Article

A Lattice-Based Blind Signature Using BLISS

Haifei Zhou * and Weihuang Wen

Posted Date: 30 September 2025

doi: 10.20944/preprints202509.2568.v1

Keywords: lattice; blind signature; BLISS; group signature

 doi:10.20944/preprints202509.2568.v1

Article

A Lattice-Based Blind Signature Using BLISS

Haifei Zhou * and Weihuang Wen

Department of Cybersecurity, Jinan University, Guangzhou, China
* Correspondence: haiferz11@gmail.com

Abstract

This paper proposes an efficient lattice-based blind signature scheme built upon the BLISS framework. By incorporating bimodal Gaussian distributions and rejection sampling techniques, the scheme ensures secure output distributions and prevents information leakage during the signing process. It achieves blindness and one-more unforgeability with only two rounds of interaction, significantly improving efficiency compared to earlier multi-round lattice-based blind signature schemes. Performance analysis demonstrates that the scheme maintains relatively compact parameters, with a public key size of about 20KB, a private key size of 99KB, and a signature size of 120KB. These characteristics make it practical for post-quantum secure environments. Overall, the proposed scheme combines provable security, anonymity, and efficiency, and is well-suited for privacy-preserving applications such as blockchain systems, electronic voting, and anonymous payments.

Keywords: lattice; blind signature; BLISS; group signature

1. Introduction

Blind signature, first proposed by Chaum in [1] involves the interaction between the user and the signer. The user first blinds the signed message to the signer, the signer signs the processed message and returns it to the user. The signer cannot get any information about the user-signed message while the user can get the signature of any signed message. David and Stern [2] defined the concept of blind signature security in 1996. They showed that blind signatures need to satisfy Blindness and Onemore-Unforgeability. Lyubashevsky designed a provably secure lattice-based one-time signature scheme in [3], and then designed lattice-based standard digital signature schemes in [4] . The schemes in [4] are based on the Fiat-Shamir framework. The overall scheme is efficient.In addition, Gentry, Peikert, and Vaikuntanathan designed a digital signature scheme [5], called GPV signature. The security of GPV signature relies on one-way trapdoor functions on lattices, which are also used by many later public-key cryptographic algorithms.

In this paper, we present an efficient lattice-based blind signature scheme that generates the signature after two rounds, providing protection against quantum attacks and ensuring user anonymity. On the other hand, we improve the bimodal signature (BLISS) into a blind version [6], so that we can use it in some other scenarios such as blockchain. We refer to [7–9] to understand the blind technology used. Besides, we provide a blind scheme from group users' vision. Currently, there has been no exploration of group blind signatures in the lattice context. By far there are only a few group blind signature schemes without lattice. Group signature provides anonymity to group members who sign messages. A group of users jointly create a public key that is used to verify signatures. Each user has a secret key that is used to generate signatures on behalf of the group. We utilized the lattice problem to provide another version of our scheme. This means that we can allow multiple blind signature users to be organized into a group and appoint a manager for administration. This new technology is rare in previous schemes and primarily addresses the needs of distributed systems. The earliest proposal was introduced by C. Popescu et al. in [10], though the scheme's security is at risk of being compromised in the future, concerning quantum attacks. W. Kong et al. in [11] applied group blind signatures to

 doi:10.20944/preprints202509.2568.v1

privacy protection in smart grids. R. Xu et al. presented a Quantum group blind signature scheme in [12], but it is not resistant to quantum attacks. Our scheme, however, is the first group blind signature scheme on the lattice by far.

The main contributions of our paper are as follows:

1. We change the form of the bimodal signature into a lattice blind signature. Our scheme is round-optimal and based on Module-LWE and Module-SIS problems. We use a rejection sampling technique on it. The scheme satisfies blindness and one-more unforgeability, which ensures the signature is unique. To prove the blindness, we proved the blinding description satisfies CPA-security first.
2. Compared with other schemes, our scheme is more efficient and provides a more stabilized signature size. However, the scheme is more complex in the user-signer interaction process.

2. Preliminaries and Techniques

In this paper, we use lowercase bold letters to represent vectors and uppercase bold letters to represent matrices. The ℓ_q-norm of a vector is defined as $\|\boldsymbol{a}\|_q = \sqrt[q]{\sum_i |a_i|^q}$and the $\ell_\infty = \max_i \|\boldsymbol{a}_i\|$, where q is a small prime. In a matrix, for $\boldsymbol{A} \in \mathbb{Z}^{n\times m}$, $\|\boldsymbol{A}\|_\infty = \max\limits_{1\le i\le m} \sum\limits_{j=1}^{n} |a_{ij}|$. By default, we use $\|\cdot\|$ for the ℓ_2-norm.

We denote $\mathbb{Z}_p$ to be the ring of integers modulo p.

We use polynomial rings $\mathcal{R} := \mathbb{Z}[x]/(X^n+1)$ and $\mathcal{R}_q := \mathbb{Z}[x]_q/(X^n+1)$, where each coefficient is taken modulo q. $\boldsymbol{I}_n$ represents n-dimension identity matrix.

Note that $\boldsymbol{b} \leftarrow \boldsymbol{B}$, where $\boldsymbol{b}$ is a column vector, denotes $\boldsymbol{b}$ is randomly taken from matrix $\boldsymbol{B}$. $U[c,d]$ represents a uniform distribution over the interval $[c,d]$.] $\boldsymbol{a}$ is another vector, $\langle \boldsymbol{a}, \boldsymbol{b}\rangle$ and $\boldsymbol{a}\cdot\boldsymbol{b}$ mean $\boldsymbol{a}$ inner product $\boldsymbol{b}$.

