocated and associate it with the ID, chooses $\mathbf{x}'_{\mathrm{ID}} \leftarrow \chi^{2m\times 2m}_{\mathrm{LWE}}$ sets $\mathbf{Y}_{\mathrm{ID}} = [\mathbf{A}|\mathbf{B}_{\mathrm{ID}}]\mathbf{x}'_{\mathrm{ID}}$, where $\mathbf{B}_{\mathrm{ID}} = \mathbf{B} + \mathrm{H}(\mathrm{ID})\mathbf{G}$, samples $\mathbf{x}''_{no_{\mathrm{ID}}} \leftarrow \mathrm{SampleLeft}(\mathbf{A}, \mathbf{D}_{no_{\mathrm{ID}}}, \mathbf{T}_{\mathbf{A}}, \sigma, \mathbf{G} - \mathbf{Y}_{\mathrm{ID}})$. Let $\mathbf{x}'_{\mathrm{ID}} = \begin{bmatrix}\mathbf{x}'_{1,\mathrm{ID}}\\ \mathbf{x}'_{2,\mathrm{ID}}\end{bmatrix}$, $\mathbf{x}''_{no_{\mathrm{ID}}} = \begin{bmatrix}\mathbf{x}''_{1,no_{\mathrm{ID}}}\\ \mathbf{x}''_{2,no_{\mathrm{ID}}}\end{bmatrix}$, $\mathbf{x}_{\mathrm{ID},no_{\mathrm{ID}}} = \begin{bmatrix}\mathbf{x}'_{1,\mathrm{ID}} + \mathbf{x}''_{1,no_{\mathrm{ID}}}\\ \mathbf{x}'_{2,\mathrm{ID}}\\ \mathbf{x}''_{2,no_{\mathrm{ID}}}\end{bmatrix} \in \mathbb{Z}_q^{3m\times 2m}$, we have $[\mathbf{A}|\mathbf{B}_{\mathrm{ID}}|\mathbf{D}_{no_{\mathrm{ID}}}]\mathbf{K}_{\mathrm{ID},no_{\mathrm{ID}}} = \mathbf{G}$. Output $\mathrm{SK}_{\mathrm{ID}} = \mathbf{x}_{\mathrm{ID},no_{\mathrm{ID}}}$.
3. $\mathbf{NumUp}(\mathrm{PP}, \mathrm{MSK}, \mathrm{NL}, t, \mathrm{RL}_t) \rightarrow \mathrm{NRno}_t$. Input $\mathrm{PP}, \mathrm{MSK}, \mathrm{NL}, t, \mathrm{RL}_t$. KGC outputs and broadcasts a set NRno_t, which represents the users who have not been revoked, using number list NL and revocation list RL_t at time t.
4. $\mathbf{GenDK}(\mathrm{PP}, \mathrm{SK}_{\mathrm{ID}}, t) \rightarrow \mathrm{DK}_{\mathrm{ID},t}$. Input $\mathrm{PP}, \mathrm{SK}_{\mathrm{ID}}, t$. Compute $\mathbf{W}_t = \mathbf{W} + \mathrm{H}(t)\mathbf{G}$. For any $B \in \mathbb{N}$, let $\mathscr{U}_B$ denote the uniform distribution on, i.e. integers between $\pm B$. For $i \in [l]$, DU chooses $\mathbf{x}_{i,t} \leftarrow \mathscr{U}_B^{4m}$, computes and sends $\mathbf{h}_{i,\mathrm{ID},t} = [\mathbf{A}|\mathbf{B}_{\mathrm{ID}}|\mathbf{D}_{no_{\mathrm{ID}}}|\mathbf{W}_t]\mathbf{x}_{i,t}$ to cloud. Cloud computes $\mathbf{x}'_{i,\mathrm{ID},t}$ by $\mathrm{SamplePre}$ such that $\mathbf{G}\mathbf{x}'_{i,\mathrm{ID},t} = \mathbf{u}_i - \mathbf{h}_{i,\mathrm{ID},t}$ and sends $\mathbf{x}'_{i,\mathrm{ID},t}$ to DU (The purpose of cloud server participation is to reduce the computational workload of users). DU computes $\mathbf{X}''^{no_{\mathrm{ID}},t}_{i,\mathrm{ID}} = \mathbf{x}_{\mathrm{ID},no_{\mathrm{ID}}}\mathbf{X}'_{i,\mathrm{ID},t}$, and has $[\mathbf{A}|\mathbf{B}_{\mathrm{ID}}|\mathbf{D}_{no_{\mathrm{ID}}}]\mathbf{X}''_{i,\mathrm{ID},no_{\mathrm{ID}},t} = \mathbf{u}_i - \mathbf{h}_{i,\mathrm{ID},t}$. Let

$$(\mathbf{x}_{i,t})^T = \left[(\mathbf{x}^1_{i,t})^T, (\mathbf{x}^2_{i,t})^T, (\mathbf{x}^3_{i,t})^T, (\mathbf{x}^4_{i,t})^T\right]^T, (\mathbf{X}''^{no_{\mathrm{ID}}}_{i,\mathrm{ID},t})^T = \left[(\mathbf{X}''^{no_{\mathrm{ID}},1}_{i,\mathrm{ID},t})^T, (\mathbf{X}''^{no_{\mathrm{ID}},2}_{i,\mathrm{ID},t})^T, (\mathbf{X}''^{no_{\mathrm{ID}},3}_{i,\mathrm{ID},t})^T\right]^T.$$

