entropy

MDPI

Article

Post-Quantum Secure Identity-Based Proxy Blind Signature Scheme on a Lattice

Fengyin Li *, Mengjiao Yang, Zhihao Song, Ping Wang and Guoping Li

School of Computer Science, Qufu Normal University, Rizhao 276800, China; ymj5859@163.com (M.Y.); szh00003499@163.com (Z.S.); wang_00_ping@163.com (P.W.); 19819513250@163.com (G.L.)
* Correspondence: lfyin318@qfnu.edu.cn; Tel.: +86-15963801253

Abstract: Blind signatures have been widely applied when privacy preserving is required, and the delegation of blind signature rights and a proxy blind signature (Proxy-BS) become necessary when the signer cannot sign. Existing Proxy-BS schemes are based on traditional cryptographically hard problems, and they cannot resist quantum attacks. Moreover, most current Proxy-BS schemes depend on public key infrastructure (PKI), which leads to high certificate storage and management overhead. To simplify key management and resist quantum attacks, we propose a post-quantum secure identity-based proxy blind signature (ID-Proxy-BS) scheme on a lattice using a matrix cascade technique and lattice cryptosystem. Under the random oracle model (ROM), the security of the proposed scheme is proved. Security shows that the proposed scheme assures security against quantum attacks and satisfies the correctness, blindness, and unforgeability. In addition, we apply the ID-Proxy-BS scheme on a lattice to e-voting and propose a quantum-resistant proxy e-voting system, which is resistant to quantum attacks and achieves the efficiency of e-voting.

Keywords: blind signature; quantum attack; identity; proxy blind signature; e-voting

Citation: Li, F.; Yang, M.; Song, Z.; Wang, P.; Li, G. Post-Quantum Secure Identity-Based Proxy Blind Signature Scheme on a Lattice. *Entropy* **2023**, *25*, 1157. https://doi.org/10.3390/e25081157

Academic Editors: Hua-Lei Yin, Kaizhi Huang and Guan-Jie Fan-Yuan

Received: 26 June 2023
Revised: 27 July 2023
Accepted: 28 July 2023
Published: 2 August 2023

1. Introduction

A proxy blind signature (Proxy-BS) is a peculiar type of digital signature and is widely applied in e-government systems [1]. Proxy-BS was first proposed by Lin et al. [2]. It allows the original signer to grant their binding signing rights to the proxy signer (P-signer), after which the P-signer signs without revealing the context of the signed message. Therefore, the two properties of Proxy-BS, namely blindness and unforgeability [3,4], guarantee the privacy of the message and security of the signature. Subsequently, a large number of Proxy-BS schemes based on public key cryptography have been proposed. The RSA-based Proxy-BS scheme [5], Proxy-BS scheme based on DLP and ECDLP [6], and Schnorr-based Proxy-BS scheme [7] have been proposed.

However, with the advent of quantum computers, traditional signature schemes such as RSA and DSA have become insecure since the probabilistic polynomial time algorithm was proposed by Shor [8]. Therefore, the lattice-based signature algorithm is one of the most promising candidate technologies. In 1996, AJTAI proposed a lattice-based cryptographic scheme and proved that it is resistant to quantum attacks [9]. Subsequently, a signature scheme based on NTRU was proposed, but it was soon broken by Regev et al. [10,11]. In 2008, Gentry et al. constructed a GPV signature scheme and proved that it satisfies security under the ROM [12]. In 2013, Ducas et al. proposed a new no-sampling algorithm that samples from a bimodal Gaussian distribution and proposed a lattice signing scheme based on this new no-sampling algorithm [13]. In 2014, Zhang et al. proposed a lattice-based Proxy-BS scheme under the standard model and proved its security based on the small integer solution (SIS) [14]. In 2022, Gu et al. proposed device-independent quantum key distribution, which can provide unconditional security for communication between users [15]. In 2023, Yin et al. proposed an experimental secure network, which enables unconditionally secure quantum digital signatures and encryption [16].

The above Proxy-BS schemes are based on the PKI [17]. In the public key cryptosystem based on the PKI, the user's identity (ID) and public key (pk) are bound through the certificate, which involves cumbersome storage and legality verification of the certificate. As an alternative to the PKI-based public key cryptosystem, in 1984, Shamir took the user's ID as the user's pk and proposed the notion of identity encryption. Identity-based cryptography (IBC) also comes from this [18].

In 2017, Gao et al. improved Rückert's scheme and proposed an identity-based blind signature scheme [19]. In 2018, Ye et al. proposed a partial Proxy-BS scheme, which was constructed based on identity and lattice [20]. Although these blind signature schemes are resistant to quantum attacks, they ignore the problem of master key leakage. In 2021, Zhou et al. proposed a lattice-based partial Proxy-BS scheme, which satisfies security such as resistance to master key disclosure attacks and unforgeability [21]. Proxy-BS can provide proxy delegation and anonymous authentication, preserve the privacy of the user, and is widely applied in e-government and blockchain systems. Therefore, we combined an identity-based cryptosystem with proxy technology on a lattice to design an efficient and quantum-resistant Proxy-BS scheme.

In this paper, we propose a post-quantum secure identity-based proxy blind signature (ID-Proxy-BS) scheme on a lattice. We apply the ID-Proxy-BS scheme to e-voting and design a quantum-resistant proxy e-voting system, which achieves multi-regional e-voting and ensures the anonymity of ballot content in e-voting. The contributions of this study are given below:

- To simplify the key management and resistance to quantum attacks, we propose a post-quantum secure identity-based proxy blind signature (ID-Proxy-BS) scheme on a lattice using a matrix cascade technique and lattice cryptosystem. In the proposed ID-Proxy-BS scheme on a lattice, we cascade user identity and the master public key to construct the public key of the lattice signature and generate random parameters through a bimodal Gaussian distribution and rejection sampling algorithm. The ID-Proxy-BS scheme has better security.
- Under the ROM, the security of the ID-Proxy-BS scheme on a lattice is proved under the assumption of the small integer solution (SIS) problem.
- To achieve efficient e-voting, we apply the ID-Proxy-BS scheme on a lattice to e-voting and design a quantum-resistant proxy e-voting system. The system achieves multi-regional e-voting and ensures the anonymity of ballot content in e-voting.

2. Preliminaries

2.1. Lattice Theory

In this section, we define the lattice and a hard problem on the lattice. The specific definitions are below:

Definition 1 (Lattice). *Let $B = \{b_1, b_2, \ldots b_k\}$, in which $b_1, b_2, \ldots b_k \in R^m$ are not correlated with each other. Then, the set of linear combinations of $b_1, b_2, \ldots b_k$ is called lattice Λ; that is,*

$$\Lambda = L(B) = \{c_1 b_1 + c_2 b_2 + \ldots c_k b_k | c_i \in Z\} \tag{1}$$

where B is a basis of $\wedge$ [22].

