Hindawi
Security and Communication Networks
Volume 2022, Article ID 7494452, 12 pages
https://doi.org/10.1155/2022/7494452

Research Article

Generic Construction of Forward-Secure Revocable Identity-Based Signature and Lattice-Based Instantiations

Yan He,[1] Baodong Qin,[1,2] Wen Gao,[1] Dong Zheng,[1,3] and Qianqian Zhao[4]

[1]*School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China*
[2]*Science and Technology on Communication Security Laboratory, Chengdu 610041, China*
[3]*Westone Cryptologic Research Center, Beijing 100166, China*
[4]*Shanghai Research and Development Center for Micro-Nano Electronics, Shanghai 201210, China*

Correspondence should be addressed to Baodong Qin; qinbaodong@xupt.edu.cn

Received 6 May 2022; Revised 20 October 2022; Accepted 27 October 2022; Published 16 November 2022

Academic Editor: Barbara Masucci

Forward-secure revocation is a powerful cryptographic technique to alleviate key exposure attacks on identity-based cryptosystems. In recent years, quantum computers have made some breakthroughs, so in the foreseeable future, existing cryptographic systems will be subject to quantum attacks. However, known forward-secure revocable identity-based signature (FS-RIBS) schemes were designed over bilinear pairing groups and may suffer from quantum computing attacks. To address this issue, this paper proposes a generic method to construct FS-RIBS schemes, taking (hierarchical) IBS schemes as a basic component. By instantiating it with some post-quantum (hierarchical) IBS schemes, e.g., lattice-based (hierarchical) IBS, we immediately obtain six FS-RIBS schemes under the hardness of the small integer solution problem, which is secure against quantum computing attacks.

1. Introduction

In 1984, Adi [1] first introduced an identity-based mechanism. The core idea is to use the user's identity as a public key for encryption or a public key for verifying signatures and give the first identity-based signature (IBS). Compared with PKI, it does not need to issue public key certificates and other related complex steps, which improves efficiency. However, it was not until 2001 that Boneh [2] proposed an identity-based encryption scheme for the first time. Boneh's [2] revocable mechanism has huge computational overhead. To reduce the runtime of revocable user computations, Ge and Wei [3] proposed a binary tree method in 2008 with a logarithmic increase in computational cost. However, it cannot resist key exposure attacks.

In 2013, Seo and Emura [4] proposed a stronger definition and security model of RIBE (revocable identity-based encryption), which can resist decryption key exposure attacks. In 2014, they [5] also gave a new security definition of RIBS (revocable identity-based signature) scheme that can resist signing key exposure attacks and introduced a scalable RIBS scheme. In 2013, Tsai et al. [6] proposed a bilinear pair-based RIBS scheme under the standard model. All RIBS schemes before Tsai were constructed by the random oracle model. All subsequent RIBS schemes [7, 8] refer to Tasi's security model and definition, where scheme [8] achieves the SU-CMA security under the standard model. However, the previous RIBS schemes cannot guarantee both efficient revocation and strong unforgeability simultaneously. In 2016, Liu et al. [9] proposed a strong unforgeable RIBS scheme that solves the above problems in the standard model. However, these RIBS schemes [6–8] cannot resist signing key exposure attacks. In 2018, Yang et al. [10] performed some optimizations based on [8]. Zhao et al. [11] also proposed an efficient communication scheme based on multi-linear mapping in 2019. With the imminent advent of quantum computers, the need for cryptographic schemes to resist quantum attacks is increasingly urgent. In 2015, Xiang [12] introduced the first lattice-based RIBS scheme using a complete subtree structure, which can prevent signing key

exposure but requires a secret channel. In 2020, Xie et al. [13] proposed the RIBS scheme under the standard model on the lattice. Later in the same year, Xie et al. [14] proposed a scheme that can resist the exposure of the signature key. As recently as 2022, Xie et al. [15] proposed a fully homomorphic RIBS (RIBFHS) scheme, which is homomorphic and is the first RIBFHS scheme that considers signature key exposure on lattices. However, its security only is sID-EU-CMA and forward security cannot be guaranteed.

Furthermore, forward security has also become a hot research topic. Its original intention is to ensure that the adversary cannot decrypt the ciphertext of the user's last period or forge the signature of the previous period after the private key of the current period is leaked. At present, few works research on the forward security of revocable signatures; only Wei et al. [16] studied forward security of revocable IBS. However, their construction security is based on traditional difficult problems and cannot resist quantum attacks. Qin et al. [17] proposed the general structure of revocable forward security encryption in 2021. Its main idea combines a node selection algorithm and identity-based hierarchical encryption. As far as we know, there is no revocable forward-secure identity-based signature scheme on the lattice. So, in this work, we propose a generic method to construct a forward-secure revocable identity-based signature (FS-RIBS) and introduce two methods to improve its verification efficiency.

1.1. Our Contributions. This article is mainly inspired by Qin et al.'s work [17]. In this work, we research on FS-RIBS and its instantiations on lattices. In a FS-RIBS system (see Figure 1), we split each user's private key into two parts: the first part is the secret key held by the user for a long time, and the second part is the signing key that is only available to sign messages signed within t time period. Any user's "long-term" (this long-term secret key is not immutable, and it evolves once in each time period) secret key is also closely related to the time period and will change with the time period, while the verification key does not change. At the start of all time periods, KGC publishes the update key on the public channel to ensure that users who have not been revoked can sign typically.

(i) Firstly, we introduce the formal definition and security model for the FS-RIBS system. The system captures signing key exposure resistance, forward security, and user revocation.

(ii) Secondly, we give a generic construction of the FS-RIBS scheme. A forward-secure RIBS scheme is built on a hierarchical IBS scheme and a standard IBS scheme. The HIBS scheme was used to obtain the signing key of the user's initial time period, and this initial signature key can deduce the signature key of the following time period. Then, a time-based update key is generated through IBS and a complete binary tree.

(iii) Thirdly, we further make two improvements to our proposed generic construction; although it will increase some signature overhead, both improvements can greatly improve the efficiency of verifying signatures and have tight security.

(iv) Finally, an instance of our generic construction on the lattice is given, which is secure against signing key exposure (SKE) attacks and is forward secure, and has scalability, as in the generic construction. We also present a comparison of our example with other related RIBS schemes, including classical and recent schemes, both bilinear map-based and lattice-based.

1.2. Related Work

1.2.1. Revocable Identity-Based Signature Schemes. The user's revocable mechanism is a basic requirement for identity-based signatures. Boneh [2] mentioned for the first time that KGC generates a private key for each user who has not been revoked by cascading the user's identity and time. Because the identity of each user is unique, this scheme has met forward security. However, this scheme does not have good scalability because the complexity of updating the key is $O(N - R)$, and time complexity increases with $N - R$. N refers to the total number of users, and R is the number of revoked users. Subsequently, Ge and Wei [3] introduced a structure that can reduce the size of the update key and reduced the update key size to $O(R\log(N/R))$. Subsequently, some works [6, 8] proposed new RIBS schemes. In 2014, Seo and Emura [5] proposed a new security model of RIBS, which can resist signing key exposure attacks and introduced a scalable RIBS scheme. All the following works [17, 18] are based on the improvement of the security model of the scheme [5], either increasing security or improving efficiency. In 2017, Wei et al. [16] proposed a scheme that can resist the exposure of signature keys and ensure forward security. However, all the above solutions are not resistant to quantum attacks. To resist quantum attacks, Xiang [12] proposed a lattice-based RIBS scheme in 2015, but its cancellation operation requires a secure channel. Subsequently, Wei et al. [16] introduced a RIBS scheme based on the NTRU lattice that the update key can be updated on the open channel. In the next few years, Xie et al. [13–15] proposed some RIBS schemes. These schemes all improve the security of the scheme in some cases. However, none of the above schemes can guarantee forward security. For now, there is no RIBS scheme on the lattice that can guarantee forward security and resist signature key exposure attacks.

1.2.2. Forward-Secure Signature Scheme. For forward security (FS), Anderson [19] firstly proposed the idea of forward-secure signature in 1997. Later, Bellare and Miner proposed a more efficient scheme [20] based on [19] and gave the formal definition and security model of forward security signature. More forward-secure digital signature algorithms [21, 22] have been proposed. However, there is little research on identity-based forward-secure digital signature algorithm. In 2008, Liu et al. introduced the first FS-IBS scheme in [23]. Zhang et al. [18] gave the first FS-IBS

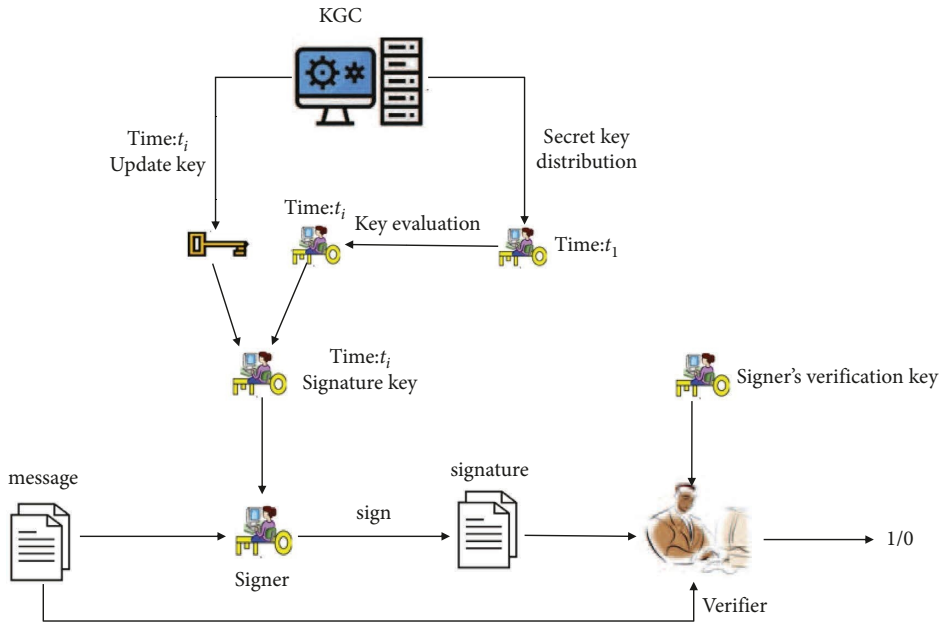

Figure 1: FS-RIBS system.

scheme in 2014. In 2021, Wu and Huang [24] further proposed an efficient forward security algorithm on the lattice, which has stronger security. But there is no revocable mechanism, it and cannot resist key exposure attacks. To the best of our knowledge, Wei et al. [16] first studied FS-RIBS and gave a construction. But, it is not resistant to quantum attacks. Qin et al. [17] proposed the general structure of revocable forward security for encryption in 2021. Its main idea combines a node selection algorithm and identity-based hierarchical encryption.