Output $\mathrm{DK}_{\mathrm{ID},t} = \{\mathbf{dk}^{no_{\mathrm{ID}}}_{i,\mathrm{ID},t}\}_{i\in[l]}$, where $[\mathbf{A}|\mathbf{B}_{\mathrm{ID}}|\mathbf{D}_{no_{\mathrm{ID}}}|\mathbf{W}_t]\mathbf{dk}^{no_{\mathrm{ID}}}_{i,\mathrm{ID},t} = \mathbf{u}_i$ and

$$(\mathbf{dk}^{no_{\mathrm{ID}}}_{i,\mathrm{ID},t})^T = \left[(\mathbf{X}''^{no_{\mathrm{ID}},1}_{i,\mathrm{ID},t} + \mathbf{x}^1_{i,t})^T, (\mathbf{X}''^{no_{\mathrm{ID}},2}_{i,\mathrm{ID},t} + \mathbf{x}^2_{i,t})^T, (\mathbf{X}''^{no_{\mathrm{ID}},3}_{i,\mathrm{ID},t} + \mathbf{x}^3_{i,t})^T, (\mathbf{x}^4_{i,t})^T\right]^T.$$

5. $\mathbf{Offline.Enc}(\mathrm{PP}, t, \mathrm{NRno}_t) \rightarrow \mathrm{IT}$. Input $\mathrm{PP}, t, \mathrm{NRno}_t$. DO chooses $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{V}, \mathbf{S}, \mathbf{R}_{no} \leftarrow \{-1, 1\}^{m\times m}$, where $no \in \mathrm{NRno}_t$, $\mathbf{e}' \leftarrow \chi^m_{\mathrm{LWE}}$, $e_i \leftarrow \chi_{\mathrm{LWE}}$, where $i \in [l]$, computes $\mathbf{c}_0 = \mathbf{s}^\top\mathbf{A} + \mathbf{e}'^\top$, $\mathbf{c}'_{no} = \mathbf{s}^\top\mathbf{D}_{no} + \mathbf{e}'^\top\mathbf{R}_{no}$, $\mathbf{c}''_t = \mathbf{s}^\top\mathbf{W}_t + \mathbf{e}'^\top\mathbf{S}$, and outputs $\mathrm{IT} = \{\mathbf{V}, \mathbf{s}, \{e_i\}_{i\in[l]}, \mathbf{e}', \mathbf{c}_0, \{\mathbf{c}'_{no}\}_{no\in\mathrm{NRno}_t}, \mathbf{c}''_t\}$.
6. $\mathbf{Online.Enc}(\mathrm{PP}, \mathrm{ID}, \mathrm{IT}, \{\mu_i\}_{i\in[l]}) \rightarrow \mathrm{CT}_{\mathrm{ID},t}$. Input $\mathrm{PP}, \mathrm{ID}, \mathrm{IT}, \{\mu_i\}_{i\in[l]}$. DO computes $C_i = \mathbf{s}^\top\mathbf{u}_i + \mu_i \cdot \lfloor \frac{q}{2} \rfloor + e_i$, $c_{\mathrm{ID}} = \mathbf{s}^\top\mathbf{B}_{\mathrm{ID}} + \mathbf{e}'^\top\mathbf{V}$, and outputs $\mathrm{CT}_{\mathrm{ID},t} = \{C_i, \mathbf{c}_0, c_{\mathrm{ID}}, \{\mathbf{c}'_{no}\}_{no\in\mathrm{NRno}_t}, \mathbf{c}''_t\}$.
7. $\mathbf{Dec}(\mathrm{CT}_{\mathrm{ID},t}, \mathrm{DK}_{\mathrm{ID},t}) \rightarrow \{\mu_i\}_{i\in[l]}$. For given $\mathrm{CT}_{\mathrm{ID},t}, \mathrm{DK}_{\mathrm{ID},t}$. each $i \in [l]$, DU computes $C'_i = C_i - [\mathbf{c}_0|\mathbf{c}_{\mathrm{ID}}|\mathbf{c}'_{no_{\mathrm{ID}}}|\mathbf{c}''_t]\mathbf{dk}_{i,\mathrm{ID},no_{\mathrm{ID}},t}$. Output 1 if $|C'_i - \lfloor \frac{q}{2} \rfloor| < \lfloor \frac{q}{4} \rfloor$, otherwise 0, where $i \in [l]$.