Let q be a prime number, matrix $B \in Z_q^{n \times m}$ and vector $u \in Z_q^n$. The q-ary lattice of the matrix B and the coset of the lattice $\Lambda_q^{\perp}(B)$ are defined as follows:

$$\Lambda_q^{\perp}(B) = \{Bx = 0 \bmod q | x \in Z^m\} \tag{2}$$

$$\Lambda_q^{u}(B) = \{Bx = u \bmod q | x \in Z^m\} \tag{3}$$

Definition 2 (SIS problem)**.** *Given a real number ω, a prime q, and a matrix $A \in Z_q^{n\times m}$, we solve a vector $y \in z^m$ such that $Ay = 0 \bmod q$ and $\| y \| \leq \omega$ [23].*

Lemma 1. *For arbitrary $A \in Z_q^{n\times m}$, $m > 64 + n\log q/\log(2d+1)$, we randomly choose a vector $x \in \{-d, \ldots, d\}^m$, and with probability $1 - 2^{100}$, we can find another $x' \in \{-d, \ldots, 0, \ldots d\}^m$ that satisfies $Ax = Ax'$ [24].*

2.2. Statistical Distance

Definition 3 (Statistical distance)**.** *Given two random variables $U, V \in S$, the statistical distance between U and V is given by*

$$\Delta(U, V) = \frac{1}{2} \sum_{n\in S} |\Pr[U = u] - \Pr[V = u]| \tag{4}$$

where S is a finite set [13].

2.3. Gaussian Distribution

Definition 4. *Gaussian distribution: For $c > 0$ and $\sigma > 0$, we have a Gaussian function $\rho_{c,\sigma}(x) = e^{-\frac{\pi||x-c||^2}{\sigma^2}}$ centered on c and parameter σ. Then, for any $x \in \wedge$, the Gaussian distribution is $D_{\wedge,\sigma,c}(x) = \frac{\rho_{\sigma,c}(x)}{\rho_{\sigma,c}(\wedge)}$ [25].*

2.4. Trapdoor Generation and Preimage Sampling Algorithm

In this section, two algorithms are mainly introduced, which are the trapdoor generation algorithm and the preimage sampling algorithm [26]. The trapdoor generation algorithm generates a trapdoor of the lattice (i.e., a short base of the lattice), which is usually used as the master private key. The preimage sampling algorithm uses a trapdoor to generate private keys.

Definition 5 (Trapdoor Generation Algorithm)**.** *Let q, m, n be positive integers, where $q \geq 2$ and $m \geq n\log q$. There exists an algorithm $TrapGen(q, m, n)$ that outputs B and a basis $T \in Z^{m\times m}$ of lattice $\Lambda^{\perp}(B)$ such that the distribution of $B \in Z_q^{n\times m}$ is statistically indistinguishable from the distribution of $Z_q^{n\times m}$, and $||\tilde{T}|| \leq O(\sqrt{n\log q})$.*

Definition 6 (Preimage Sampling Algorithm)**.** *Given a matrix B, a trapdoor basis T of lattice $\Lambda^{\perp}(B)$, a target term $u \in Z_q^n$, and $x \geq ||\tilde{T}|| \cdot \omega(\sqrt{\log q})$, there exists a polynomial algorithm $SamplePre(B, T, x, u)$ that outputs a vector $y \in \Lambda^u(B)$, and the distribution of y is statistically close to $G_{\Lambda^u(B),x}$.*

3. Security Model

The proxy blind signature (Proxy-BS) scheme satisfies the blindness and unforgeability of the signature scheme. Blindness primarily considers adversary signers. An adversary signer cannot find an arbitrary message–signature pair by implementing a specific signature algorithm. Unforgeability considers malicious original signers F_1. Next, we prove the security of the scheme through games between an adversary signer and a user, adversary F_1 and the challenger.

3.1. Blindness

The blindness is proved through a game Game_S^{blind} between an adversary signer and two users.

Definition 7 (Blindness)**.** *The scheme satisfies blindness if no adversary S wins the game with non-negligible probability δ. This game Game_S^{blind} is below.*

Game_S^{blind}: *U_1 and U_2 are two users, S is an adversary. The specific process of this game is as follows:*

Setup: We have a random coin $b \in \{0,1\}$, which cannot be known by S. U_1 and U_2 randomly select two messages m_b and m_{1-b}, respectively, and send them to S.

Signature: After S has received the message from U_1 and U_2, S executes the blind signature algorithm with two users $U_1(m_b)$ and $U_2(m_{1-b})$ simultaneously, and finally U_1 and U_2 generate signatures $\sigma(m_b)$ and $\sigma(m_{1-b})$, respectively, and send them to S.

Guess: After S has received the signature from U_1 and U_2, S guesses b.

The adversary S's advantage in winning the above game is $|\Pr[Game_S^{Blind} = 1] - \frac{1}{2}|$, where $\Pr[\text{Game}_S^{Blind} = 1]$ is the probability that $\text{Game}_S^{Blind} = 1$.

3.2. Unforgeability

The Proxy-BS scheme satisfies existential unforgeability under adaptive chosen message attack (EUF-CMA). The EUF-CMA security model has a malicious original signer F_1. F_1 knows the proxy key, but not the proxy signer's private key. We demonstrate the security of the Proxy-BS scheme through a game between the adversary and the challenger.

Definition 8 (EUF-CMA)**.** *The scheme satisfies EUF-CMA security if no adversary F_1 wins the game with non-negligible probability δ. This game Game_{F_1} is given below.*

Game_{F_1}: *T is a challenger, F_1 is an adversary. F_1 knows the proxy key. The specific process of this game is as follows:*

Random oracle queries: F_1 queries the hash value of the message m_i, and T returns the hash result of m_i to F_1.

Signature queries: F_1 queries the signature of the message m_i, T returns signature to F_1.

Forge: F_1 returns a forged signature of a message. If the signature is valid, F_1 wins the game. The advantage of F_1 in winning the game is the probability of returning a valid signature.

4. Identity-Based Proxy Blind Signature Model

This section introduces an identity-based proxy blind signature scheme model, which consists of five algorithms (Setup, KeyGen, ProxyKeyGen, Proxy-BS, Verify) [27]. This algorithm is completed by the interaction between the original signer O-signer, the proxy signer P-signer, and the user User. The specific steps are as follows.

1. $\text{Setup}(1^\lambda) \rightarrow pp$: It inputs security parameters and generates system parameters;
2. $\text{KeyGen}(pp, ID_o, ID_p, \sigma) \rightarrow S_o, S_p$: It inputs system parameters, public keys of O-signer and P-signer, and generates private keys of O-signer and P-signer;
3. $\text{ProxyKeyGen}(pp, ID_o, ID_p, S_o) \rightarrow S$: It inputs system parameters, O-signer's key pair, and P-signer's public key, and generates a proxy key;
4. $\text{Proxy} - \text{BS}(pp, S_p, S, M) \rightarrow c$: It inputs system parameters, message, and P-signer's private key and proxy key, and the algorithm generates a blind signature of the message;
5. $\text{Verify}(pp, ID_o, ID_pM, c) \rightarrow 1$ or 0: It inputs a message and its corresponding blind signature; the algorithm verifies that the signature is valid. If it is, the signature is accepted; otherwise, the signature is rejected.

5. Identity-Based Proxy Blind Signature (ID-Proxy-BS) Scheme on a Lattice

To achieve the anti-quantum attack performance of the proxy blind signature (Proxy-BS) scheme and solve the certificate management problem of the Proxy-BS scheme, this section proposes an identity-based proxy blind signature (ID-Proxy-BS) scheme on a lattice using a matrix cascade technique and lattice cryptosystem. This scheme cascades user identity and the master public key to construct the public key of the lattice signature, and generates random parameters through a bimodal Gaussian distribution and rejection sampling algorithm.