2. Preliminary

Notations. We use "$U|V$" to represent a concatenation of two elements U and V, which can be binary strings, matrices, etc. We use "t" to represent a time period in binary form. We denote sets with capital italic, e.g., U and V. Security parameter is λ. **mpk** means master public key, and **msk** means master secret key. The revocation list is represented by **RL**. A complete binary tree is represented by **BT**.

2.1. The Algorithm of Node Selection. In order to prevent the time complexity of revoking users from increasing linearly, our revocation scheme adopts a node selection algorithm. The core idea of the algorithm is to use a complete binary tree to find the fewest nodes required to cover all non-revoked users. In this tree, each leaf node has a one-to-one correspondence with an identity. The set of all nodes on the path from the root node of the user **ID** to the leaf node is represented by Path (**ID**). x_l and x_r are used to represent the left and right child nodes of node x. This algorithm $\mathbf{KUN}(\mathbf{BT}, \mathbf{RL}, t)$ will input **RL**, a binary tree **BT**, and t time period. The algorithm has the following four steps:

(1) Let sets U and V be empty sets.

(2) $\forall(\mathbf{ID}_i, t_i) \in \mathbf{RL}$, if $t_i \le t$, add $(\mathbf{ID}_i)$ to U.

(3) $\forall x \in U$, if $x_l \notin U$, then addend x_l to V; if $x_r \notin U$, then addend x_r to V.

(4) If $\mathbf{RL} \notin \varnothing$, return V; else return the root node.

Figures 2 and 3 give a simple example of this algorithm, in which Figure 2 shows that no user has been revoked, and Figure 3 shows that the user with $\mathbf{I\ D} = 3$ has been revoked.

2.2. Definition of (H)IBS. In this section, we introduce the formal definition of (H)IBS constructions. First, we give the definition of IBS, which can easily be extended to HIBS. There are 4 PPT algorithms in an IBS system:

(i) **Setup** $(\lambda, l_{\mathrm{id}})$: on input λ and identity length l_{id}, output **mpk** and **msk.**

(ii) **Extract** (**mpk**, **msk**, **ID**): on input (**mpk, msk**) and an arbitrary identity $\mathbf{I\ D}$, it outputs the user's secret key $\mathrm{usk}_{\mathbf{I\ D}}$, associated with $\mathbf{I\ D}$.

(iii) **Sign** $(M, \mathbf{I\ D}, \mathrm{usk}_{\mathbf{I\ D}})$: on input a message $M \in \mathcal{M}$, $\mathbf{I\ D}$ and $\mathrm{usk}_{\mathbf{I\ D}}$. A signature σ is returned.

(iv) **Verify** $(\mathrm{mpk}, M, \mathbf{I\ D}, \sigma)$: on input **mpk**, M, $\mathbf{I\ D}$, and σ, it returns 0 if σ is invalid and 1 otherwise.

Essentially, the HIBS scheme only has one more feature than the IBS scheme, which is the feature of hierarchy, that is, the user of the parent node can deduce the key of the user of its child node, but the user of the leaf node cannot deduce the key of the parent node. However, there is no connection between the users of the IBS scheme. So, we just need to add a **Derive** algorithm to the IBS scheme. Let the maximum depth of our HIBS system be d; set a user $\mathbf{I\ D} = (\mathbf{ID}_1, \ldots, \mathbf{ID}_k)$, and the signature private key is $\mathrm{usk}_{\mathbf{I\ D}}$, where $k \le d$. The **Derive** algorithm inputs **ID** and $\mathrm{usk}_{\mathbf{I\ D}}$ and obtains the key $\mathrm{usk}_{\mathbf{I\ D}|r}$ of the following hierarchy where r is 0 or 1. Through iteration, the

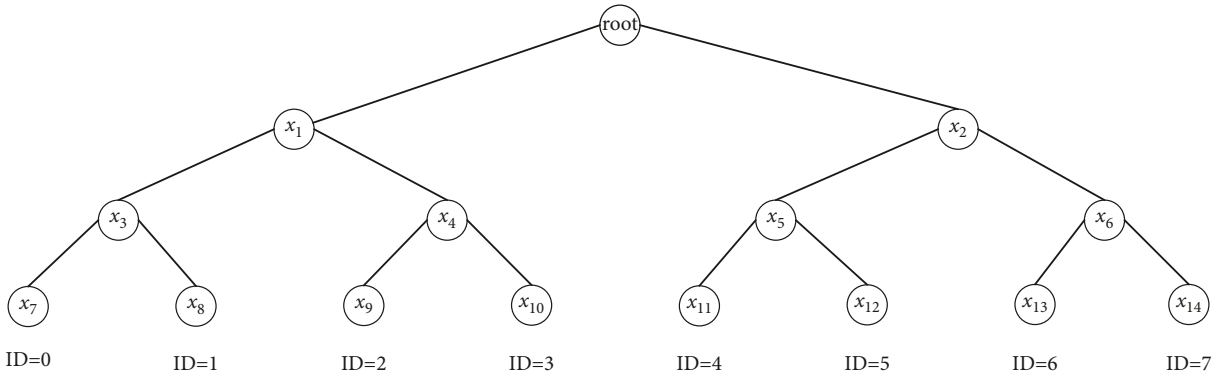

Figure 2: No user is revoked: $U = \varnothing$ and $V = \{\text{root}\}$.

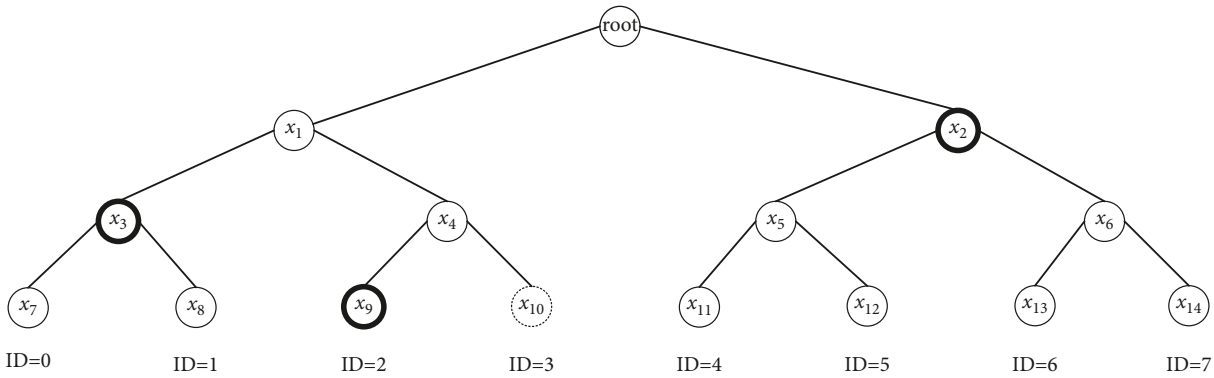

Figure 3: **ID** = 3 is revoked: $U = \{\text{root}, x_1, x_4, x_{10}\}$ and $V = \{x_2, x_3, x_9\}$.

user **ID** can get keys of all users whose depth is up to d and prefixed with **ID**. When $d = 1$, it is the IBS scheme.

Next, we give the security model of the (H)IBS scheme. Strong unforgeability under adaptive chosen message attack (SU-CMA) is the required security for our HIBS and IBS schemes. We set the maximum hierarchy depth of our HIBS scheme to be d (IBS is the case of $d = 1$). It formally defines the game between adversary $\mathcal{A}$ and challenger $\mathcal{C}$.

(1) **Setup:** $\mathcal{C}$ gets (**mpk, msk**) by running **Setup**$(\lambda, l_{\text{id}}, d)$ and sends **mpk** to adversary $\mathcal{A}$.

(2) **Phase 1:** $\mathcal{A}$ adaptively makes a polynomial number of the following queries:

(i) **Create key**: for any identity $\mathbf{ID}_{|1} = (\mathbf{ID}_1)$ at depth 1, the challenge runs $\text{usk}_{\mathbf{ID}_{|1}} \leftarrow$ **Extract** (**mpk, msk**, $\mathbf{ID}_1$). It adds $(\mathbf{ID}_{|1}, 1, \text{usk}_{\mathbf{ID}_{|1}})$ to a key list *KL*.

(ii) **Secret key**: $\mathcal{A}$ can query a secret key for an identity $\mathbf{ID}_{|k} = (\mathbf{ID}_1, \ldots, \mathbf{ID}_k)$ where $k \le d$. $\mathcal{C}$ first checks whether the key list has a secret key $\text{usk}_{\mathbf{ID}_{|i}}$ for identity $\mathbf{ID}_{|i}$ which is a prefix of identity $\mathbf{ID}_{|k}$. If so, $\mathcal{C}$ runs $\text{usk}_{\mathbf{ID}_{|k}} \leftarrow$ **Derive**$(\text{usk}_{\mathbf{ID}_{|i}}, \mathbf{ID}_{|k})$ and returns to $\mathcal{A}$ the secret key $\text{usk}_{\mathbf{ID}_{|k}}$. If no such tuple, $\mathcal{C}$ returns $\perp$. If $i = k$, $\mathcal{C}$ sends $\text{usk}_{\mathbf{ID}_{|i}}$ to $\mathcal{A}$.

(iii) **Signature query:** $\mathcal{A}$ can adaptively query $\mathcal{C}$ for polynomial signatures. The identity and message of these signatures are arbitrary. Here, suppose $\mathcal{A}$ queries q times, the message set is $\{M_1, \ldots, M_q\}$, and the identity set is $\{\mathbf{ID}_1, \ldots, \mathbf{ID}_q\}$. Note that $\mathbf{ID}_i$ where $i = 1, 2, \ldots, q$ refers to the i-th identity. $\mathcal{C}$ calculates the signature of these messages by **Sign**$((M_i, \mathbf{ID}_i, \text{usk}_{\mathbf{ID}_i})$ where $i = 1, 2, \ldots, q$ to form a set $\{(M_1, \sigma_{\mathbf{ID}_1}^{M_1}), \ldots, (M_q, \sigma_{\mathbf{ID}_q}^{M_q})\}$ and returns the set to $\mathcal{A}$.