Correctness

If user $\mathrm{ID} \notin \mathrm{RL}_t$, then $no_{\mathrm{ID}} \in \mathrm{NRno}_t$. So $C'_i = C_i - [\mathbf{c}_0|\mathbf{c}_{\mathrm{ID}}|\mathbf{c}'_{no_{\mathrm{ID}}}|\mathbf{c}''_t]\mathbf{dk}_{i,\mathrm{ID},no_{\mathrm{ID}},t} = \mu_i \cdot \lfloor \frac{q}{2} \rfloor + \Delta$, where $i \in [l]$, $\Delta = e_i - \mathbf{e}'^\top[\mathbf{I}_m|\mathbf{V}|\mathbf{R}_{no_{\mathrm{ID}}}|\mathbf{S}]\mathbf{dk}^{no_{\mathrm{ID}}}_{i,\mathrm{ID},t}$.

From Lemmas 1 and 4, we have $||\mathbf{x}^j_{i,t}|| \le \sqrt{m}B, j \in [4]$, $||e_i|| \le \sigma$, $||\mathbf{e}'|| \le \sqrt{m}\sigma$. Since matrices $\mathbf{V}$, $\mathbf{R}_{no}$, and $\mathbf{S}$ are uniformly randomly selected from $\{-1, 1\}^{m\times m}$, so we have $||\mathbf{V}||$, $||\mathbf{R}_{no_{\mathrm{ID}}}||$, and $||\mathbf{S}|| \le O(\sqrt{m})$. Therefore, if $(1 + \sigma^2 m) < B/2^\lambda$, $\sigma BO(\sqrt{m^3}) < q/4$, we have $\Delta \le \sigma + 2m^2\sigma^2 + mB\sigma + O(\sqrt{m}) \cdot (2\sqrt{m^3}\sigma + 3B\sqrt{m}) < \sigma BO(\sqrt{m^3}) < q/4$.

Finally, judge $|C'_i - \lfloor \frac{q}{2} \rfloor| < \lfloor \frac{q}{4} \rfloor$ to get μ_i.

Security

Theorem 1 *If the LWE assumption is difficult, then the OO-IRIBE-EnDKER scheme is IND-sRID-CPA secure.*

Proof The proof unfolds through various games.

$\mathbf{Game}_0^{(b)}$: This is the security game for OO-IRIBE-EnDKER.

$\mathbf{Game}_1^{(b)}$: Select $\mathbf{V}^*$, $\{\mathbf{R}^*_{no}\}_{no\in\mathrm{NL}}$ and $\mathbf{S}^* \leftarrow \mathbb{Z}_2^{m\times m}$. Compute $\mathbf{B}^{(b)} = \mathbf{A}\mathbf{V}^* - \mathrm{H}(\mathrm{ID}^{(b)})\mathbf{G}$, $\mathbf{D}_{no} = \begin{cases}\mathbf{A}\mathbf{R}^*_{no} + \mathbf{G}, & no \in \mathrm{NRno}^*_t,\\ \mathbf{A}\mathbf{R}^*_{no}, & \text{otherwise.}\end{cases}$, and $\mathbf{W} = \mathbf{A}\mathbf{S}^* - \mathrm{H}(t^*)\mathbf{G}$. The remaining is the same as $\mathbf{Game}_0^{(b)}$.

By Lemma 5, The advantage of distinguishing between $\mathbf{Game}_0^{(b)}$ and $\mathbf{Game}_1^{(b)}$ by the adversary is negligible.

$\mathbf{Game}_2^{(b)}$: Except for the generation of $\mathrm{SK}_{\mathrm{ID}}$, the rest is the same as $\mathbf{Game}_1^{(b)}$.

Scheme	The size of SK	The size of CT		KGC's periodic workload	En-DKER	LWE
		Online	Offline			
XYM19[10]	α	$O(1)$	–	β	×	×
QZZ+19[11]	$O(1)$	$O(1)$	–	β	×	×
WHL+23[12]	α	β	–	≈ 0	√	√
CLL+12[21]	α	$O(1)$	–	β	×	√
KMT19[22]	α	$O(1)$	–	β	×	√
WZH+19[25]	α	$O(1)$	–	β	×	√
TW21[27]	α	$O(1)$	–	β	×	√
YXY23[45]	$O(1)$	$O(1)$	–	β	×	√
Ours	$O(1)$	$O(1)$	δ	≈ 0	√	√

Table 2. RIBE schemes theoretically compare.

Scheme	The size of SK	The size of CT· $\log q$		KGC's periodic workload
		Online	Offline	
WHL+23[12]	$6m^2 \log\sigma \cdot \alpha$	$2m + 1 + m \cdot \beta$	–	≈ 0
CLL+12[21]	$2m \log\sigma \cdot \alpha$	$3m + 1$	–	$\beta \cdot T_{\mathrm{SL}}$
KMT19[22]	$4m^2 + 2m \log\sigma \cdot \alpha$	$6m + 1$	–	$\beta \cdot T_{\mathrm{SL}}$
WZH+19[25]	$4m^2 + 2m \log\sigma \cdot \alpha$	$6m + 1$	–	$\beta \cdot T_{\mathrm{SL}}$
TW21[27]	$2m^2 \log\sigma \cdot \alpha$	$3m + 1$	–	$\beta \cdot T_{\mathrm{SL}}$
YXY23[45]	$m^2 + nm \log\sigma \cdot \alpha$	$6m + 3n - 2$	–	$\beta \cdot T_{\mathrm{SL}}$
Ours	$6m^2 \log\sigma$	m	$m + 1 + m \cdot \delta$	≈ 0

Table 3. Lattice-based RIBE schemes theoretically compare.