The ID-Proxy-BS scheme on a lattice proposed in this section is shown in Figure 1. There are six entities in the proposed scheme; they are key generation center KGC, user U,

original signer O-signer, proxy signer P-signer, and verifier Verifier. This scheme contains five algorithms; namely, system initialization (Setup), key generation (KeyGen), proxy delegation (ProxyDelegation), proxy key generation (ProxyKeyGen), proxy blind signature (Proxy-BS), and signature verification (Signature Verification). The specific algorithms are as follows.

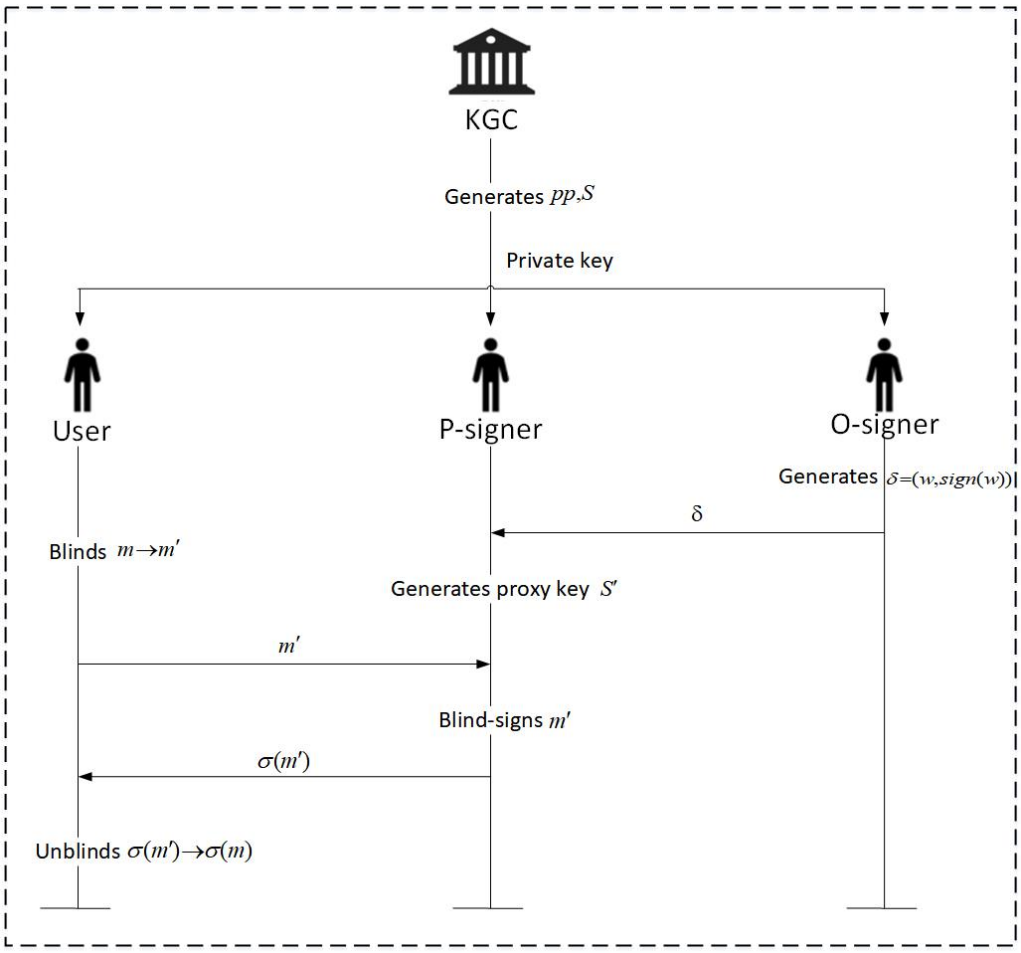

Figure 1. Identity-based proxy blind signature scheme on a lattice.

5.1. Setup

The system initialization generates the system public parameters and hash functions using the parameter setting method of the lattice cryptography, and generates the system master public key and master private key using the trapdoor generation algorithm on a lattice. The specific algorithm is below:

(1) Parameter setting: λ denotes the security parameters, $q = ploy(n)$, $m = O(n \lg q)$, $u = qI_n$, $\sigma \in Z_q^n$.
(2) Hash function settings: $H : \{0,1\}^* \rightarrow Z_{2q}^{n \times m}$, $H_1 : \{0,1\}^* \rightarrow Z_{2q}^{n \times 3m}$.
(3) KGC runs $TrapGen(1^\lambda)$ to generate $A \in Z_{2q}^{n \times m}$ and a basis $S \in Z_{2q}^{m \times n}$ of lattice $\Lambda_{2q}^{\perp}(A)$, where $\| S \| \leq O(\sqrt{n \log q})$.
(4) The public parameter is set to $pp = \{A, H, H_1\}$; the master private key is $msk = S$.

5.2. KeyGen

In this section, the master public key and the user identity are cascaded to construct the user public key, and the user's private key is generated through the preimage sampling algorithm on the lattice. The identities of the original signer O-signer and the proxy signer P-signer are ID_p and ID_o, respectively. The specific algorithm is below:

KGC selects the identity ID_o and ID_p, KGC uses the system's master key to run $S_o \in Z_{2q}^{2m\times n} \leftarrow \text{SamplePre}(A \parallel H(ID_o), S, u, \sigma)$ such that $[A \parallel H(ID_o)]S_o = qI_n (\text{mod} 2q)$ where $\parallel S_o \parallel \leq \sigma\sqrt{2m}$. Similarly, KGC runs $S_p \leftarrow \text{SamplePre}(A \parallel H(ID_p), S, u, \sigma)$. The private keys of O-signer and P-signer are S_o and S_p, respectively.

5.3. ProxyDelegation

The proxy delegation algorithm completes the authorization of O-Signer's signature to P-Signer by generating authorization information through the preimage sampling algorithm on the lattice to sign the authorization certificate. Without loss of generality, this section assumes an authorization certificate, which includes the identity of O-signer, the ID of P-signer, and the proxy authorization period. The specific process is as follows:

(1) After O-signer determines the object for P-signer to authorize, O-signer generates an authorization certificate ω and publishes it.
(2) O-signer runs the algorithm $\delta_1 \leftarrow \text{SamplePre}(A||H(ID_o), S_o, u, H(\omega))$, where $\delta_2 = \omega$. O-signer will send authorization information $\delta = (\delta_1, \delta_2)$ to P-signer.

5.4. ProxyKeyGen

In this section, P-signer generates a proxy key based on the authorization information sent by O-signer through the preimage sampling algorithm on the lattice. The specific algorithm is below:

(1) After P-signer receives δ, it verifies that the equation $[A||H(ID_o)]\delta_1 = qI_n (\text{mod} 2q)$ holds. If the equality holds, P-signer accepts the authorization; otherwise, O-signer re-authorizes.
(2) If Equation (1) holds, P-signer runs $\text{SamplePre}(A||H(ID_o) \parallel H(ID_p), S_p, u, \delta_2)$ to generate a proxy key $S' \in Z_{2q}^{3m\times n}$ such that $[A\|H(ID_q)\|H(ID_p)]S' = qI_n (\text{mod}\, 2q)$ and $\|S'\| \leq \sigma\sqrt{3m}$.