(4) **Forgery:** the adversary $\mathcal{A}$ forges a signature $\sigma_{\mathbf{ID}^*}^{M^*}$ of M^*. $\mathcal{A}$ will succeed if the following three conditions hold:

(1) **Verify** $(\mathbf{mpk}, \mathbf{ID}^*, M^*, \sigma_{\mathbf{ID}^*}^{M^*})) = 1$.

(2) $\mathbf{ID}^*$ or its any prefix cannot be queried during the secret key query phase.

(3) $(M^*, \sigma_{\mathbf{ID}^*}^{M^*})$ cannot be queried during the signature query phase.

The advantage of $\mathcal{A}$ in the above game is defined as $\text{Adv}_{(H)\text{IBS},\mathcal{A}}^{\text{SU-CMA}}(\lambda) = \Pr[\mathcal{A} \text{ succeeds}]$.

Definition 1. For any PPT adversary $\mathcal{A}$, if the above advantage of $\mathcal{A}$ is negligible in λ, then the (H)IBS is SU-CMA secure.

Multi-Identity Security. In the forgery stage, multiple identities can be submitted, and as long as one is successfully

verified, the adversary is won. We assume there are n identities. By a hybrid argument, we can prove that the advantage of $\mathcal{A}$ to forge a signature successfully is no more than $n \cdot \mathrm{Adv}^{\mathrm{SU-CMA}}_{(H)\mathrm{IBS},\mathcal{A}}(\lambda)$.

3. Definition of FS-RIBS Scheme

3.1. Syntax of FS-RIBS Scheme. A forward-secure revocable identity-based signature (FS-RIBS) is made up of the following 8 algorithms:

(i) (**mpk, msk, ST, RL**) ←**Setup**($(\lambda, l_{\mathrm{id}}, l_{\mathrm{time}})$: λ is the security parameter of the algorithm, $\{0,1\}^{l_{\mathrm{id}}}$ represents the user's identity space, and the algorithm has $2^{l_{\mathrm{time}}}$ time periods. This algorithm inputs λ, l_{id}, and l_{time} and outputs (**mpk**, **msk**) and two empty sets **ST** and **RL.**

(ii) $\mathrm{sk}^{(t_1)}_{\mathbf{ID}}$←**KeyGen** (**mpk, msk, ID, ST**): the algorithm generates a secret key for the newly added user **ID**∈ $\{0,1\}^{l_{\mathrm{id}}}$ and then outputs a secret key $\mathrm{sk}^{(t_1)}_{\mathbf{ID}}$ that can be evolved in initial time period $t_1 \doteq 0\ l_{\mathrm{time}}$ 1.

(iii) $\mathrm{sk}^{(t)}_{\mathbf{ID}}$←**SKEval** (**mpk**, $sk^{(t-1)}_{\mathbf{ID}}, t$): this algorithm outputs the secret key $\mathrm{sk}^{(t)}_{\mathbf{ID}}$ of the current time period t from the secret key $\mathrm{sk}^{(t-1)}_{\mathbf{ID}}$ of the previous time period t-1 through evolution.

(iv) uk_t←**SKUpdate** (**mpk, msk, RL, ST**, t): the algorithm outputs the update key uk_t within time period $t \in \{0,1\}^{l_{time}}$.

(v) Sign$k_{\mathbf{ID},t}$←**SKGen** $(\mathrm{sk}^{(t)}_{\mathbf{ID}}, uk_t)$: in time period t, this algorithm inputs update key uk_t and user **ID** secret key $\mathrm{sk}^{(t)}_{\mathbf{ID}}$ and returns a signing key Sign$k_{\mathbf{ID},t}$ within time period t.

(vi) $\sigma_{\mathbf{ID},t}$←**Sign** (Sign$k_{\mathbf{ID},t}, t$, **ID**, M): on input a message $M \in \mathcal{M}$, the algorithm signs it within the time period t, identity **ID**, and signing key Sign $k_{\mathbf{ID},t}$ and outputs a signature $\sigma_{\mathbf{ID},t}$.

(vii) 1/0 ←**Verify** (**mpk**, M, t, **ID**, $\sigma_{\mathbf{ID},t}$): this algorithm verifies the signature $\sigma_{\mathbf{ID},t}$ and outputs 0 if $\sigma_{\mathbf{ID},t}$ is an invalid signature, and 1 otherwise.

(viii) **RL**←**Revoke** (**RL, ID**, t): suppose that the input identity **ID** is not a non-revoked user at time period t; then, (**ID**, t) is added to **RL** by key authority, and it outputs new **RL.**

Correctness. An FS-RIBS needs to meet correctness as follows. For any message M and identity **ID**, if the user is not revoked at time period t, then for **(mpk, msk, ST, RL)**← **Setup** $(\lambda, l_{\mathrm{id}}, l_{\mathrm{time}})$, $\mathrm{sk}^{(t_1)}_{\mathbf{ID}}$←**KeyGen (mpk, msk, ID, ST)**, $\mathrm{sk}^{(t)}_{\mathbf{ID}}$←**SKEval** (**mpk**, $sk^{(t-1)}_{\mathbf{ID}}, t$), uk_t←**SKUpdate** (**mpk, msk, ST, RL,**t), Sign $k_{\mathbf{ID},t}$←**SKGen** $(\mathrm{sk}^{(t)}_{\mathbf{ID}}, \mathrm{uk}_t)$, and $\sigma_{\mathbf{ID},t}$←**Sign**(Sign $k_{\mathbf{ID},t}$, **ID**, t, M), **Verify** (**mpk**, M, t, **ID**, $\sigma_{\mathbf{ID},t}$) = 1 holds with overwhelming probability.

3.2. Attacker Model. We refer to [25–27] and give what capabilities the attacker is allowed to have in our scheme combined with the actual situation. Attackers are divided into two different types:

(1) T1 adversary is able to query $\mathrm{sk}^{(t)}_{\mathbf{ID}^*}$ of $\mathbf{ID}^*$ within time period $t \le t^*$. Thus, the user $\mathbf{ID}^*$ must have been revoked before t^* time period.

(2) T2 adversary does not do the above query. However, it is allowed to query a signing key within any $t \ne t^*$ and can query the secret key of $\mathbf{ID}^*$ after time period t^*.

Both adversaries are allowed to obtain all public parameters of the system.

3.3. Security Definition of FS-RIBS Scheme. Next, we give a security definition of FS-RIBS, which is resistant to signing key exposure and can guarantee forward security. The FS-RIBS scheme is SU-CMA secure.

Definition 2. (SU-CMA). The SU-CMA security of FS-RIBS is defined by the following experiment played between a challenger $\mathcal{C}$ and a PPT adversary $\mathcal{A}$.

(1) **Setup:**$\mathcal{C}$ gets **mpk**, **msk**, **RL**, and a state **ST** by running **Setup** $(\lambda, l_{\mathrm{id}}, l_{\mathrm{time}})$. **mpk** is sent by $\mathcal{C}$ to $\mathcal{A}$. Then, $\mathcal{A}$sends$\mathcal{C}$that he wants to challenge$\mathbf{ID}^*$and challenge time periodt^*.

(2) **Query phase:**$\mathcal{A}$ is allowed to make adaptive polynomial queries to $\mathcal{C}$ as follows:

(i) Create key query : if $\mathcal{A}$ queries the identity $\mathbf{ID} \in \{0,1\}^{l_{\mathrm{id}}}$ and creates key in time period $t \in \{0,1\}^{l_{\mathrm{time}}}$, firstly, $\mathcal{C}$ judges whether t is the initial time period of the **ID**. If $\mathcal{C}$ finds this to be the case, then it gets an initial secret key $\mathrm{sk}^{(t)}_{\mathbf{ID}}$ by running **KeyGen** (**mpk, msk, ID, ST**). Next, it adds triple (**ID**, t, $\mathrm{sk}^{(t)}_{\mathbf{ID}}$) to the secret key list **SKL**. Otherwise, $\mathcal{C}$ queries in **SKL** whether there exists a triple (**ID**, $sk^{(t)}_{\mathbf{ID}}, t'$) satisfying $t' < t$. If this is the case, it iteratively runs **SKEval** (**mpk**, $\mathrm{sk}^{(t)}_{\mathbf{ID}}, t' + 1$) until **SKEval** (**mpk**, $\mathrm{sk}^{(t-1)}_{\mathbf{ID}}, t$), gets secret key $\mathrm{sk}^{(t)}_{\mathbf{ID}}$ in time period t, and updates the triple (**ID**, $\mathrm{sk}^{(t)}_{\mathbf{ID}}$, t') with (**ID**, $\mathrm{sk}^{(t)}_{\mathbf{ID}}$, t). If this is not the case, $\mathcal{C}$ returns $\perp$ to $\mathcal{A}$.

(ii) Secret key query: if $\mathcal{A}$ wants to query the secret key with $\mathbf{ID} \in \{0,1\}^{l_{\mathrm{id}}}$ in $t \in \{0,1\}^{l_{\mathrm{time}}}$, $\mathcal{C}$ searches the **SKL** for triple (**ID**, t, $\mathrm{sk}^{(t)}_{\mathbf{ID}}$). If it searched such triple, $\mathcal{C}$ sends $\mathrm{sk}^{(t)}_{\mathbf{ID}}$ to $\mathcal{A}$; otherwise, it sends $\perp$ to $\mathcal{A}$.

(iii) Update key query: if $\mathcal{A}$ sends $\mathcal{C}$ a query for the update key at t time period, $\mathcal{C}$ gets uk_t and sends it to $\mathcal{A}$ by running **SKUpdate** (**mpk, msk, ST, RL,**t).

(iv) Signing key query: if $\mathcal{A}$ does a signing key query for **ID** within the time period t, firstly, $\mathcal{C}$

searches the **SKL** for the triple (**ID**, $t\prime$, $\mathrm{sk}_{\mathbf{ID}}^{(t)}$) satisfying $t \geq t\prime$. If it does not search such triple, $\mathscr{C}$ responds $\perp$. On the contrary, $\mathscr{C}$ evolves $sk_{\mathbf{ID}}^{(t')}$ from time period t' to t by iterative running **SKEval** (**mpk**, $sk_{\mathbf{ID}}^{(t')}$, $t' + 1$) until **SKEval** (**mpk**, $\mathrm{sk}_{\mathbf{ID}}^{(t-1)}$, t) and gets the signing key $\mathrm{sk}_{\mathbf{ID}}^{(t)}$ by running algorithm **SKGen** ($\mathrm{sk}_{\mathbf{ID}}^{(t)}$, uk_t). $\mathscr{C}$ returns $\mathrm{sk}_{\mathbf{ID}}^{(t)}$ to $\mathscr{A}$.