- If $\mathrm{ID} = \mathrm{ID}^b$ and $\mathrm{ID} \in \mathrm{RL}^*_{t^*}$, then $\mathbf{B}_{\mathrm{ID}} = \mathbf{AV}^*$, and $\mathbf{D}_{no_{\mathrm{ID}}} = \mathbf{AR}^*_{no_{\mathrm{ID}}} + \mathbf{G}$. Sample $\mathbf{x}''_{no_{\mathrm{ID}}}$ by SampleRight and $\mathbf{T_G}$ such that $[\mathbf{A}|\mathbf{AR}^*_{no_{\mathrm{ID}}} + \mathbf{G}]\mathbf{x}''_{no_{\mathrm{ID}}} = \mathbf{G} - \mathbf{Y}_{\mathrm{ID}}$.
- If $\mathrm{ID} \neq \mathrm{ID}^b$, then $\mathbf{B}_{\mathrm{ID}} = \mathbf{AV}^* - \mathrm{H}(\mathrm{ID}^{(b)})\mathbf{G}$. First select a random matrix $\mathbf{x}''_{no_{\mathrm{ID}}}$ in $\chi^{2m\times 2m}_{\mathrm{LWE}}$, and set $\mathbf{Y}_{\mathrm{ID}} = [\mathbf{A}|\mathbf{D}_{no_{\mathrm{ID}}}]\mathbf{x}''_{no_{\mathrm{ID}}}$. Sample $\mathbf{x}'_{\mathrm{ID}}$ by SampleRight and $\mathbf{T_G}$ such that $([\mathbf{A}|\mathbf{AV}^* + (\mathrm{H}(\mathrm{ID}) - \mathrm{H}(\mathrm{ID}^{(b)})]\mathbf{G})\mathbf{x}'_{\mathrm{ID}} = \mathbf{G} - \mathbf{Y}_{\mathrm{ID}}$.

By Lemma 3, The advantage of distinguishing between $\mathbf{Game}_1^{(b)}$ and $\mathbf{Game}_2^{(b)}$ by the adversary is negligible.

$\mathbf{Game}_3^{(b)}$: Except for the generation of $\mathrm{DK}_{\mathrm{ID},t}$, the rest is the same as $\mathbf{Game}_2^{(b)}$. When $\mathrm{ID} = \mathrm{ID}^{(b)}$, $t \neq t^*$, and $\mathrm{ID} \notin \mathrm{RL}^*_{t^*}$, sample $\widetilde{\mathbf{x}}_t$ by SampleRight and $\mathbf{T_G}$ such that $[\mathbf{A}|\mathbf{AV}^* + (\mathrm{H}(t) - \mathrm{H}(t^*))\mathbf{G}]\widetilde{\mathbf{x}}_t = \mathbf{G}$, choose $\mathbf{x}_{i,t} \leftarrow \mathscr{U}_B^{4m}$, compute $\mathbf{h}_{i,\mathrm{ID},t} = [\mathbf{A}|\mathbf{B}_{\mathrm{ID}}|\mathbf{D}_{no_{\mathrm{ID}}}|\mathbf{W}_t]\mathbf{x}_{i,t}$ and get $\mathbf{x}'_{i,\mathrm{ID},t}$ by running SamplePre such that $\mathbf{x}'_{i,\mathrm{ID},t} = \mathbf{u}_i - \mathbf{h}_{i,\mathrm{ID},t}$. Let

$$(\mathbf{dk}^{no_{\mathrm{ID}}}_{i,\mathrm{ID},t})^T = \left[(\widetilde{\mathbf{X}''}^1_{i,\mathrm{ID},t} + \mathbf{x}^1_{i,t})^T, (\mathbf{x}^2_{i,t})^T, (\mathbf{x}^3_{i,t})^T, (\widetilde{\mathbf{X}''}^2_{i,\mathrm{ID},t} + \mathbf{x}^4_{i,t})^T\right]^T$$

where $\widetilde{\mathbf{x}}''_{i,\mathrm{ID},t} = \widetilde{\mathbf{x}}_t \mathbf{X}'_{i,\mathrm{ID},t}$, $\widetilde{\mathbf{X}''}_{i,\mathrm{ID},t} = [(\widetilde{\mathbf{X}''}^1_{i,\mathrm{ID},t})^T, (\widetilde{\mathbf{X}''}^2_{i,\mathrm{ID},t})^T]^T$, $\mathbf{x}_{i,t} = [(\mathbf{x}^1_{i,t})^T, (\mathbf{x}^2_{i,t})^T, (\mathbf{x}^3_{i,t})^T, (\mathbf{x}^4_{i,t})^T]^T$.