5.5. Proxy-BS

The Proxy-BS algorithm first generates random blinding factors to hide the original message through a bimodal Gaussian distribution, then signs the blinded message through P-signer 's private key and the proxy key, and finally obtains the signature of the original message by removing the blinding factor. This section includes three stages; namely, blinding, proxy blind signature, and unblinding. The specific algorithm is below:

Before the blinding phase, P-signer randomly selects two vectors $r_1 \leftarrow D_{\sigma_2}^{2m}, r_2 \leftarrow D_{\sigma_2}^{3m}$ and computes commitment $x_1 \leftarrow [A \parallel H(ID_p)]r_1, x_2 \leftarrow [A \parallel H(ID_o) \parallel H(ID_p)]r_2$ to U.

5.5.1. Blinding

If a signature is required, user U uses P-signer 's commitment x_1, x_2, blinding factor y_1, y_2, and message m to hash to complete the blinding process. Then, U sends a blind message to P-signer. It is known that m is the message to be blinded. The specific algorithm is as follows:

(1) U randomly selects two blinding factors $y_1 \leftarrow D_{\sigma_3}^{2m}, y_2 \leftarrow D_{\sigma_3}^{3m}$.
(2) U calculates $c_1 \leftarrow H_1(x_1 + [A||H(ID_p)]y_1 \text{ mod } 2q, m)$, $c_2 \leftarrow H_1(x_2 + [A||H(ID_o)||H(ID_p)]y_2 \text{ mod } 2q, m)$.
(3) U selects a bit $b \in \{0, 1\}$.
(4) U computes the blinded message $\mu_1 \leftarrow (-1)^b c_1$, $\mu_2 \leftarrow (-1)^b c_2$.
(5) U sends blind message (μ_1, μ_2) to P-signer.

5.5.2. Proxy Blind Signature

P-signer signs the received blind message (μ_1, μ_2) according to the parameters generated by the preimage sampling algorithm on the lattice. P-signer uses random vector r_1, r_2,

own private key, and proxy key to perform a proxy blind signature and sends the signature (z_1, z_2) to U. The specific algorithm is as follows:

(1) P-signer uses the random vector selected when generating the commitment for the user $r_1 \leftarrow D_{\sigma_2}^{2m}$, $r_2 \leftarrow D_{\sigma_2}^{3m}$.
(2) P-signer calculates the signature $z_1 \leftarrow r_1 + \mu_1 S_p$, $z_2 \leftarrow r_2 + \mu_2 S'$ of the blind message (μ_1, μ_2).
(3) P-signer returns the blind signature (z_1, z_2) to U.

5.5.3. Unblinding

User U receives the blind signature (z_1, z_2) from P-signer and U unblinds the signature to recover the signature of the message m. The specific steps are as follows:

(1) U uses the blinding factor $y_1 \leftarrow D_{\sigma_3}^{2m}$, $y_2 \leftarrow D_{\sigma_3}^{3m}$ selected in the blinding message phase.
(2) U calculates the signature $e_1 \leftarrow y_1 + z_1$, $e_2 \leftarrow y_2 + z_2$ of the original message m.

5.6. Signature Verification

The signature (e_1, e_2) is verified based on the public key of P-signer and O-signer, and the hash values c_1 and c_2 are generated by the user during the blinding. If the signature matches the conditions, it is accepted; otherwise, it is rejected. The signature verification algorithm is shown below:

(1) $\| e_1 \| \leq B_1$, $\| e_2 \| \leq B_2$ (where $B_1 = \eta\sqrt{2m\sigma}$, $B_2 = \eta\sqrt{3m\sigma}$, $\eta \in [1.1, 1.4]$).
(2) $\|e_1\|_\infty \leq q/4$, $\|e_2\|_\infty \leq q/4$.
(3) $c_1 = H_1([A||H(ID_p)]e_1 + qc_1 \bmod 2q, m)$.
(4) $c_2 = H_1([A||H(ID_o)||H(ID_p)]e_2 + qc_2 \bmod 2q, m)$.

If conditions (1), (2), (3), and (4) are met, the signature is valid; otherwise, the signature is invalid.

6. Performance Analysis

6.1. Correctness

In this section, we give proof of correctness for the ID-Proxy-BS scheme on a lattice. When receiving the signature (e_1, e_2), (c_1, c_2), the Verifier first runs the signature verification algorithm to verify that the signature is valid. It judges the four conditions $\| e_1 \| \leq B_1$, $\| e_2 \| \leq B_2$, $\| e_1\|_\infty \leq q/4$, $\| e_2\|_\infty \leq q/4$; if any one of them is not met, the signature is invalid. Otherwise, according to the public key of P-signer and O-signer and the hash value (c_1, c_2) generated by the user during the blinding, the Verifier verifies whether the following two equations are true. The details are as follows:

(1) The Verifier verifies that equation $c_1 = H_1([A||H(ID_p)]e_1 + qc_1 \bmod 2q, m)$ holds:

$$\begin{aligned}
&[A||H(ID_p)]e_1 + qc_1 = [A||H(ID_p)](y_1 + z_1) + qc_1 \\
&= [A||H(ID_p)]y_1 + [A||H(ID_p)]z_1 + qc_1 \\
&= [A||H(ID_p)](r_1 + \mu_1 S_p) + [A||H(ID_p)]y_1 + qc_1 \\
&= [A||H(ID_p)]r_1 + (-1)^b[A||H(ID_p)]S_p c_1 + [A||H(ID_p)]y_1 + qc_1 \\
&= x_1 + (-1)^b qc_1 + qc_1 + [A||H(ID_p)]y_1 \\
&= x_1 + [A||H(ID_p)]y_1 (\bmod 2q)
\end{aligned} \tag{5}$$

(2) The Verifier verifies that equation $c_2 = H_1([A||H(ID_o)||H(ID_p)]e_2 + qc_2 \bmod 2q, m)$ holds:

$$\begin{aligned}
&[A||H(ID_o)||H(ID_p)]e_2 + qc_2 = [A||H(ID_o)||H(ID_p)](y_2 + z_2) + qc_2 \\
&= [A||H(ID_o)||H(ID_p)]y_2 + [A||H(ID_o)||H(ID_p)]z_2 + qc_2 \\
&= [A||H(ID_o)||H(ID_p)](r_2 + \mu_2 S') + [A||H(ID_o)||H(ID_p)]y_2 + qc_2 \\
&= [A||H(ID_o)||H(ID_p)]r_2 + (-1)^b[A||H(ID_o)||H(ID_p)]S'c_2 + [A||H(ID_o)||H(ID_p)]y_2 + qc_2 \\
&= x_2 + (-1)^b qc_2 + qc_2 + [A||H(ID_o)||H(ID_p)]y_2 \\
&= x_2 + [A||H(ID_o)||H(ID_p)]y_2 (\mathrm{mod} 2q)
\end{aligned} \tag{6}$$

If (1) and (2) above are valid, the ID-Proxy-BS scheme on a lattice satisfies correctness.

6.2. Blindness

Theorem 1. *The ID-Proxy-BS on-lattice scheme proposed in this paper satisfies blindness.*

Proof. An adversary signer S cannot obtain useful information from signed messages. Suppose the adversary S, having the advantage $A\mathrm{dv}(S^*)$, interacts with two different users U_0, U_1 to attack our scheme.

Setup: We are given a random coin $b \in \{0, 1\}$, which cannot be known by S. U_1 and U_2 randomly select two messages m_b and m_{1-b}, respectively, and send them to S.

Signature: After S has received the message from U_1 and U_2, S executes the blind signature algorithm with two users $U_1(m_b)$ and $U_2(m_{1-b})$ simultaneously, and finally U_1 and U_2 generate signatures $\sigma(m_b)$ and $\sigma(m_{1-b})$, respectively, and send them to S.