(v) Revocation query: $\mathscr{C}$ returns **RL** to $\mathscr{A}$ if it receives $\mathscr{A}$'s request to query the revocation list for time period t.

(vi) Signature query: $\mathscr{A}$ can adaptively query $\mathscr{C}$ for polynomial signatures. The identity, time period, and the message of these signatures are arbitrary. Here, suppose $\mathscr{A}$ queries q times; the message set is $\{M_1, \ldots, M_q\}$, the time period set is $\{t_1, \ldots, t_q\}$, and the identity set is $\{\mathbf{ID}_1, \ldots, \mathbf{ID}_q\}$. $\mathscr{C}$ calculates the signature of these messages by **Sign** ($(\mathrm{Sign}\, k_{\mathbf{ID}_i,t_i}, \mathbf{ID}_i, t_i, M_i)$ where $i = 1, 2, \ldots, q$ to form a set $\{(M_1, \sigma_{\mathbf{ID}_1,t_1}^{M_1}), \ldots, (M_q, \sigma_{\mathbf{ID}_1,t_q}^{M_q})\}$ and returns the set to $\mathscr{A}$.

The above query has the following restrictions:

(i) $\mathscr{A}$ cannot query the signing key whose $\mathbf{ID}^*$ is within time period t^*.

(ii) $\mathscr{A}$ can query the secret key of $\mathbf{ID}^*$ in time period $t < t^*$, provided that $\mathbf{ID}^*$ must be revoked before time period t^*.

(iii) If the identity $\mathbf{ID}_i$ is not a non-revoked user within time period t_i, return $\sigma_{\mathbf{ID}_i,t_i}^{M_1} = \perp$ to $\mathscr{A}$.

(3) **Forgery:** the adversary $\mathscr{A}$ forged a signature $\sigma_{\mathbf{ID}^*,t^*}^{M^*}$ of M^*. The adversary can win the game unless $(M^*, \sigma_{\mathbf{ID}^*,t^*}^{M^*}) \notin \{(M_1, \sigma_{\mathbf{ID}_1,t_1}^{M_1}), \ldots, (M_q, \sigma_{\mathbf{ID}_1,t_q}^{M_q})\}$ and **Verify**(**mpk**, $(\mathbf{mpk}, M^*, t^*, \mathbf{ID}^*, \sigma_{\mathbf{ID}^*,t^*}^{M^*}) = 1$, $\mathbf{ID}^*, \sigma_{\mathbf{ID}^*,t^*}^{M^*}) = 1$.

In the above experiment, the probability of $\mathscr{A}$ successfully forging a verified signature is defined as

$$\mathrm{Adv}_{\mathrm{FS-RIBS},\mathscr{A}}^{\mathrm{SU-CMA}}(\lambda). \tag{1}$$

For any PPT adversary $\mathscr{A}$, if $\mathrm{Adv}_{\mathrm{FS-RIBS},\mathscr{A}}^{\mathrm{SU-CMA}}(\lambda)$ is negligible in λ, then the FS-RIBS scheme is SU-CMA secure.

4. Our Generic Construction

The two fundamental schemes in our generic construction are HIBS and IBS. HIBS consists of five algorithms, **HIBS.Setup, HIBS.Extract, HIBS.Derive, HIBS.Sign,** and **HIBS.Verify** and its maximum depth is $l_{\mathrm{time}} + 1$. The IBS is composed of 4 algorithms: **IBS.Setup, IBS.Extract, IBS.-Sign,** and **IBS.Verify**. We let the message spaces of our HIBS and IBS schemes be $\mathscr{M}$ for both. As described in Construction 1, we construct a FS-RIBS scheme consisting of eight algorithms: **RIBS.Setup, RIBS.KeyGen, RIBS.SKEval, RIBS.SKUpdate, RIBS.SKGen, RIBS.Sign, RIBS.Verify,** and **RIBS.Revoke**. Obviously, the message space of this scheme is $\mathscr{M}$, $\{0,1\}^{l_{\mathrm{id}}}$ is the identity space of this scheme, and $\{0,1\}^{l_{\mathrm{time}}}$ is the time period space of this scheme.

In the construction, the signature key of each user is related to a discrete time period. Specifically, it is necessary to cascade a certain time period T after each user **ID**, where $t \in T = \{0, 1, \ldots, 2^{l_{\mathrm{time}}} - 1\}$ is binary. In other words, when generating the signature key, the **ID** is concatenated with a certain time period T as the input identity, which will lead to each user **ID** having different signature keys in different time periods, which ensures its forward security. More specifically, a time period can be represented by the integer $t = E_1 E_2 \ldots E_{l_{\mathrm{time}}} \in \{0,1\}^{l_{\mathrm{time}}}$ of l_{time}-bit, arranged from the top of the tree to the bottom. For $t \in T$, a set of $l_{\mathrm{time}} + 1$ identities is represented by $J_t = \{J_{t,1}, J_{t,2}, \ldots, J_{t,l_{\mathrm{time}}+1}\}$ and $J_{t,c}$ is treated as an identity vector. For, $c = 1 \cdots l_{\mathrm{time}} + 1$:

$$J_{t,c} = \begin{cases} (E_1, E_2, \ldots, E_{c-1}, 1), & \text{if } E_c = 0 \text{ and } 1 \leq c \leq l_{\mathrm{time}}, \\ \perp, & \text{if } E_c = 1 \text{ and} 1 \leq c \leq l_{\mathrm{time}}, \\ (E_1, E_2, \ldots, E_{l_{\mathrm{time}}}), & \text{if } c = l_{\mathrm{time}} + 1. \end{cases} \tag{2}$$

We give an example as shown in Figure 4. In the figure, time $t = 0010$ and $|T| = 2^4$ time periods, and the set $J_2 = \{1, 01, \perp, 0011, 0010\}$.

4.1. Basic Construction

Construction 1 (Forward-Secure RIBS Scheme). Our generic construction of FS-RIBS scheme is detailed as follows

(i) (**mpk**, **msk**, **ST**, **RL**)←**RIBS.Setup** ($\lambda, l_{\mathrm{id}}, l_{\mathrm{time}}$): it runs **HIBS.Setup** ($\lambda, l_{\mathrm{time}} + 1$) and **IBS.Setup** ($\lambda, l_{time} + l_{i\,d}$) to obtain ($\mathbf{mpk}_1, \mathbf{msk}_1$) and ($\mathbf{mpk}_2, \mathbf{msk}_2$), respectively. It initializes **BT**, whose depth is l_{id}. All leaf nodes are closely related to an identity. Ultimately, it outputs $\mathbf{mpk} = (\mathbf{mpk}_1, \mathbf{mpk}_2)$, $\mathbf{msk} = (\mathbf{msk}_1, \mathbf{msk}_2)$, an empty revocation list **RL**, and **ST** = **BT.**

(ii) $\mathrm{sk}_{\mathbf{ID}}^{(t_1)}$← textbfRIBS.KeyGen (**mpk, msk, ID, ST**): generate a secret key set for any user $\mathbf{ID} \in \{0,1\}^{l_{\mathrm{id}}}$, and the algorithm first calculates the set $J_t = \{J_{t_1,1}, J_{t_1,2}, \ldots, J_{t_1,l_{\mathrm{time}}+1}\}$ for initial time period $0^{l_{\mathrm{time}}}$ 1. For $c = 1$, $c = 1, \ldots, l_{\mathrm{time}}$, +1, if $J_{t_1,c} \neq \perp$, it runs **HIBS.Extract** ($\mathbf{mpk}_1, \mathbf{msk}_1, \mathbf{ID}, |J_{t_1,c}$) to get a secret key $K_{t_1,c}$. If $J_{t_1,c} = \perp$, it sets $K_{t_1,c} = \perp$. Ultimately, this algorithm outputs the secret key $\mathrm{sk}_{\mathbf{ID}}^{(t_1)} = \{1, (K_{t,1}, \ldots, K_{t,l_{\mathrm{time}}+1})\}$.

(iii) $\mathrm{sk}_{\mathbf{ID}}^{(t)}$←**SKEval** ($\mathbf{mpk}, \mathrm{sk}_{\mathbf{ID}}^{(t-1)}, t$): for $t \in \{0,1\}^{l_{\mathrm{time}}}$, firstly, the algorithm calculates the two sets J_{t-1} and J_t. For $c_2 = 1, \ldots, l_{\mathrm{time}}$ +1, if $J_{t,c_2} \neq \perp$, there must be an element c_1 in the set $\{1, \ldots, l_{\mathrm{time}} + 1\}$ such that a prefix of (**ID**, J_{t,c_2}) is (**ID**, J_{t-1,c_1}). It then runs **HIBS.Derive** ($\mathbf{mpk}_1, K_{t-1,c_1}, \mathbf{ID}, |J_{t,c_2}$) to gain

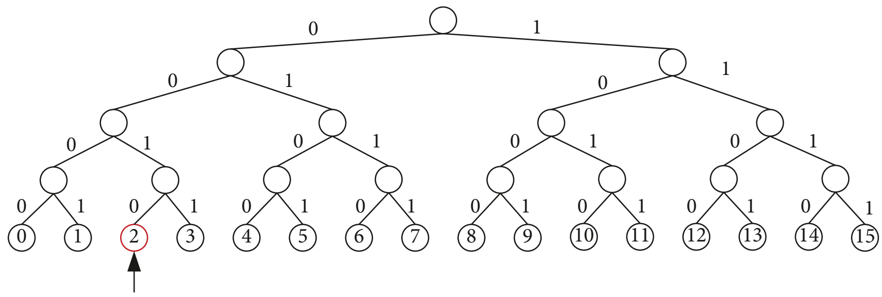

Figure 4: $t = 0010$.

the corresponding key K_{t,c_2}. If $J_{t,c_2} = \perp$, it sets $K_{t,c_2} = \perp$. Ultimately, it returns $\mathrm{sk}_{\mathbf{I\,D}}^{(t)} = \{t, (K_{t,1}, \ldots, K_{t,l_{\mathrm{time}}+1})\}$.