Since $(1 + \sigma^2 m) < B/2^\lambda$, the statistical distance between $\mathbf{dk}_{i,\mathrm{ID},no_{\mathrm{ID}},t}$ in $\mathbf{Game}_2^{(b)}$ and $\mathbf{dk}_{i,\mathrm{ID},no_{\mathrm{ID}},t}$ in $\mathbf{Game}_3^{(b)}$ is negligible by Lemma 4, as evidenced in reference[12]. Therefore, $\mathbf{Game}_2^{(b)}$ and $\mathbf{Game}_3^{(b)}$ are statistically indistinguishable.

$\mathbf{Game}_4^{(b)}$: Except for the generation of $\mathbf{A}$ and challenge ciphertexts, the rest is same as $\mathrm{Game}_3^{(b)}$. Choose $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\mathbf{s} \leftarrow \mathbb{Z}_q^n$, $\mathbf{e}' \leftarrow \chi^m_{\mathrm{LWE}}$, $e_i \leftarrow \chi_{\mathrm{LWE}}$, $i \in [l]$, compute $\mathbf{c}_0 = \mathbf{s}^\top\mathbf{A} + \mathbf{e}'^\top$, $\mathbf{c}_0 = \mathbf{s}^\top\mathbf{A} + \mathbf{e}'^\top$, $c_{\mathrm{ID}} = \mathbf{s}^\top\mathbf{AV}^* + \mathbf{e}'^\top\mathbf{V}^* = \mathbf{s}^\top\mathbf{B}^{(b)}_{\mathrm{ID}} + \mathbf{e}'^\top\mathbf{V}^*$, $\mathbf{c}'_{no} = \mathbf{s}^\top(\mathbf{AR}^*_{no} + \mathbf{G}) + \mathbf{e}'^\top\mathbf{R}^*_{no} = \mathbf{s}^\top\mathbf{D}^{(b)}_{no} + \mathbf{e}'^\top\mathbf{R}^*_{no}$, $\mathbf{c}''_t = \mathbf{s}^\top\mathbf{AS}^* + \mathbf{e}'^\top\mathbf{S}^* = \mathbf{s}^\top\mathbf{W}^{(b)}_{t^*} + \mathbf{e}'^\top\mathbf{S}^*$.

By Lemma 3, The advantage of distinguishing between $\mathbf{Game}_3^{(b)}$ and $\mathbf{Game}_4^{(b)}$ by the adversary is negligible.

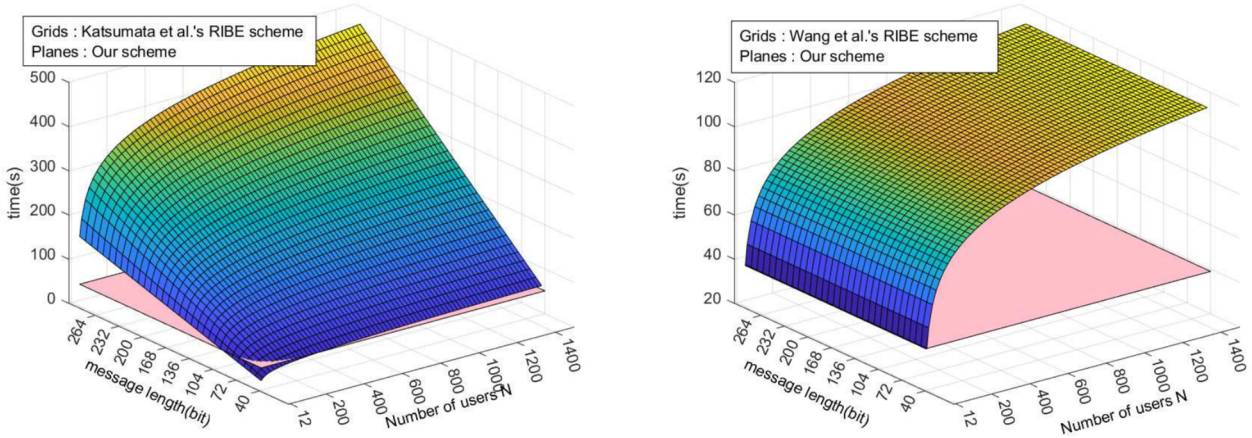
$\mathbf{Game}_5^{(b)}$: Except for the generation of challenge ciphertexts, the rest is same as $\mathrm{Game}_4^{(b)}$. Select $C_i \leftarrow \mathbb{Z}_q$ and $\mathbf{c}_0, c_{\mathrm{ID}}, \mathbf{c}'_{no}, \mathbf{c}''_t \leftarrow \mathbb{Z}_q^m$, where $i \in l$ and $no \in \mathrm{NRno}^*_{t^*}$.

Algorithm	TrapGen	SamplePre	SampleLeft
Time (ms)	32	166	194

Table 4. PPT polynomial algorithm.

Parameter n	16	32	64	128
Setup (ms)	22.73	68.10	141.77	732.55
GenSK (s)	1.08	7.14	16.84	69.09
GenDK (ms)	134.05	542.86	1547.01	3267.83
Offline.Enc (ms)	5.37	31.17	43.49	155.40
Online.Enc (ms)	0.01	0.02	0.02	0.04
Dec (ms)	0.10	0.37	0.27	1.11

Table 5. Time cost of each algorithm in our scheme, with encryption and decryption bit set to 1.