Guess: After S has received the signature from U_1 and U_2, S guesses b.

When performing the proxy blind signature algorithm, due to the random variables, we only need to prove the blinded messages μ and (c, e) and note that since c is the result of a hash function and is randomly generated, we do not have to account for it. The specific analysis process is as follows:

- The distribution of μ. The interaction of adversary S with $\sigma(m_b)$ and $\sigma(m_{1-b})$, respectively, generates μ_b and μ_{1-b}. The statistical distance of μ_b and μ_{1-b} is $\Delta = (\mu_s, \mu_{1-b}) = \frac{1}{2} \sum_{\widetilde{\mu} \in \mathbb{Z}^n} |\Pr(\mu_b = \widetilde{\mu}) - \Pr(\mu_{1-b} = \widetilde{\mu})|$. Since $\mu \leftarrow (-1)^b c$ and it is output with probability $\min(\frac{D^{\mu}_{\sigma_1}(\mu)}{M_1 D^m_{c,\sigma_1(\mu)}}, 1)$, μ_b and μ_{1-b} have the same distribution $D^m_{\sigma_1}$ through the rejection sampling algorithm. The statistical distance satisfies $\Delta(\mu_b, \mu_{1-b})$ = 0, and they are independent of the signed messages, so the adversary S cannot distinguish them.
- The distribution of e. Similar to μ because e_b and e_{1-b} have the same distribution $D^m_{\sigma_2}$ through the rejection sampling algorithm. Their statistical distance satisfies $\Delta(e_b, e_{1-b}) = 0$ and they are independent of signed messages, so the adversary S cannot distinguish them. The final P-signer cannot associate the message with the signatures μ and (c, e).

□

6.3. Unforgeability

Theorem 2. *In the random oracle model, the ID-Proxy-BS on-lattice scheme satisfies EUF-CMA security if no adversary F_1 forges a valid proxy blind signature with a non-negligible advantage ε assuming that the SIS problem is hard.*

Proof. Suppose there is a probabilistic polynomial adversary F_1 who performs q_H hash queries and q_s signature queries, and forges a valid proxy blind signature with non-negligible advantage ε. F_1 outputs the challenge identity ID. The following simulates the interaction between the challenger T and the adversary F_1.

Hash queries: T maintains an initialized empty list L_1 to store the hash value of the message m. F_1 inputs m. T first checks the corresponding tuple in L_1. If it exists, T returns

$(m, H(m))$ to F_1; if not, T chooses $c \leftarrow \{v \in \{-1,0,1\}^k : ||v||_1 \leq k\}$ and selects $e \leftarrow D^m_{\sigma_3}$, with $c = H([A||H(ID)]e + qc \bmod 2q, m)$. T stores (e, c) and returns c to F_1.

Signature queries: T maintains an initialized empty list L_2 to store the signature of the message m. When F_1 sends a query for the signature of the message m, T first checks the corresponding tuple in L_2. If it exists, T returns (m, c, e) to F_1; otherwise, T will run the proxy blind signature algorithm to generate the signature pair (c, e) to F_1.

Forgery: After F_1 decides to end these queries, F_1 outputs a forged signature. T will use this forged signature to solve the SIS problem. Suppose $c = c_j$. There are two possibilities for c_j: one is c_j generated in the signature queries and the other is generated in the hash queries.

When c_j is generated in signature queries, due to the fact that $c = c_j$, then $H([A||H(ID)]e + qc_j, m) = H([A||H(ID)]e' + qc_j, m')$. If $m \neq m'$ or $[A\|H(ID)]e + qc_j \neq [A\|H(ID)]e' + qc_j$, this means that F_1 has found a preimage of c_j. Therefore, $m = m'$, $[A||H(ID)]e + qc_j = [A||H(ID)]e' + qc_j$, and $A(e - e') = 0 \bmod 2q$. Since $e - e' \neq 0$, the SIS problem is solved.

When c_j is generated in hash queries, T records the adversary's forged signatures (e, c_j) on messages m, and selects randomly $c'_t, ..., c'_t \leftarrow B^k$. According to Lemma [18], the probability that F_1 generates a new forged signature $(e', c'_j)(c_j \neq c'_j)$ is $(\varepsilon - \frac{1}{B^n_k})(\frac{q-1/B^n_k}{q_s+q_H} - \frac{1}{B^n_k})$. Since $[A||H(ID)]e - qc_j = [A||H(ID)]e' - qc'_j$, the public key and the private key satisfy $[A||H(ID)]S = qI_n \bmod 2q$; therefore, we can obtain the equation $[A||H(ID)](e - e') = q(c_j - c'_j)I_n \bmod 2q$. Since $c_j \neq c'_j$, we can deduce that $e - e' \neq 0 \bmod 2q$. We know $q(c_j - c'_j) \bmod q = 0$, so $[A||H(ID)](e - e') = 0 \bmod 2q$. It can be seen that we find a non-zero vector v with a probability of at least $\beta = (\frac{1}{2} - 2^{-100})(\varepsilon - \frac{1}{B^n_k})(\frac{q-1/B^n_k}{q_s+q_H} - \frac{1}{B^n_k})$ such that $[A||H(ID)]v = 0$. □

6.4. Efficiency Analysis

In this subsection, we present a comparison with the current literature Refs. [13,18,28]. Assuming that the parameters (n, m, d, k, q, σ) in this paper are the same as those in the existing literature, the specific comparison result will show in Table 1. The parameters of the proposed scheme are set as shown in Table 2.

Table 1. Comparison of the proposed solution w.r.t. to the state-of-the-art.

Document	Public Key Length	Private Key Length	Signature Length
[18]	$3mn \log q$	$3mn \log q$	$(mn + dm) \log(12\sigma)$
[28]	$mn \log(2d + 1)$	$nk \log q$	$2m \log(12\sigma)$
[13]	$mn \log q$	$mk \log q$	$2m \log(12\sigma)$
This article	$mn \log(2q)$	$mn \log(2q)$	$(5m) \log(12\sigma)$

Table 2. Parameter settings.

Parameter	Value
n	512
q	2^{27}
m	13,824
d	1
λ	128
σ_1	64
σ_2	2^{20}
σ_3	2^{30}
Signature length	289.2 KB
Secret key length	24,192 KB
Public key length	24,192 KB

According to Table 1, compared with [18] and [13], the key length and signature length of this scheme are relatively large. The public key length, private key length, and signature length of the ID-Proxy-BS on-lattice scheme are smaller than those in [28].

In this study, we set the security parameter λ to 128 bits. At the same time, we chose appropriate parameters n, q, m to ensure the security of public and private keys. Since the signature obeys the distribution $D^m_{\sigma_3}$, the signature of the proposed scheme in this paper is $(5m)\log(12\sigma_3)$ bits. Based on the specific values of these parameters, we provide the comparison results of our scheme with the current schemes, as shown in Figure 2.