(iv) $uk_t \leftarrow \mathbf{SKUp\,da\,te}(\mathbf{mpk}, \mathbf{msk}, \mathbf{ST}, \mathbf{RL}, t)$: for $t \in \{0,1\}^{l_{\mathrm{time}}}$, firstly, this algorithm runs node selection algorithm to get cover set **KUN (BT,RL**,t). Then, for $\forall x \in \mathbf{KUN}(\mathbf{BT}, \mathbf{RL}, t)$, it runs $\mathbf{IBS.Extract}(\mathbf{mpk}_2, \mathbf{msk}_2, t|v_x)$ to get the key L_x corresponding to identity $t|v_x$. Ultimately, it outputs the update key set $uk_t = \{t, \{L_x\}_{x \in KUN(\mathbf{BT}, \mathbf{RL}, t)}\}$.

(v) Sign $k_{\mathbf{I\,D},t} \leftarrow \mathbf{SKGen}(\mathrm{sk}_{\mathbf{I\,D}}^{(t)}, \mathrm{uk}_t)$: suppose that a user's $uk_t = \{t, \{L_x\}_{x \in \mathbf{KUN}(\mathbf{BT}, \mathbf{RL}, t)}\}$ and $\mathrm{sk}_{\mathbf{I\,D}}^{(t)} = \{t, (K_{t,1}, \ldots, K_{t,l_{\mathrm{time}}+1})\}$. Suppose that **ID** is a non-revoked user within time period t; there must exist a $x^* \in \mathbf{KUN}(\mathbf{BT}, \mathbf{RL}, t) \cap \mathrm{Path}(\mathbf{I\,D})$. It outputs **ID**'s signature key Sign $k_{\mathbf{I\,D}}^{(t)} = (K_{t,l_{\mathrm{time}}+1}, L_{x^*})$.

(vi) $\sigma_{\mathbf{I\,D},t} \leftarrow \mathbf{Sign}(\mathrm{Sign}\,k_{\mathbf{I\,D},t}, \mathbf{I\,D}, t, M)$: for a message $M \in \mathscr{M}$, suppose that **ID** is a non-revoked user within t time period; the signer has a valid signing key $\mathrm{sk}_{\mathbf{I\,D}}^{(t)} = (K_{t,l_{\mathrm{time}}+1}, L_{x^*})$. Then, it computes $\sigma_1 \leftarrow \mathbf{HIBS.Sign}(K_{t,l_{\mathrm{time}}+1}, \mathbf{I\,D}|J_{t,l_{\mathrm{time}}+1}, M)$, and $\sigma_2 \leftarrow \mathbf{IBS.Sign}(L_{x^*}, t|v_{x^*}, M)$. Finally, the algorithm returns a signature $\sigma_{\mathbf{I\,D},t} = (\sigma_1, \sigma_2)$.

(vii) $1/0 \leftarrow \mathbf{Verify}(\mathbf{mpk}, M, t, \mathbf{I\,D}, \sigma_{\mathbf{I\,D},t})$: for a signature $\sigma_{\mathbf{I\,D},t} = (\sigma_1, \sigma_2)$, the algorithm computes $V_1 \leftarrow \mathbf{HIBS.Verify}(\mathbf{mpk}_1, M, \mathbf{I\,D}|J_{t,l_{\mathrm{time}}+1}, \sigma_1)$ and $V_{2,x} \leftarrow \mathbf{IBS.Verify}(\mathbf{mpk}_2, M, t|v_x, \sigma_2)$ for each node $x \in \mathrm{Path}(\mathbf{I\,D})$. Note that $\{V_{2,x}\}_{x \in Path(\mathbf{I\,D})}$ is a set. If there is a $V_2 \in V_{2,x}$ such that $V_1 \times V_2 = 1$, the algorithm outputs 1, and 0 otherwise.

(viii) **RL**←**Revoke** (**RL, ID**, t): suppose that the input identity **ID** is not a non-revoked user at time period t; then (**ID**, t) is added to **RL** by key authority and outputs new **RL.**

Correctness. The correctness of Con.1 (Construction 1) is determined by the correctness of the fundamental HIBS and IBS schemes. Suppose that identity **ID** is a non-revoked user within time period t; in the IBS scheme, the signing key corresponding to $t|v_{x^*}$ is L_{x^*}, and $K_{t,l_{\mathrm{time}}+1}$ is the signing key corresponding to $\mathbf{I\,D}|J_{t,l_{\mathrm{time}}+1}$ in the HIBS scheme. The two signature algorithms **IBS.Sign** and **HIBS.Sign** can correctly sign the message M. We can correctly get $\sigma_{\mathbf{I\,D},t}$ by $\mathbf{HIBS.Sign}(K_{t,l_{\mathrm{time}}+1,M})$ and $\mathbf{IBS.Sign}(L\{\_x^*\}, t|v_{x^*}, M)$. Then, compute $V_1 \leftarrow \mathbf{HIBS.Verify}(\mathbf{mpk}_1, M, t, \mathbf{I\,D}|J_{t,l_{\mathrm{time}}+1}, \sigma_1)$ and $V_{2,x} \leftarrow \mathbf{IBS.Verify}(\mathbf{mpk}_2, M, (t|v_x, \sigma_2))$ for each node $x \in \mathrm{Path}(\mathbf{I\,D})$. There always exists a $V_2 \in V_{2,x}$ such that $V_1 \times V_2 = 1$ holds.

Security. The SU-CMA security of Con.1 is determined by the SU-CMA security of the fundamental HIBS scheme and IBS scheme. Especially, it is ensured by Theorem 1.

Theorem 1. *If the fundamental HIBS and IBS schemes are SU-CMA secure, the FS-RIBS scheme in Con.1 is SU-CMA secure.*

Outline of Proof. Firstly, we emphasize the core idea of security proof and then introduce a strict proof of security reduction. For this proof, adversaries are classified into two types as described in Section 3.2. T2 adversary is designed to break Con.1's forward security. For T1 adversary, we need to build an emulator to store the master secret key of the fundamental HIBS and reduce the SU-CMA security of the FS-RIBS scheme to the SU-CMA security of the fundamental IBS scheme. For T2 adversary, the emulator holds the master secret key of the fundamental IBS scheme and reduces the SU-CMA security of the FS-RIBS scheme to the SU-CMA security of fundamental HIBS scheme.

Proof. Let adversary $\mathscr{A}$ break the SU-CMA security of the FS-RIBS scheme; then, we build a PPT emulator $\mathscr{E}$ to break the SU-CMA security of the fundamental IBS scheme or HIBS scheme. The emulator works in two steps: firstly, it randomly gets a bit b. Secondly, if $b = 0$, $\mathscr{A}$ is regarded as $\mathscr{E}$ a T1 adversary, else a T2 adversary. So, the probability of $\mathscr{E}$ correctly or incorrectly guessing the adversary's type is 1/2.

(i) For T1 adversary, $\mathscr{E}$ is given $\mathbf{mpk}_2$ of the fundamental IBS scheme. It emulates the process as follows:

(1) **Setup:** it produces the master key pair $(\mathbf{mpk}_1, \mathbf{msk}_1)$ of the fundamental HIBS scheme. $\mathscr{E}$ initializes **RL** and **BT**. It sends $\mathbf{mpk}_1$ and $\mathbf{mpk}_2$ to $\mathscr{A}$. Then, $\mathscr{A}$ sends a challenge identity $\mathbf{ID}^*$ and a challenge time period t^* to $\mathscr{E}$.

(2) **Phase 1:** since $\mathscr{E}$ gets the $\mathbf{msk}_1$ of HIBS scheme, it can respond to $\mathscr{A}$'s secret key query and create key query for any time period t and any **ID**. If $\mathscr{A}$ needs an update key query within time period t, $\mathscr{E}$ first calculates the set $\mathbf{KUN}(\mathbf{BT},\mathbf{ST},t)$. Then, it sends the set of identities $\{t|v_x\}_{x\in\mathbf{KUN}(\mathbf{BT},\mathbf{ST},t)}$ to the challenger of the fundamental IBS scheme to get the corresponding update keys $\{L_x\}_{x\in\mathbf{KUN}(\mathbf{BT},\mathbf{ST},t)}$. Ultimately, $\mathscr{E}$ sends $\{L_x\}_{x\in\mathbf{KUN}(\mathbf{BT},\mathbf{ST},t)}$ to $\mathscr{A}$. $\mathscr{E}$ can get corresponding update keys from its challenger, so $\mathscr{E}$ can respond to $\mathscr{A}$'s signing queries.

(3) **Signature query phase:** $\mathscr{A}$ can adaptively query $\mathscr{E}$ for polynomial signatures. The identity, time period, and message of these signatures are arbitrary. Here, suppose $\mathscr{A}$ queries q times, the message set is $\{M_1,\ldots,M_q\}$, and the time period set is $\{t_1,\ldots,t_q\}$. For $i=1,2,\ldots,q$, it calculates $\sigma^{1,M_i}_{\mathbf{ID}_i,t_i}\leftarrow\mathbf{HIBS.Sign}(K_{t_i,l_{\text{time}}+1},M_i)$ and $\sigma^{2,M_i}_{\mathbf{ID}_i,t_i}\leftarrow\mathbf{IBS.Sign}(L_{x^*},M_i)$ if $\mathbf{ID}_i$ is a non-revoked user within time period t_i, respectively. Finally, it returns $\sigma^{M_i}_{\mathbf{ID}_i,t_i}=\{\sigma^{1,M_i}_{\mathbf{ID}_i,t_i},\sigma^{2,M_i}_{\mathbf{ID}_i,t_i}\}$ to $\mathscr{A}$.