(a) Comparing with[21] (b) Comparing with[12]

Fig. 4. GenSK algorithm time cost.

By LWE assumption, we have $\mathbf{Game}_4^{(b)}$ and $\mathbf{Game}_5^{(b)}$ are computationally indistinguishable. The ciphertext doesn't rely on bit b, thus $\mathscr{A}$'s advantage becomes zero. □

Performance

Theoretical evaluation

From Table 2, we can get the comparison of RIBE schemes from the theoretical aspect. Additionally, our scheme is compared with other lattice-based RIBE schemes in Table 3, where T_{SL} represents the time cost of algorithm SampleLeft, $\alpha = O(logN)$, $\beta = O(r\log(N/r))$, and $\delta = O(N-r)$. The two parts that require computation by the KGC are maintained at a relatively small constant level in our scheme. Although the ciphertext size is large, by utilizing online-offline techniques, we can complete the majority of encryption operations during the offline phase.

Experimental evaluations

This section begins by presenting the outcomes of our implementation, followed by a comprehensive analysis of its performance. Our scheme is implemented on an Ubuntu laptop equipped with 16GB RAM and an AMD Ryzen7 6800HS CPU. We utilize the NTL library and C++ programming, and optimize it with multi-threaded parallel programming to improve its performance.

Our scheme's time cost is divided into matrix operations, algorithm TrapGen, SampleLeft and SamplePre. Table 4 presents the average running time for 10 runs of the these algorithm with parameters of n = 32, q=99991, and s = 4. Then, we evaluate the time cost of each function in the solution for increasing values of n, as shown in Table 5, with the encryption/decryption bit length set to 1 bit.

Setup algorithm time cost analysis Each binary tree node in[12] needs to be assigned a matrix, resulting in the public parameters PP involving $2N-1$ matrices. However, in our scheme, we no longer utilize binary trees but instead employ a number list as a replacement, so the size of the parameters has been reduced to N.

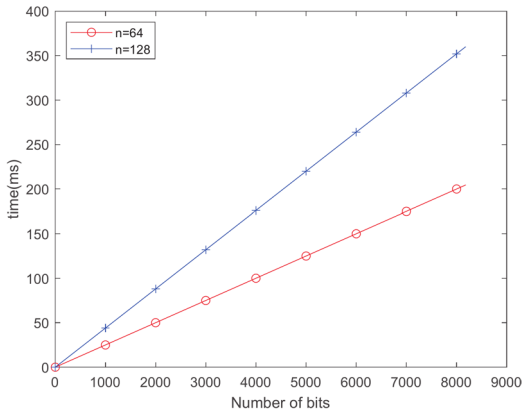


Fig. 5. Time cost of Online.Enc algorithm.

GenSK algorithm time cost analysis As depicted in Table 5, algorithm GenSK accounts for the most substantial temporal consumption within the entire scheme. This is primarily attributed to its iterative utilization of algorithm SampleLeft. Encouragingly, the Gram–Schmidt orthogonalization process in algorithm SampleLeft emerges as the most time-intensive phase, and its recurrence in each iteration compounds this cost. Therefore, by preprocessing the Gram–Schmidt orthogonalization, the time cost of algorithm GenSK significantly decreases, no longer being m times the runtime of algorithm SampleLeft for a single execution.

From Fig. 4a, we get that the time cost of GenSK in[22] shows different trends with the number of users and encryption bits. When the number of users remains constant and the encryption/decryption bit count increases, the time cost of[22] rises, whereas our scheme's time cost remains unchanged. Similarly, when the encryption/decryption bit count is fixed and the number of users grows, the time cost of[22] increases, while our scheme's time cost remains constant. Therefore, our solution maintains a constant and low time cost, irrespective of either the number of encrypted bits or users. This affirms the superiority of our revocation approach in handling large-scale users and encrypted data.

As shown in Fig. 4b, we compare the GenSK algorithm in[12]. Even though the plaintext bits number increases, the key generation overhead of the two schemes remains constant. However, when the user number increases, the key production overhead of[12] grows at a logarithmic level, and our scheme keeps it constant.

Encryption algorithm time cost analysis Table 5 represent the time cost of online encrypting one bit. From Fig. 5, it can be seen that the selection of parameter n has a significant impact on the encryption consumption time.

Conclusion

To enhance privacy protection and efficient member management, this paper proposes an integrated revocation model and constructs a lattice-based OO-IRIBE-EnDKER scheme. In our scheme, the periodic workload for KGC is maintained at a constant level, and the size of the secret key remains constant as well. Consequently, this scheme is particularly well-suited for scenarios involving high-workload KGCs and reduces storage requirements for system users. Furthermore, we demonstrate the correctness and prove the security of our scheme. Experimental results indicate that our scheme performs better than existing schemes. In future work, we aim to develop a lattice-based integrated revocation ABE scheme.

Data availability

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Code availability

The datasets used and/or analysed during the current study are available from the corresponding author on reasonable request.