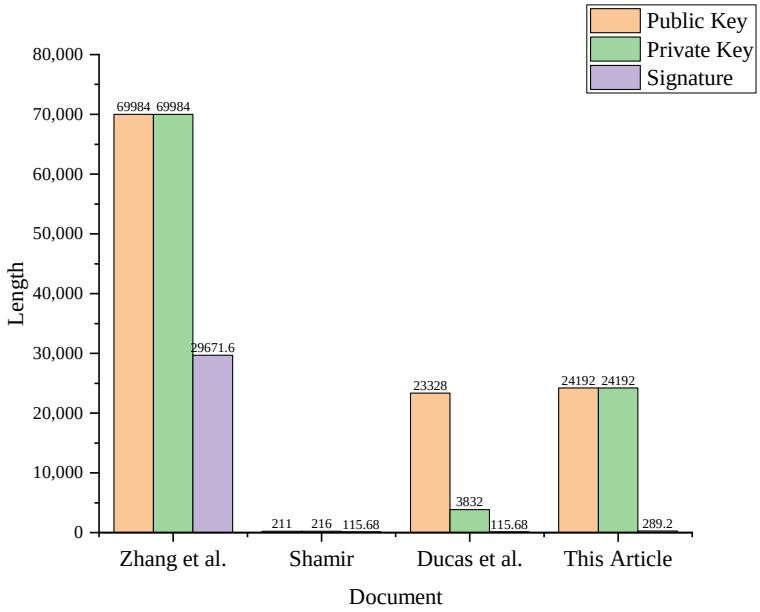

Figure 2. The specific results of the proposed solution compared to the literature Refs. [13,18,28].

7. A Quantum-Resistant Proxy E-Voting System

In this section, first, we give the conditions that a secure e-voting system needs to satisfy. Then, we apply the identity-based proxy blind signature (ID-Proxy-BS) on-lattice scheme to e-voting, and design a quantum-resistant proxy e-voting system. Finally, we perform a performance analysis of the proposed e-voting system.

7.1. Basic Requirements for E-Voting

E-voting has stimulated people's research interest due to its advantages of saving time and effort [29]. When building an e-voting system, it is necessary to ensure the privacy of voters and the accuracy of voting. Therefore, an e-voting system should meet the following basic requirements:

(1) Legitimacy: Only legitimate voters who have passed identity verification can vote.
(2) Anonymity: Except for the voter themselves, no one else knows what the voter voted for.
(3) Verifiability: Every voter can verify whether their votes have been counted correctly.

7.2. A Quantum-Resistant Proxy E-Voting System

The above-mentioned e-voting does not take into account the quantum security and transmission efficiency of ballots during transmission. Therefore, in this section, we apply the identity-based proxy blind signature (ID-Proxy-BS) on-lattice scheme to e-voting, and propose a multi-region proxy e-voting system that is resistant to quantum attacks. The architecture of the e-voting system is shown in Figure 3. There are k constituencies in this system, and each constituency sets up a proxy signature agency and counts votes separately,

thereby improving voting efficiency. Second, the voter hides the content of the ballot in the signature, so that the privacy of the voter is protected. Finally, based on the characteristics of the lattice, the proposed e-voting system can resist quantum attacks.

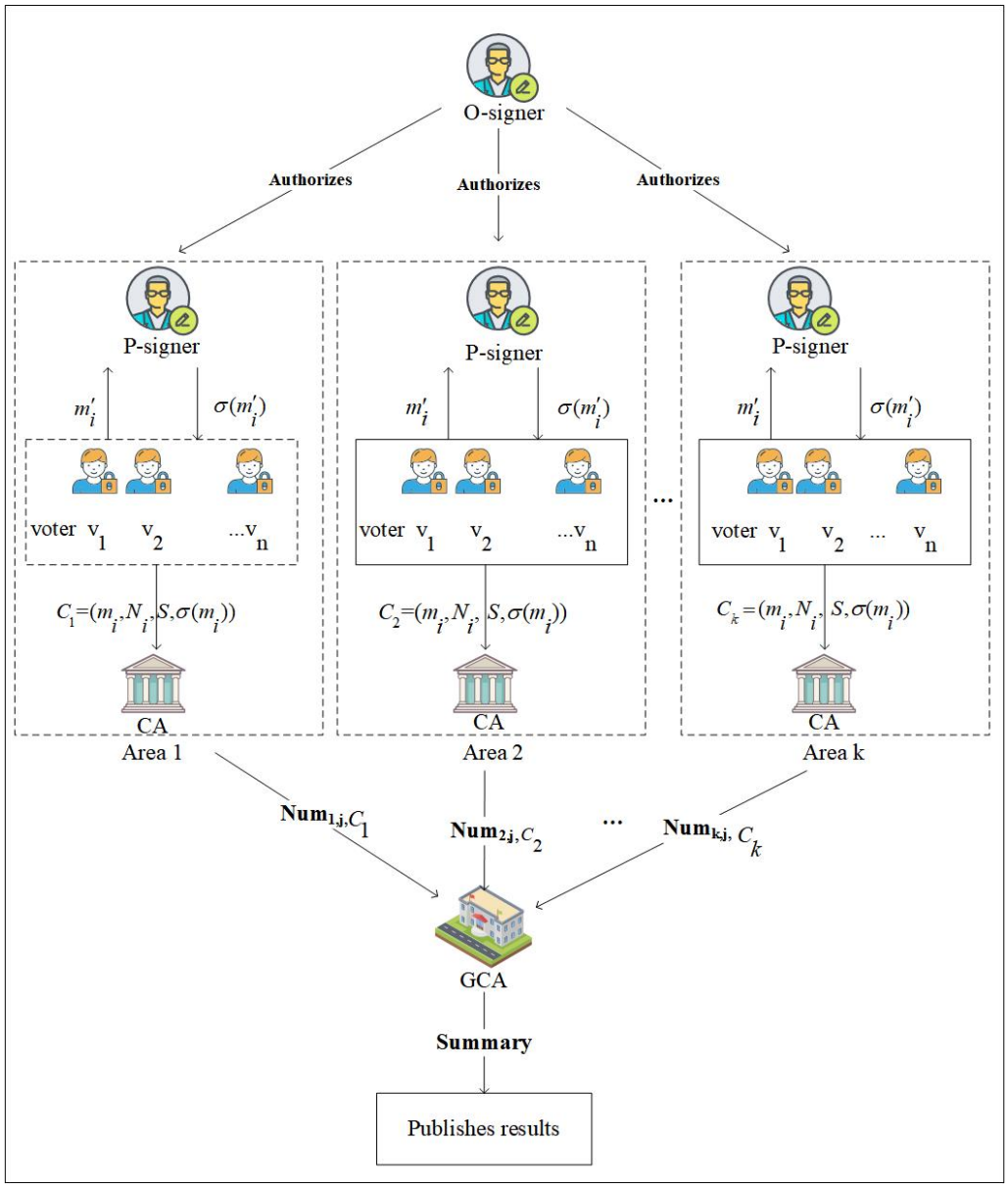

Figure 3. E-voting system based on ID-Proxy-BS on-lattice scheme.

The quantum-resistant proxy e-voting system consists of five entities, which are voters, registration agency, voting agency, counter agency, and general counter agency.

- Voter: A voter; that is, the owner of the content of the ballot.
- Registration agency (RA): The registration agency checks the identity of voters.
- Voting agency: The voting agency signs the voter's ballot to validate that ballot.
- Counter agency (CA): The counter agency is responsible for counting the number of votes in the constituency.
- General counter agency (GCA): The General counter agency is responsible for counting the total votes and publishing the results.

Specifically, the proposed e-voting system in this paper mainly includes four stages: setup, vote writing stage, voting stage, and vote counting stage. Table 3 shows the symbols and definitions used in this system.

Table 3. Symbol definition.