(4) **Forgery:** let us assume that $\mathscr{A}$ successfully constructs a signature $\sigma^{M^*}_{\mathbf{ID}^*,t^*}=(\sigma^{1,M^*}_{\mathbf{ID}^*,t^*},\sigma^{2,M^*}_{\mathbf{ID}^*,t^*})$, and this signature $(M^*,\sigma^{M^*}_{\mathbf{ID}^*,t^*})\notin\{(M_1,\sigma^{M_1}_{\mathbf{ID}_1,t_1}),\ldots,(M_q,\sigma^{M_q}_{\mathbf{ID}_q,t_q})\}$. Now, we calculate the probability of success of $\mathscr{A}$. First, we calculate $V_1^*\leftarrow\mathbf{HIBS.Verify}(\mathbf{mpk}_1,M^*,t^*,\mathbf{ID}^*|J_{t^*,l_{time}+1},\sigma^{1,M^*}_{\mathbf{ID}^*,t^*})$ and $V^*_{2,x}\leftarrow\mathbf{IBS.Verify}(\mathbf{mpk}_2,M^*,t^*|v_x,\sigma^{2,M^*}_{\mathbf{ID}^*,t^*})$ for $\forall x\in\text{Path}(\mathbf{ID}^*)$. Then, in the above emulated experiment, since $\mathbf{ID}^*$ has been revoked before the challenge t^* time period, for any (even the challenge) time period t, the sets of identities $\{t^*|v_x\}_{x\in\text{Path}(\mathbf{ID}^*)}\cap\{t|v_x\}_{x\in\mathbf{KUN}(\mathbf{BT},\mathbf{ST},t)}=\varnothing$. Therefore, the challenge identities that $\mathscr{E}$ transmits to its own challenger are indeed valid. Naturally, if $(M^*,\sigma^{M^*}_{\mathbf{ID}^*,t^*}))$ is a valid FS-RIBS signature, there must exist one $x^*\in\text{Path}(\mathbf{ID}^*)$, so that $1\leftarrow\mathbf{IBS.Verify}(\mathbf{mpk}_2,M^*,t^*|v_{x^*},\sigma^{2,M^*}_{\mathbf{ID}^*,t^*})$. That is, $(M^*,\sigma^{2,M^*}_{\mathbf{ID}^*,t^*})$ is a valid IBS signature under identity $t^*|v_{x^*}$. Thus, $\mathscr{E}$ has the same success probability of breaking the SU-CMA security of the fundamental IBS scheme. Therefore, we have

$$\text{Adv}^{\text{SU-CMA}}_{\text{FS-RIBS},\mathscr{A}}(\lambda)\le\text{Adv}^{\text{SU-CMA}}_{\text{IBS},\mathscr{A}_1}(\lambda),\tag{3}$$

where $\mathscr{A}_1$ is any PPT adversary who can break the SU-CMA security of the fundamental IBS scheme.

(ii) Next, for T2 adversary, we introduce a PPT algorithm $\mathscr{E}$ to emulate the experiment and reduce the SU-CMA security of our FS-RIBS scheme to the SU-CMA security of the fundamental HIBS scheme. $\mathscr{E}$ is the master public key of the HIBS scheme and gets the master key pair $(\mathbf{mpk}_2,\mathbf{msk}_2)$ of IBS by itself.

$\mathscr{E}$ can respond to $\mathscr{A}$'s queries about creating keys and secret keys. Obviously, $\mathscr{A}$ may query the secret key within t^*. $\mathscr{E}$ can answer the update key queries using $\mathbf{msk}_2$ of the fundamental IBS scheme. The signature query is the same as the signature query of T-1. Let us assume that $\mathscr{A}$ successfully constructs a signature $\sigma^{M^*}_{\mathbf{ID}^*,t^*}=(\sigma^{1,M^*}_{\mathbf{ID}^*,t^*},\sigma^{2,M^*}_{\mathbf{ID}^*,t^*})$. Because the $\mathbf{ID}^*$ is a non-revoked user in the time period t^*, its $\sigma^{2,M^*}_{\mathbf{ID}^*,t^*}$ is necessary to pass the verification. Then, because $\mathscr{A}$ can only query for the signing key $(K_{t,l_{\text{time}}+1})_{t\neq t^*}$, $\mathscr{A}$ successfully forges $\sigma^{1,M^*}_{\mathbf{ID}^*,t^*}$ which is equivalent to breaking the SU-CMA security of the fundamental HIBS scheme. Thus, for Type-2 adversary, we will have

$$\text{Adv}^{\text{SU-CMA}}_{\text{FS-RIBS},\mathscr{A}}(\lambda)\le\text{Adv}^{\text{SU-CMA}}_{\text{HIBS},\mathscr{A}_2}(\lambda),\tag{4}$$

where $\mathscr{A}_2$ is any PPT adversary who can attack the SU-CMA security of the fundamental IBS scheme.

Considering the above two cases comprehensively, we can get the following inequality:

$$\text{Adv}^{\text{SU-CMA}}_{\text{FS-RIBS},\mathscr{A}}(\lambda)\le\frac{1}{2}\text{Adv}^{\text{SU-CMA}}_{\text{IBS},\mathscr{A}_1}(\lambda)+\frac{1}{2}\text{Adv}^{\text{SU-CMA}}_{\text{HIBS},\mathscr{A}_2}(\lambda).\tag{5}$$

□

4.2. Improvement. In Con.1, to determine the validity of the second part signature σ_2, Con.1 requires computing IBS verification algorithm l_{id} times for each identity $t|v_x$, where $x\in\text{Path}(\mathbf{I\ D})$. Next, we introduce two simple methods to solve this problem.

4.2.1. The First Method. The difference from Con.1 is that the second component of IBS scheme is replaced with a HIBS scheme. That is, the HIBS scheme will be used to get the update keys of the FS-RIBS scheme. Additionally, the value of each selected node in the node section algorithm is regarded as the identity vector of the fundamental HIBS scheme. For example, suppose that $v_{x_{12}}=101$ as in Figures 2 and 3. Therefore, for $t\in\{0,1\}^{l_{\text{time}}}$, the identity vector $(t,1,0,1)$ is used to represent $t|v_{x_{12}}$. The details of this improved FS-RIBS scheme are given in Construction 2.

Construction 2 (Forward-Secure RIBS Scheme). The construction is described as follows.

(i) $(\mathbf{mpk},\mathbf{msk},\mathbf{ST},\mathbf{RL})\leftarrow\mathbf{RIBS.Setup}(\lambda,l_{\text{id}},l_{\text{time}})$: *it gets* $(\mathbf{mpk}_1,\mathbf{msk}_1)$ *by running* $\mathbf{HIBS.Setup}(\lambda,l_{\text{time}}+1)$ *and* $(\mathbf{mpk}_2,\mathbf{msk}_2)$ by running $\mathbf{HIBS.Setup}(\lambda,l_{\text{id}}+1)$. *A complete binary tree of depth* l_{id} *is initialized by the algorithm. Each leaf node corresponds to an identity. Ultimately, it returns* $\mathbf{mpk}=(\mathbf{mpk}_1,\mathbf{mpk}_2)$, $\mathbf{msk}=(\mathbf{msk}_1,\mathbf{msk}_2)$, $\mathbf{ST}=\mathbf{BT}$, *and* **RL.**

(ii) $\text{sk}^{(t_1)}_{\mathbf{I\ D}}\leftarrow\mathbf{RIBS.KeyGen}(\mathbf{mpk},\mathbf{msk},\mathbf{ID},\mathbf{ST})$: *this algorithm is the same as in* Construction 1.

(iii) $\text{sk}^{(t)}_{\mathbf{I\ D}}\leftarrow\mathbf{SKEval}(\mathbf{mpk},sk^{(t-1)}_{\mathbf{I\ D}},t)$: *this algorithm is the same as in* Construction 1.

(iv) $\mathrm{uk}_t \leftarrow \mathbf{SKUp\ da\ te}(\mathbf{mpk}, \mathbf{msk}, \mathbf{ST}, \mathbf{RL}, t)$: for $t \in \{0,1\}^{l_{\mathrm{time}}}$, *firstly, it calculates the cover set* $\mathbf{KUN}(\mathbf{BT}, \mathbf{RL}, t)$. *Then,* $\forall x \in \mathbf{KUN}(\mathbf{BT}, \mathbf{RL}, t)$, *it runs* $\mathbf{HIBS.Extract}(\mathbf{mpk}_2, \mathbf{msk}_2, t|v_x)$*to get the key* L_x *corresponding to the hierarchical identity* $t|v_x$. *Ultimately, it returns the update key* $uk_t = \left\{t, \{L_x\}_{x \in KUN(BT,RL,t)}\right\}$.

(v) $\mathrm{Sign}k_{\mathbf{I\ D},t} \leftarrow \mathbf{SKGen}(sk_{\mathbf{I\ D}}^{(t)}, uk_t)$: *suppose that a user's current secret key is* $sk_{\mathbf{I\ D}}^{(t)} = \left\{t, (K_{t,1}, \ldots, K_{t,l_{\mathrm{time}}+1})\right\}$ *and current update key is* $uk_t = \left\{t, \{L_x\}_{x \in \mathbf{KUN}(\mathbf{BT},\mathbf{RL},t)}\right\}$. *Suppose that* **ID** *is a non-revoked user at time period* t; *there must be a node such that* $x^* \in \mathbf{KUN}(\mathbf{BT}, \mathbf{RL}, t) \cap \mathrm{Path}(\mathbf{I\ D})$. *Therefore, a prefix of* $t|v_{\mathbf{I\ D}}$ *must be* $t|v_{x^*}$. Firstly, *The algorithm runs* $\mathbf{HIBS.Extract}(\mathbf{mpk}_2, L_{x^*}, t|v_{\mathbf{I\ D}})$*to get the corresponding key* $L_{\mathbf{I\ D}}$. *It returns the corresponding signing key* $\mathrm{Sign}k_{\mathbf{I\ D}}^{(t)} = (K_{t,l_{\mathrm{time}}+1}, L_{\mathbf{I\ D}})$.

(vi) $\sigma_{\mathbf{I\ D},t} \leftarrow \mathbf{Sign}(\mathrm{Sign}\,k_{\mathbf{I\ D},t}, \mathbf{I\ D}, t, M)$: *if the identity* **ID** *is a non-revoked user within time period,* $\mathrm{Sign}\,k_{\mathbf{I\ D}}^{(t)} = (K_{t,l_{\mathrm{time}}+1}, L_{\mathbf{I\ D}})$. *Then, it computes* $\sigma_1 \leftarrow \mathbf{HIBS.Sign}(K_{t,l_{\mathrm{time}}+1}, \mathbf{I\ D}|J_{t,l_{\mathrm{time}}+1}, M)$, *and* $\sigma_2 \leftarrow \mathbf{IBS.Sign}(L_{\mathbf{I\ D}}, t|v_{\mathbf{I\ D}}, M)$. *Finally, the algorithm returns a signature* $\sigma_{\mathbf{I\ D},t} = (\sigma_1, \sigma_2)$.