Received: 3 January 2025; Accepted: 5 May 2025
Published online: 14 May 2025

References

1. Büyüközkan, G. & Göçer, F. Digital supply chain: Literature review and a proposed framework for future research. *Comput. Ind.* **97**, 157–177 (2018).
2. Peng, J., Chen, L. & Zhang, B. Transportation planning for sustainable supply chain network using big data technology. *Inf. Sci.* **609**, 781–798 (2022).
3. Shamir, A. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology: Proceedings of CRYPTO 84 4*, 47–53 (Springer, 1985).
4. Boldyreva, A., Goyal, V. & Kumar, V. Identity-based encryption with efficient revocation. In *Proceedings of the 15th ACM Conference on Computer and Communications Security*, 417–426 (2008).

5. Shi, Y., Zheng, Q., Liu, J. & Han, Z. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation. *Inf. Sci.* **295**, 221–231 (2015).
6. Ma, X. & Lin, D. Generic constructions of revocable identity-based encryption. In *Information Security and Cryptology: 15th International Conference, Inscrypt 2019, Nanjing, China, December 6–8, 2019, Revised Selected Papers 15*, 381–396 (Springer, 2020).
7. Emura, K., Seo, J. H. & Watanabe, Y. Efficient revocable identity-based encryption with short public parameters. *Theoret. Comput. Sci.* **863**, 127–155 (2021).
8. Seo, J. H. & Emura, K. Revocable identity-based encryption revisited: Security model and construction. In *Public-Key Cryptography–PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26–March 1, 2013. Proceedings 16*, 216–234 (Springer, 2013).
9. Emura, K., Takayasu, A. & Watanabe, Y. Adaptively secure revocable hierarchical IBE from k-linear assumption. *Des. Codes Crypt.* **89**, 1535–1574 (2021).
10. Xu, S., Yang, G. & Mu, Y. Revocable attribute-based encryption with decryption key exposure resistance and ciphertext delegation. *Inf. Sci.* **479**, 116–134 (2019).
11. Qin, B., Zhao, Q., Zheng, D. & Cui, H. (Dual) server-aided revocable attribute-based encryption with decryption key exposure resistance. *Inf. Sci.* **490**, 74–92 (2019).
12. Wang, Q., Huang, H., Li, J. & Yuan, Q. Revocable IBE with En-DKER from lattices: A novel approach for lattice basis delegation. In *European Symposium on Research in Computer Security*, 66–85 (Springer, 2023).
13. Boyen, X. & Waters, B. Anonymous hierarchical identity-based encryption (without random oracles). In *Advances in Cryptology-CRYPTO 2006: 26th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20–24, 2006. Proceedings 26*, 290–307 (Springer, 2006).
14. Yan, B. *et al.* Factoring integers with sublinear resources on a superconducting quantum processor. arXiv preprint arXiv:2212.12372 (2022).
15. Campbell, R., Diffie, W. & Robinson, C. Advancements in quantum computing and AI may impact PQC migration timelines. *preprints.org* (2024).
16. Tesoro, M., Siloi, I., Jaschke, D., Magnifico, G. & Montangero, S. Quantum inspired factorization up to 100-bit RSA number in polynomial time. arXiv preprint arXiv:2410.16355 (2024).
17. Priestley, B. & Wallden, P. A practically scalable approach to the closest vector problem for sieving via qaoa with fixed angles. arXiv preprint arXiv:2503.08403 (2025).
18. Shor, P. W. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 124–134 (IEEE, 1994).
19. Attrapadung, N. & Imai, H. Attribute-based encryption supporting direct/indirect revocation modes. In *Cryptography and Coding: 12th IMA International Conference, Cryptography and Coding 2009, Cirencester, UK, December 15–17, 2009. Proceedings 12*, 278–300 (Springer, 2009).
20. Qin, B., Deng, R. H., Li, Y. & Liu, S. Server-aided revocable identity-based encryption. In *Computer Security–ESORICS 2015: 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21–25, 2015, Proceedings, Part I 20*, 286–304 (Springer, 2015).
21. Chen, J., Lim, H. W., Ling, S., Wang, H. & Nguyen, K. Revocable identity-based encryption from lattices. In *Information Security and Privacy: 17th Australasian Conference, ACISP 2012, Wollongong, NSW, Australia, July 9–11, 2012. Proceedings 17*, 390–403 (Springer, 2012).
22. Katsumata, S., Matsuda, T. & Takayasu, A. Lattice-based revocable (hierarchical) IBE with decryption key exposure resistance. In *Public-Key Cryptography—PKC 2019: 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14–17, 2019, Proceedings, Part II 22*, 441–471 (Springer, 2019).
23. Agrawal, S., Boneh, D. & Boyen, X. Efficient lattice (h) IBE in the standard model. In *Eurocrypt*, Vol. 6110, 553–572 (Springer, 2010).
24. Zhang, Y., Liu, X. & Hu, Y. Simplified server-aided revocable identity-based encryption from lattices. In *Provable and Practical Security: 16th International Conference, ProvSec 2022, Nanjing, China, November 11–12, 2022, Proceedings*, 71–87 (Springer, 2022).
25. Wang, S., Zhang, J., He, J., Wang, H. & Li, C. Simplified revocable hierarchical identity-based encryption from lattices. In *Cryptology and Network Security: 18th International Conference, CANS 2019, Fuzhou, China, October 25–27, 2019, Proceedings 18*, 99–119 (Springer, 2019).
26. Takayasu, A. & Watanabe, Y. Lattice-based revocable identity-based encryption with bounded decryption key exposure resistance. In *Information Security and Privacy: 22nd Australasian Conference, ACISP 2017, Auckland, New Zealand, July 3–5, 2017, Proceedings, Part I 22*, 184–204 (Springer, 2017).
27. Takayasu, A. & Watanabe, Y. Revocable identity-based encryption with bounded decryption key exposure resistance: Lattice-based construction and more. *Theoret. Comput. Sci.* **849**, 64–98 (2021).
28. Guo, Y., Lu, Z., Ge, H. & Li, J. Revocable blockchain-aided attribute-based encryption with escrow-free in cloud storage. *IEEE Trans. Comput.* **72**, 1901–1912 (2023).
29. Li, J., Yao, W., Han, J., Zhang, Y. & Shen, J. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage. *IEEE Syst. J.* **12**, 1767–1777 (2017).
30. Chen, S., Li, J., Zhang, Y. & Han, J. Efficient revocable attribute-based encryption with verifiable data integrity. *IEEE Internet Things J.* **11**, 10441–10451 (2023).
31. Guo, F., Mu, Y. & Chen, Z. Identity-based online/offline encryption. In *Financial Cryptography and Data Security: 12th International Conference, FC 2008, Cozumel, Mexico, January 28–31, 2008. Revised Selected Papers 12*, 247–261 (Springer, 2008).
32. Liu, J. K. & Zhou, J. An efficient identity-based online/offline encryption scheme. In *International Conference on Applied Cryptography and Network Security*, 156–167 (Springer, 2009).
33. Lai, J., Mu, Y., Guo, F. & Susilo, W. Improved identity-based online/offline encryption. In *Information Security and Privacy: 20th Australasian Conference, ACISP 2015, Brisbane, QLD, Australia, June 29–July 1, 2015, Proceedings 20*, 160–173 (Springer, 2015).
34. Cui, J., Zhou, H., Xu, Y. & Zhong, H. Ooabks: Online/offline attribute-based encryption for keyword search in mobile cloud. *Inf. Sci.* **489**, 63–77 (2019).
35. Zuo, B., Li, J., Zhang, Y. & Shen, J. Identity-based online/offline encryption scheme from LWE. *Information* **15**, 539 (2024).
36. Mondal, P., Chamani, J. G., Demertzis, I. & Papadopoulos, D. $\{$I/O-Efficient$\}$ dynamic searchable encryption meets forward & backward privacy. In *33rd USENIX Security Symposium (USENIX Security 24)*, 2527–2544 (2024).
37. Sahai, A., Seyalioglu, H. & Waters, B. Dynamic credentials and ciphertext delegation for attribute-based encryption. In *Advances in Cryptology–CRYPTO 2012: 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2012. Proceedings*, 199–217 (Springer, 2012).
38. Naor, D., Naor, M. & Lotspiech, J. Revocation and tracing schemes for stateless receivers. In *Advances in Cryptology-CRYPTO 2001: 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19–23, 2001 Proceedings 21*, 41–62 (Springer, 2001).
39. 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*, 197–206 (2008).
40. Micciancio, D. & Peikert, C. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Eurocrypt*, Vol. 7237, 700–718 (Springer, 2012).