Symbol	Definition
V_i	Voters
ID_i	Identity
RF	Registration form
m_i	Content of the ballot
RA	Registration agency
O-signer	Original signer
P-signer	Proxy signer
CA	Counting agency
GCA	Tallying agency

7.2.1. Setup

Let λ be the security parameters, $q = ploy(n)$, $m \geq 2n \lg q$. Hash function $H : \{0,1\}^* \rightarrow Z_{2q}^{n \times m}$. First, the registration agency RA runs $(A, S) \leftarrow TrapGen(1^n)$ to generate the system's master public key A and master private key S. Then, the RA runs SamplePre$(A \parallel H(ID_i), S, u, \sigma)$ to generate the user's private key. It is known that the public and private key pairs of O-signer and P-signer are (ID_o, S_o) and (ID_P, S_P), respectively. Finally, the RA is responsible for registering every legal voter. The specific process is as follows:

(1) The RA publishes a list of voters and sends the registration form RF to voter V_i who is on the list.
(2) V_i runs $x_i \leftarrow$ SamplePre$(A \parallel H(ID_i), S_i, \sigma)$, then V_i fills in (ID_i, x_i) on RF, and sends RF to the RA.
(3) The RA receives the RE completed by V_i; the RA uses V_i's public key to verify the legitimacy of V_i's identity. If $[A \parallel H(ID_i)]x_i = qI_n \bmod 2q$ and $\parallel x_i \parallel \leq \sigma\sqrt{2m}$, the RA randomly selects a ballot number $N_i \in \{0,1\}^*$ for V_i, and runs $X_i \leftarrow$ SamplePre$(A \parallel H(ID_i)||N_i, S, \sigma)$. The RA sends (ID_i, N_i, X_i) to V_i.
(4) After V_i receives (ID_i, N_i, X_i), V_i uses the RA's public key to verify the legitimacy of the ballot. If $AX_i = qI_n \bmod 2q$ and $\parallel X_i \parallel \leq \sigma\sqrt{3m}$, V_i accepts the ballot number; otherwise, V_i re-applies to the RA for the ballot number.

7.2.2. Vote Writing Stage

Suppose there are n voters $V_1, V_2, \cdots V_n$ and m candidates $C_1, C_2, \cdots C_m$. If V_i wants to vote for candidate C_j, it is recorded as $m_i[j] = 1$; otherwise, $m_i[j] = 0$. V_i fills in the ballot as $m_i = m_i[1]m_i[2] \cdots m_i[m]$.

7.2.3. Voting Stage

In the voting stage, O-signer grants their signing rights to the P-signers of each constituency, and the P-signers of each constituency sign the blinded ballots in the areas under their jurisdiction.

(1) Proxy delegation
After O-signer determines the object P-signer to authorize, it runs ProxyDelegation $(A, H(ID_o), S_o, \omega)$ to generate authorization information $\delta = (\delta_1, \delta_2)$ and sends it to P-signer. After P-signer receives δ, it verifies $[A||H(ID_o)]\delta_1 = qI_n(\bmod 2q)$ whether it is established. If the equality is established, P-signer accepts the authorization, otherwise, O-signer re-authorizes.
(2) Proxy key generation
If the authorization is successful, P-signer runs SamplePre$(A||H(ID_o) \parallel H(ID_p), S_p, u, \delta_2)$ to generate a proxy key $S' \in Z_{2q}^{3m \times n}$.
(3) Blind signature generation
① V_i runs the blinding algorithm to obtain blinded ballots (μ_1, μ_2) of m_i and send (μ_1, μ_2) to P-signer.

② P-signer signs the blinded ballot (μ_1, μ_2) to obtain blinded signature (z_1, z_2) and sends (z_1, z_2) to V_i.
③ V_i unblinds the signature (z_1, z_2) to obtain (e_1, e_2). (m_i, N_i, S, e_1, e_2) is the proxy blind signature of the ballot.

7.2.4. Counting Stage

The voter V_i sends signed ballots (m_i, N_i, S, e_1, e_2) to the counting agency CA. The CA verifies the legitimacy and uniqueness of the ballot; that is, the CA verifies whether ①–④ are established at the same time:
① $\| e_1 \| \leq B_1$, $\| e_2 \| \leq B_2$ (where $B_1 = \eta\sqrt{2m\sigma}$, $B_2 = \eta\sqrt{3m\sigma}$, $\eta \in [1.1, 1.4]$).
② $\|e_1\|_\infty \leq q/4$, $\|e_2\|_\infty \leq q/4$.
③ $c_1 = H_1([A||H(ID_p)]e_1 + qc_1 \bmod 2q, m)$.
④ $c_2 = H_1([A||H(ID_o)||H(ID_p)]e_2 + qc_2 \bmod 2q, m)$.

If the verification passes and the ballot number N_i is unique, the CA accepts the ballot; otherwise, the CA discards it. After the voting is completed, the CA first calculates the voting results of all voters V_i for each C_j; then, the CA calculates the number of votes $m_1[j] + m_2[j] + \cdots + m_n[j]$ for each C_j. Finally, the CA of each constituency sends the number of votes $Num_{k,j}$ of C_j and signed ballots C_k=(m_i, N_i, S, e_1, e_2) to GCA to summarize and publish the voting results.

7.3. Performance Analysis

The e-voting system proposed in this paper has the following characteristics.

(1) Legality. Before voting, every voter must be registered and verified by the RA before becoming a legal voter. In the registration phase, the voter V_i registers using their own identity ID_i and signs with their own private key, i.e., (ID_i, x_i). Even if an adversary fills in the registration information to pretend to be a voter, they cannot know the private key S_i of the voter. Since the SIS problem is a hard problem, the adversary cannot forge x_i to be a legitimate voter.
(2) Anonymity. In the voting stage, V_i can obtain P-signer's blind signature through the ID-Proxy-BS scheme. Therefore, the e-voting system proposed in this paper enables anonymous voting by voters, and no one can associate the vote with the voter except the voter themselves.
(3) Efficiency: In the e-voting system proposed in this paper, O-signer grants signature rights to the P-signer for each constituency by region, and the P-signers for each constituency sign the blinded ballots for the region under their jurisdiction at the same time, thus increasing the efficiency of voting.
(4) Verifiability. ① In the registration stage, V_i obtains the unique ballot number N_i. ② The total number of signed ballots (m_i, N_i, S, e_1, e_2) and the total number of ballots $m_1[j] + m_2[j] + \cdots m_n[j]$ of C_j published on the electronic bulletin board by the CA can be used by voters to verify that the ballot papers have been counted.

In the e-voting system proposed in this section, voters hide the content of the ballot in their signatures and realize anonymous voting. In large-scale elections, setting up agencies for each district improves the efficiency of e-voting. Based on the characteristics of a lattice, the proposed e-voting system can resist quantum attacks. Therefore, the e-voting system proposed in this paper is anonymous, efficient, and resistant to quantum attacks.

8. Conclusions

In this paper, to simplify key management and resist quantum attacks, we have proposed a post-quantum secure identity-based proxy blind signature (ID-Proxy-BS) scheme on a lattice using a matrix cascade technique and lattice cryptosystem. In the proposed scheme, firstly, we cascaded the user identity and the master public key to construct the public key of the lattice signature, and generated random parameters through a bimodal Gaussian distribution and rejection sampling algorithm. Then, the security of the ID-Proxy-BS scheme was proved based on the SIS problem under the ROM. Finally, we applied

the scheme to e-voting, and designed a quantum-resistant proxy e-voting system. The system enables multi-regional electronic voting and satisfies anonymity, high efficiency, and anti-quantum attack.