(vii) $1/0 \leftarrow \mathbf{Verify}(\mathbf{mpk}, M, t, \mathbf{I\ D}, \sigma_{\mathbf{I\ D},t})$: *for a signature* $\sigma_{\mathbf{I\ D},t} = (\sigma_1, \sigma_2)$, *the algorithm computes* $V_1 \leftarrow \mathbf{HIBS.Verify}(\mathbf{mpk}_1, M, \mathbf{I\ D}|J_{t,l_{time}+1}, \sigma_1)$ *and* $V_{2,x} \leftarrow \mathbf{HIBS.Verify}(\mathbf{mpk}_2, M, (t|v_{\mathbf{I\ D}}, \sigma_2))$. *If* $V_1 \times V_2 = 1$, *the algorithm outputs 1, and 0 otherwise.*

(viii) $\mathbf{RL} \leftarrow \mathbf{Revoke}(\mathbf{RL}, \mathbf{I\ D}, t)$: *suppose that the input identity* **ID** *is not a non-revoked user at time period* t; *then,* (**ID**, t) *is added to* **RL** *by key authority and outputs new* **RL.**

Correctness. Similar to the first generic construction, the correctness of Construction 2 (Con.2) is based on the correctness of two basic HIBS schemes. The difference from Con.1 is that L_{x^*} is the signing key corresponding to identity vector $t|v_{x^*}$ in the second HIBS scheme, and the actual signature key $L_{\mathbf{I\ D}}$ is extracted from L_{x^*} as $t|v_x$ is a prefix identity vector of $t|v_{\mathbf{I\ D}}$. Therefore, the two verify algorithms of HIBS schemes can verify σ_1 and σ_2, respectively.

Security. The SU-CMA security of Con.2 is determined by the SU-CMA security of the fundamental HIBS schemes. Then, we have Theorem 2.

Theorem 2. *If the fundamental HIBS schemes are SU-CMA secure, then the FS-RIBS scheme in Con.2 is SU-CMA secure.*

The proof of Theorem 2 is basically the same as Theorem 1. The only difference is that uk_t is obtained by a HIBS scheme. We omit its proof.

4.2.2. The Second Method. Observe that, in Con.1, as the verifier does not know the target node x^* used by the signer to generate the second part signature σ_2, he must run the IBS verification algorithm l_{id} times for each node $x \in \mathrm{Path}(\mathbf{I\ D})$. So, to solve this issue, the signer can indicate the target node x^* in the signature. The second improved FS-RIBS scheme (referred to as Construction 3) is identical to that of Con.1, except for the following differences in algorithms **Sign** and **Verify**.

(i) The modified signing algorithm $\mathbf{Sign}(\mathrm{Sign}k_{\mathbf{I\ D},t}, \mathbf{I\ D}, t, M)$: for a message $M \in \mathcal{M}$, if **ID** is a non-revoked user within time period t, the signer should have a valid signing key $\mathrm{sk}_{\mathbf{I\ D}}^{(t)} = (K_{t,l_{\mathrm{time}}+1}, L_{x^*})$. Then, it sets $M' = M|v_{x^*}$ and computes $\sigma_1 \leftarrow \mathbf{HIBS.Sign}(K_{t,l_{\mathrm{time}}+1}, \mathbf{I\ D}|J_{t,l_{\mathrm{time}}+1}, M')$, and $\sigma_2 \leftarrow \mathbf{IBS.Sign}(L_{x^*}, t|v_{x^*}, M')$. Finally, the algorithm returns a signature $\sigma_{\mathbf{I\ D},t} = (\sigma_1, \sigma_2, x^*)$.

(ii) The modified verification algorithm $\mathbf{Verify}(\mathbf{mpk}, M, t, \mathbf{I\ D}, \sigma_{\mathbf{I\ D},t})$: for a signature $\sigma_{\mathbf{I\ D},t} = (\sigma_1, \sigma_2, x^*)$, firstly, the algorithm judges whether $x^* \in \mathrm{Path}(\mathbf{I\ D})$. If this is not the case, it outputs $\perp$; otherwise, it sets $M' = M|v_{x^*}$ and computes $V_1 \leftarrow \mathbf{HIBS.Verify}(\mathbf{mpk}_1, M', \mathbf{I\ D}|J_{t,l_{time}+1}, \sigma_1)$ and $V_2 \leftarrow \mathbf{IBS.Verify}(\mathbf{mpk}_2, M', t|v_{x^*}, \sigma_2)$. If $V_1 \times V_2 = 1$, the algorithm outputs 1, and 0 otherwise.

In Con.1, if we change the message M to $M' = M|v_{x^*}$, where x^* is the corresponding node x^* in the signing key L_{x^*}, this is just the above improved Construction 3 (Con.3). So, the correctness and security of Con.3 can be proved similarly as in Con.1. We omit the details.

5. Lattice-Based Instantiation and Comparison

In this section, we instantiate our generic construction to several lattice-based (H)IBS schemes and compare them with other lattice-based RIBS games. These schemes have or do not have forward security.

5.1. Instantiations. The instantiation of the fundamental HIBS scheme uses the scheme of Rückert [28], and the instantiation of the fundamental IBS scheme uses the scheme of Liu et al. [29]. It produces an adaptively secure FS-RIBS scheme (represented by "Con.1+ [28, 29]"). In addition, the instantiations of Construction 2 and Construciton 3 are represented by "Con.2+ [28]" and "Con.3+ [28, 29]," respectively). To reduce the storage overhead of instantiation, we further replace the above HIBS scheme with the HIBS scheme of Tian et al. [30] and the above IBS scheme with the IBS scheme of Chen et al. [31] (represented by "Con.1+ [30, 31]," "Con.2+ [30]," and "Con.3+ [30, 31]," respectively). Next, we take Con.1+ [28, 29] as an example to introduce the detailed requirement and parameter settings:

(1) The schemes in [28, 29] are strongly unforgeable under choice message attack. Their security is based on SIS over lattices.

(2) $\mathbf{mpk}_1 = (A^*, [A], [B], y)$, where $A^* \in Z_q^{n \times m_1 + m_2}$, S^* is a trapdoor $\wedge_q^{\perp}(A^*)$, $[A] := (A_i^{(0)}, A_i^{(1)})_1^{l_k + 2^{l_{\mathrm{time}}}}$, $[B] := (B_i^{(0)}, B_i^{(1)})_1$, $y \leftarrow Z_q^n$. $\mathbf{msk}_1 = S^*$. The sizes of q, m_1, m_2, n are defined in Proposition 1 of Rückert [28].

Table 1: Security comparison of RIBS schemes.

Schemes	FS	SKER	SD/RO	SU/EU	RQA	Adaptive	DP
SE13 [4]	No	Yes	SD	EU	No	No	CDH
WLH17 [16]	Yes	Yes	SD	EU	No	Yes	q-DHE
HTH17 [34]	No	No	RO	EU	Yes	Yes	SIS/NTRU
XWW20 [13]	No	Yes	RO	EU	Yes	No	SIS
XWW20 [14]	No	No	SD	EU	Yes	No	SIS
XWZ22 [15]	No	Yes	RO	EU	Yes	No	SIS
Con.1+ [28, 29]	Yes	Yes	SD	SU	Yes	No	SIS
Con.1+ [30, 31]	Yes	Yes	RO	SU	Yes	Yes	SIS
Con.2+ [28]	Yes	Yes	SD	SU	Yes	No	SIS
Con.2+ [30]	Yes	Yes	RO	SU	Yes	Yes	SIS
Con.3+ [28, 29]	Yes	Yes	SD	SU	Yes	No	SIS
Con.3+ [30, 31]	Yes	Yes	RO	SU	Yes	Yes	SIS

Table 2: Comparison of space cost.

Traditional schemes	$\lvert\mathbf{mpk}\rvert$	$\lvert sk_{\mathbf{I\,D}}\rvert$	$\lvert uk_t\rvert$	$\lvert S\rvert$
SE13 [4]	$O(\lambda)$	$O(1)$	$O(L)$	$O(1)$
WLH17 [16]	$O(\lambda)$	$O(1)$	$O(L)$	$O(1)$
Post-quantum schemes	$\lvert\mathbf{mpk}\rvert$	$\lvert sk_{\mathbf{I\,D}}\rvert$	$\lvert uk_t\rvert$	$\lvert S\rvert$
HTH17 [34]	$O(\lambda)$	$O(\lambda\log\lambda)$	$O(\lambda\log\lambda)$	$O(\lambda+\log\lambda)$
	$\lvert\mathbf{mpk}\rvert(\circ\mathbb{Z}_q^{n\times m})$	$\lvert sk_{\mathbf{I\,D}}\rvert(\circ\mathbb{Z}^{m\times m})$	$\lvert uk_t\rvert(\circ\mathbb{Z}^{m\times m})$	$\lvert S\rvert(\circ\mathbb{Z}_q^{m})$
XWW20 [13]	$O(l)$	$O(1)$	$O(L)$	$O(1)$
XWW20 [14]	$O(l)$	$O(1)$	$O(L)$	$O(1)$
XWZ22 [15]	$O(l)$	$O(1)$	$O(L)$	$O(1)$
Con.1+ [28, 29]	$O(l+\log T)$	$O(\log T)$	$O(L)$	$O(l)$
Con.1+ [30, 31]	$O(1)$	$O(\log T)$	$O(L)$	$O(1)$
Con.2+ [28]	$O(l+\log\ T)$	$O(\log T)$	$O(L)$	$O(l+\log\ T)$
Con.2+ [30]	$O(1)$	$O(\log T)$	$O(L)$	$O(1)$
Con.3+ [28, 29]	$O(l+\log\ T)$	$O(\log T)$	$O(L)$	$O(l)$
Con.3+ [30, 31]	$O(1)$	$O(\log T)$	$O(L)$	$O(1)$

(3) The definitions of $\mathbf{mpk}_2$ and $\mathbf{msk}_2$ are not different from those in Section 3 of Liu et al. [29].

(4) The key extraction algorithm is the same as that defined in [28, 29]. The difference is that only input in [28, 29] is the identity, while our HIBS part (user's long-term private key) input is $\mathbf{I\,D}|J_{t_1,c}$, and the IBS part (user's temporary private key) input is $t|v_x$.