41. Ajtai, M. Generating hard instances of the short basis problem. In *Automata, Languages and Programming: 26th International Colloquium, ICALP'99 Prague, Czech Republic, July 11–15, 1999 Proceedings 26*, 1–9 (Springer, 1999).
42. Alwen, J. & Peikert, C. Generating shorter bases for hard random lattices. *Theory Comput. Syst.* **48**, 535–553 (2011).
43. Regev, O. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM* **56**, 1–40 (2009).
44. Asharov, G. *et al.* Multiparty computation with low communication, computation and interaction via threshold FHE. In *Advances in Cryptology—EUROCRYPT 2012: 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15–19, 2012. Proceedings 31*, 483–501 (Springer, 2012).
45. Zhang, Y., Liu, X., Hu, Y. & Jia, H. Cloud-aided scalable revocable IBE with ciphertext update from lattices in the random oracle model. In *International Conference on Frontiers in Cyber Security*, 387–403 (Springer, 2023).

Author contributions

Haodong Huang Writing—original draft, Methodology, Software, Validation. Juyan Li Writing—review and editing, Methodology, Supervision. Shujun Bi Writing—review and editing, Methodology, Supervision. Qi Yuan Writing—review and editing, Methodology, Supervision, Funding acquisition.

Funding

This work was supported by the Heilongjiang Provincial Natural Science Foundation of China (LH2020F050); Fundamental Research Funds Heilongjiang Provincial Universities (145309213).

Declarations

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Additional information

Correspondence and requests for materials should be addressed to S.B.