Author Contributions: Writing—review, editing, methodology, and validation, F.L.; writing—original draft, methodology, and formal analysis, M.Y.; methodology and formal analysis, Z.S.; validation and resources, P.W.; formal analysis and validation, G.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Ohkubo, M.; Miura, F.; Abe, M.; Fujioka, A.; Okamoto, T. An Improvement on a Practical Secret Voting Scheme. In *Lecture Notes in Computer Science, Proceedings of the Information Security, Second International Workshop, ISW'99, Kuala Lumpur, Malaysia, 6–7 November 1999*; Mambo, M., Zheng, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1729, pp. 225–234. [CrossRef]
2. Amit, K.; Sunder, L. Proxy Blind Signature Scheme. 2003. Available online: http://eprint.iacr.org/2003/072 (accessed on 1 July 2023).
3. Juels, A.; Luby, M.; Ostrovsky, R. Security of Blind Digital Signatures (Extended Abstract). In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, CA, USA, 17–21 August 1997*; Kaliski, B.S., Jr., Ed.; Springer: Berlin/Heidelberg, Germany, 1997; Volume 1294, pp. 150–164. [CrossRef]
4. Pointcheval, D.; Stern, J. Security Arguments for Digital Signatures and Blind Signatures. *J. Cryptol.* **2000**, *13*, 361–396. [CrossRef]
5. Burt, K. RSA Digital Signature Scheme. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 1061–1064. [CrossRef]
6. Liu, W.; Tong, F.; Luo, Y.; Zhang, F. A proxy blind signature scheme based on elliptic curve with proxy revocation. In Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Washington, DC, USA, 30 July–1 August 2007; pp. 99–104. [CrossRef]
7. Jun, X.X.; Jin, P.; Zhen, X.G. New proxy signature scheme based on Schnorr signature scheme. *J. Chongqing Univ. Posts Telecommun.* **2005**, *17*, 742–744.
8. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
9. Ajtai, M. Generating Hard Instances of Lattice Problems (Extended Abstract). In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; Miller, G.L., Ed.; ACM: New York, NY, USA, 1996; pp. 99–108. [CrossRef]
10. Hoffstein, J.; Pipher, J.; Silverman, J.H. NSS: An NTRU Lattice-Based Signature Scheme. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, 6–10 May 2001*; Pfitzmann, B., Ed.; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2045, pp. 211–228. [CrossRef]
11. Hoffstein, J.; Howgrave-Graham, N.; Pipher, J.; Silverman, J.H.; Whyte, W. NTRUSIGN: Digital Signatures Using the NTRU Lattice. In *Lecture Notes in Computer Science, Proceedings of the Topics in Cryptology—CT-RSA 2003, the Cryptographers' Track at the RSA Conference 2003, San Francisco, CA, USA, 13–17 April 2003*; Joye, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2003; Volume 2612, pp. 122–140. [CrossRef]
12. Gentry, C.; Peikert, C.; Vaikuntanathan, V. Trapdoors for hard lattices and new cryptographic constructions. In Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, BC, Canada, 17–20 May 2008; Dwork, C., Ed.; ACM: New York, NY, USA, 2008; pp. 197–206. [CrossRef]
13. Ducas, L.; Durmus, A.; Lepoint, T.; Lyubashevsky, V. Lattice Signatures and Bimodal Gaussians. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—CRYPTO 2013—33rd Annual Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2013*; Canetti, R., Garay, J.A., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8042, pp. 40–56. [CrossRef]
14. Zhang, L.; Ma, Y. A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model. *Math. Probl. Eng.* **2014**, *2014*, 307637. [CrossRef]
15. Gu, J.; Cao, X.Y.; Fu, Y.; He, Z.W.; Yin, Z.J.; Yin, H.L.; Chen, Z.B. Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **2022**, *67*, 2167–2175. [CrossRef] [PubMed]
16. Yin, H.L.; Fu, Y.; Li, C.L.; Weng, C.X.; Li, B.H.; Gu, J.; Lu, Y.S.; Huang, S.; Chen, Z.B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2023**, *10*, nwac228. [CrossRef] [PubMed]

17. Rückert, M. Lattice-Based Blind Signatures. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—ASIACRYPT 2010—16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, 5–9 December 2010*; Abe, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2010; Volume 6477, pp. 413–430. [CrossRef]
18. Li, F.; Liu, Z.; Li, T.; Ju, H.; Wang, H.; Zhou, H. Privacy-aware PKI model with strong forward security. *Int. J. Intell. Syst.* **2022**, *37*, 10049–10065. [CrossRef]
19. Gao, W.; Hu, Y.; Wang, B.; Xie, J. Identity-Based Blind Signature from Lattices in Standard Model. In *Lecture Notes in Computer Science, Proceedings of the Information Security and Cryptology—12th International Conference, Inscrypt 2016, Beijing, China, 4–6 November 2016*; Revised Selected Papers; Chen, K., Lin, D., Yung, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; Volume 10143, pp. 205–218. [CrossRef]
20. Ye, Q.; Zhou, J.; Tang, Y. Identity-based Against Quantum Attacks Partially Blind Signature Scheme from Lattice. *Netinfo Secur.* **2018**, *18*, 46. [CrossRef]
21. Zhou, Y.; Dong, S.; Yang, Y.Y. A Lattice-based Identity-based Proxy Partially Blind Signature Scheme in the Standard Model. *Netinfo Secur.* **2021**, *21*, 37–43. [CrossRef]
22. Micciancio, D. Lattice-Based Cryptography. In *Encyclopedia of Cryptography and Security*, 2nd ed.; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 713–715. [CrossRef]
23. Ajtai, M. Generating Hard Instances of Lattice Problems. *Electron. Colloquium Comput. Complex.* **1996**, *TR96-007*, 99–108.
24. Lyubashevsky, V. Lattice Signatures without Trapdoors. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology— EUROCRYPT 2012—31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012*; Pointcheval, D., Johansson, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 738–755. [CrossRef]
25. Micciancio, D.; Regev, O. Worst-Case to Average-Case Reductions Based on Gaussian Measures. *SIAM J. Comput.* **2007**, *37*, 267–302. [CrossRef]
26. Bellare, M.; Neven, G. Multi-signatures in the plain public-Key model and a general forking lemma. In Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS 2006, Alexandria, VA, USA, 30 October–3 November 2006; Juels, A., Wright, R.N., di Vimercati, S.D.C., Eds.; ACM: New York, NY, USA, 2006; pp. 390–399. [CrossRef]
27. Micciancio, D.; Peikert, C. Trapdoors for Lattices: Simpler, Tighter, Faster, Smaller. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—EUROCRYPT 2012—31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, 15–19 April 2012*; Pointcheval, D., Johansson, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; Volume 7237, pp. 700–718. [CrossRef]
28. Shamir, A. Identity-Based Cryptosystems and Signature Schemes. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, CA, USA, 19–22 August 1984*; Blakley, G.R., Chaum, D., Eds.; Springer: Berlin/Heidelberg, Germany, 1984; Volume 196, pp. 47–53. [CrossRef]
29. Chaum, D. Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—EUROCRYPT '88, Workshop on the Theory and Application of of Cryptographic Techniques, Davos, Switzerland, 25–27 May 1988*; Günther, C.G., Ed.; Springer: Berlin/Heidelberg, Germany, 1988; Volume 330, pp. 177–182. [CrossRef]