(5) $\mathbf{HIBS.Sign}(K_{t,l_{\text{time}}+1}, \mathbf{I\,D}|J_{t,l_{\text{time}}+1}, M)$ is constructed as in Section 4.2 [28] and $\mathbf{IBS.Sign}(L_{x^*}, t|v_{x^*})$ is constructed in Section 3 [29]. The bottom layer of the signature algorithms in both parts is based on the SIS problem, in which the **HIBS.Sign ()** algorithm is based on the **SamplePre** algorithm proposed by Craig et al. [32]. **IBS.Sign ()** algorithm is based on **SampleLeft** algorithm proposed by Agrawal et al. [33].

The instantiation details of other schemes ("Con.2+ [28]" and "Con.3+ [28, 29]") are similar to the above schemes and will not be repeated.

5.2. Comparison. We mainly compare security and storage overhead through two tables. We compare the security of our six schemes ("Con.1+ [28, 29]," "Con.2+ [28]," "Con.3+ [28, 29]," "Con.1+ [30, 31]," "Con.2+ [30]," and "Con.3+ [30, 31]") with other RIBS schemes in Table 1, in terms of whether it has forward security (FS), whether it is signing key exposure resistance (SKER), whether it is under the standard model or the random oracle model (SD/RO), whether it is existential unforgeability or strong unforgeability (SU/EU), whether it is resistant to quantum attacks (RQA), whether it is adaptive or not adaptive, and what difficult problems (DPs) are these schemes based on. We list in Table 2 space cost of our six schemes and other RIBS schemes in terms of $\mathbf{mpk}(|\mathbf{mpk}|sk_{\mathbf{I\,D}}(|sk_{\mathbf{I\,D}}|))$, $uk_t(|uk_t|)$, and signature $(|S|)$. In Table 2, the binary string length of the message is l, T is the maximum time period, and $L = R\log(N/R)$. $\circ$ means that the complexity of the subsequent scheme must be multiplied by the vector or matrix after $\circ$.

It can be seen from Table 1 that our schemes can resist most attacks, including quantum computing attacks, forward security, revocation (backward security), standard model, signing key exposure attacks, and strong unforgeability. From Table 2, we can see that the master key and signature size of our "Con.1+ [28, 29]," "Con.2+ [28,]" and "Con.3+ [28, 29]" are large. This is because the underlying HIBS scheme [28] does not apply lattice basis delegation [35]. As shown in "Con.1+ [30, 31]," "Con.1+ [30]" and "Con.3+ [30, 31]," we then used the technique of [30] and the lattice basis delegation [31] to reduce the size of the signature as well as the system master key to a constant size.

6. Conclusion and Future Work

This paper introduced a generic method to construct forward-secure revocable identity-based signature and introduced two methods to improve its verification efficiency. In addition, the paper instantiated the generic construction from various lattice-based (H)IBS schemes and obtained the first lattice-based FS-RIBS schemes. In the future, we will try to optimize the fundamental HIBS or IBS scheme to improve its practicality.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This study was supported by the National Natural Science Foundation of China (grant nos. 62002288 and 61872292), the Basic Research Program of Qinghai Province (grant no. 2020-ZJ-701), the fund of Science and Technology on Communication Security Laboratory (grant no. 6142103190101), and the Natural Science Foundation of Shanghai (grant no. 19ZR1454100).

References

[1] S. Adi, "Identity-based cryptosystems and signature schemes," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 47–53, Springer, Berlin, Germany, 1984.

[2] D. Boneh, "Identity-based encryption from the weil pairing," *Advances in Crytology, Crypto*, pringer, Berlin, Germany, 2001.

[3] A. Ge and P. Wei, "Identity-based broadcast encryption with efficient revocation," 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 I, Volume 11442 of Lecture Notes In Computer Science*, D. Lin and K. Sako, Eds., pp. 405–435, Springer, Cham, Switzerland, 2019.

[4] J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: security model and construction," in *International Workshop on Public Key Cryptography*, pp. 216–234, Springer, Cham, Switzerland, 2013.

[5] J. H. Seo and K. Emura, "Revocable identity-based cryptosystem revisited: security models and constructions," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 7, pp. 1193–1205, 2014.

[6] T.-T. Tsai, Y.-M. Tseng, and T.-Y. Wu, "Provably secure revocable id-based signature in the standard model," *Security and Communication Networks*, vol. 6, no. 10, pp. 1250–1260, 2013.

[7] Y. Sun, F. Zhang, L. Shen, and R. Deng, "Revocable identity-based signature without pairing," in *Proceedings of the 2013 5th International Conference on Intelligent Networking and Collaborative Systems*, pp. 363–365, IEEE, Xi'an, China, September 2013.

[8] Y. H. Hung, T. T. Tsai, Y. M. Tseng, and S. S. Huang, "Strongly secure revocable id-based signature without random oracles," *Information Technology and Control*, vol. 43, no. 3, pp. 264–276, 2014.

[9] Z. Liu, X. Zhang, Y. Hu, and T. Takagi, "Revocable and strongly unforgeable identity-based signature scheme in the standard model," *Security and Communication Networks*, vol. 9, no. 14, pp. 2422–2433, 2016.

[10] X. Yang, T. Ma, P. Yang, F. An, and C. Wang, "Security analysis of a revocable and strongly unforgeable identity-based signature scheme," *Information Technology and Control*, vol. 47, no. 3, pp. 575–587, 2018.

[11] J. Zhao, B. Wei, and Y. Su, "Communication-efficient revocable identity-based signature from multilinear maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 1, pp. 187–198, 2019.

[12] X. Xiang, "Adaptive secure revocable identity-based signature scheme over lattices," *Computer Engineering*, vol. 10, p. 25, 2015.

[13] C. Xie, J. Weng, J. Weng, and L. Hou, "Scalable revocable identity-based signature over lattices in the standard model," *Information Sciences*, vol. 518, pp. 29–38, 2020.

[14] C. Xie, J. Weng, and J. Wen, "Scalable revocable identity-based signature scheme with signing key exposure resistance from lattices," *Security and Communication Networks*, vol. 2020, Article ID 1743421, 11 pages, 2020.

[15] C. Xie, J. Weng, and D. Zhou, "Revocable identity-based fully homomorphic signature scheme with signing key exposure resistance," *Information Sciences*, vol. 594, pp. 249–263, 2022.

[16] J. Wei, W. Liu, and X. Hu, "Forward-secure identity-based signature with efficient revocation," *International Journal of Computer Mathematics*, vol. 94, no. 7, pp. 1390–1411, 2017.

[17] B. Qin, B. Xue, Z. Dong, H. Cui, and Y. Luo, "Forward-secure revocable identity-based encryption," in *International Conference on Information and Communications Security*, pp. 321–340, Springer, Cham, Switzerland, 2021.

[18] X. Zhang, C. Xu, C. Jin, and R. Xie, "Efficient forward secure identity-based shorter signature from lattice," *Computers & Electrical Engineering*, vol. 40, no. 6, pp. 1963–1971, 2014.

[19] R. Anderson, "Two Remarks on Public Key Cryptology," 1997, https://www.cl.cam.ac.uk/users/rja14.

[20] M. Bellare and S. K. Miner, "A forward-secure digital signature scheme," in *Annual International Cryptology Conference*, pp. 431–448, Springer, Berlin, Germany, 1999.

[21] J. Yu, F. Kong, X. Cheng, R. Hao, and J. Fan, "Forward-secure identity-based public-key encryption without random oracles," *Fundamenta Informaticae*, vol. 111, no. 2, pp. 241–256, 2011.

[22] X. Chen, F. Zhang, H. Tian, B. Wei, and K. Kim, "Discrete logarithm based chameleon hashing and signatures without key exposure," *Computers & Electrical Engineering*, vol. 37, no. 4, pp. 614–623, 2011.

[23] Y. Liu, X. Yin, and L. Qiu, "Id-based forward-secure signature scheme from the bilinear pairings," in *Proceedings of the 2008 International symposium on electronic commerce and security*, pp. 179–183, IEEE, Guangzhou, China, August 2008.

[24] G. Wu and R. Huang, "An efficient identity-based forward secure signature scheme from lattices," in *Proceedings of the 2021 International Wireless Communications and Mobile Computing (IWCMC)*, pp. 626–631, IEEE, Harbin, China, June 2021.

[25] H. Krawczyk, "HMQV: a high-performance secure diffie-hellman protocol," in *Advances in Cryptology - CRYPTO 2005:*

25th Annual International Cryptology Conference, V. Shoup, Ed., pp. 546–566, Springer, Berlin, Heidelberg, 2005.

[26] S. Qiu and D. Wang, "Revisiting three anonymous two-factor authentication schemes for roaming service in global mobility networks," *Journal of Surveillance, Security and Safety*, vol. 2, no. 2, pp. 66–82, 2021.

[27] J. Wei, X. Chen, X. Huang, X. Hu, and S. Willy, "RS-HABE: revocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2301–2315, 2021.

[28] M. Rückert, "Strongly unforgeable signatures and hierarchical identity-based signatures from lattices without random oracles," in *International Workshop on Post-Quantum Cryptography*, pp. 182–200, Springer, Berlin, Heidelberg, 2010.

[29] Z. Liu, Y. Hu, X. Zhang, and F. Li, "Efficient and strongly unforgeable identity-based signature scheme from lattices in the standard model," *Security and Communication Networks*, vol. 6, no. 1, pp. 69–77, 2013.

[30] M. Tian, L. Huang, and W. Yang, "Efficient hierarchical identity-based signatures from lattices," *International Journal of Electronic Security and Digital Forensics*, vol. 5, no. 1, pp. 1–10, 2013.

[31] J. S. Chen, Y. P. Hu, H. Liang, and W. Gao, "Novel efficient identity-based signature on lattices," *Frontiers of Information Technology & Electronic Engineering*, vol. 22, no. 2, pp. 244–250, 2021.

[32] G. Craig, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," 2007, https://eprint.iacr.org/2007/432.

[33] S. Agrawal, D. Boneh, and X. Boyen, "Efficient Lattice (H)ibe in the Standard Model," *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 2015.

[34] Y.-H. Hung, Y.-M. Tseng, and S.-S. Huang, "Revocable Id-Based Signature with Short Size over Lattices," *Security and Communication Networks*, vol. 2017, Article ID 7571201, 9 pages, 2017.

[35] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical ibe," in *Annual Cryptology Conference*, pp. 98–115, Springer, Berlin, Heidelberg, 2010.