2.1. Lattices

Given a set of n linearly independent vectors $\boldsymbol{b}_1$,$\boldsymbol{b}_2$,$\cdots$,$\boldsymbol{b}_n$ in $\mathbb{Z}^n$, the lattice Λ generated by these vectors is defined as:

$$\Lambda = \{\sum_{i=1}^{n} a_i b_i | \boldsymbol{a}_i \in \mathbb{Z}\}$$

Given $\mathbb{A} \in \mathbb{Z}^n$, a vector $\boldsymbol{u} \in \mathbb{Z}_q^n$ and a prime number q , we define two types of lattices:

$$\Lambda_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^n | \boldsymbol{A}\boldsymbol{e} = \boldsymbol{0} \mod q\}$$
$$\Lambda_q^{\boldsymbol{u}}(\boldsymbol{A}) = \{\boldsymbol{e} \in \mathbb{Z}^n | \boldsymbol{A}\boldsymbol{e} = \boldsymbol{u} \mod q\}$$

2.2. Discrete Bimodal Gaussian Distribution

For a d-dimensional lattice, a center point $\boldsymbol{c} \in \mathbb{R}^d$, and a standard deviation parameter $\sigma > 0$, a probability distribution ρ over $\Lambda_{\mathbf{c}}$, where $\Lambda_{\mathbf{c}} = \{\boldsymbol{x} \in \Lambda \mid \|\boldsymbol{x}-\boldsymbol{c}\|_2 \le \alpha\sigma\}$ is the set of discrete lattice points within a d-dimensional sphere of radius $\alpha\sigma$ centered at $\boldsymbol{c}$, and α is a constant. The discrete Gaussian distribution is often used in lattice-based cryptography to define encryption schemes and security parameters. The discrete Gaussian distribution on a lattice with center point $\mathbf{c}$ and deviation σ is given by:

$$\rho_{\mathbf{c},\sigma}(x) = \frac{1}{Z_\sigma} \exp\left(-\frac{\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{2\sigma^2}\right),$$

where Z_σ is the normalization constant, defined as:

$$Z_\sigma = \sum_{x\in\Lambda} \exp\left(-\frac{\pi\|\boldsymbol{x}-\boldsymbol{c}\|^2}{2\sigma^2}\right).$$

Here, Λ is the lattice over which the distribution is defined, and $\boldsymbol{x}$ is a lattice point.

 doi:10.20944/preprints202509.2568.v1

Next, we give the following definition for transforming a discrete Gaussian distribution into a bimodal Gaussian distribution through processing.

We set two variance parameters σ_1 and σ_2 and a $\Lambda \subseteq \mathbb{Z}^d$, a center point $\boldsymbol{c} \in \mathbb{R}^d$, and variance parameters $\sigma_1, \sigma_2 > 0$. The lattice fits the double-sided Gaussian distribution.

The distribution Λ on a lattice has properties where a random point in Λ moves in two random directions with σ_1 and σ_2 variance, respectively, and arrives at a random point following a double-sided Gaussian distribution. In an n-dimensional Euclidean space, given two points $\boldsymbol{c}_1, \boldsymbol{c}_2$ and variance parameters σ_1, σ_2, the bimodal Gaussian distribution function on the lattice is defined as:

$$\mathcal{D}_{\Lambda,\boldsymbol{c}_1,\boldsymbol{c}_2,\sigma_1,\sigma_2}(x) = \frac{1}{Z}\left(e^{-\frac{\|x-\boldsymbol{c}_1\|^2}{2\sigma_1^2}} + e^{-\frac{\|x-\boldsymbol{c}_2\|^2}{2\sigma_2^2}}\right),$$

where $\boldsymbol{x} \in \Lambda_{\boldsymbol{c}_1,\boldsymbol{c}_2}, \|\boldsymbol{x}-\boldsymbol{c}_1\|_\infty \leq \sqrt{n}\sigma_1, \|\boldsymbol{x}-\boldsymbol{c}_2\|_\infty \leq \sqrt{n}\sigma_2$ and Z is the normalization constant[6].

$\mathcal{D}_{\Lambda,\boldsymbol{c}_1,\boldsymbol{c}_2,\sigma_1,\sigma_2}(x)$ shares some properties with the discrete Gaussian distribution, for example, its contour can be seen as the lattice points on the level curves of $\mathcal{D}(\Lambda_{\boldsymbol{c}_1,\boldsymbol{c}_2})$ on $\Lambda_{\boldsymbol{c}_1,\boldsymbol{c}_2}$. Moreover, it also satisfies classical Gaussian distribution properties such as the 3σ rule.

2.3. Rejection Sampling

Suppose we want to generate samples from a target probability density function $f(x)$. Let $g(x)$ be another probability density function such that $f(x) \leq Mg(x)$ for all x, where M is a known constant. We sample x according to Algorithm 1:

Algorithm 1 Rejection Sampling

Input: Target probability density function $f(x)$, bimodal Gaussian proposal distribution $g(x)$, constant M such that $f(x) \leq Mg(x)$ for all x
Output: Sample x from $f(x)$

1: **repeat**
2: Sample x_0 from $g(x)$
3: Sample u from $U[0,1]$
4: **if** $u \leq \frac{f(x_0)}{Mg(x_0)}$ **then**
5: Accept x_0 as a sample and exit loop
6: **end if**
7: **until** sample is accepted

2.4. Blind Signatures

A general form of blind signature model typically consists of the following four entities:

- *Message owner (User)* $\mathcal{U}$: possesses the message to be signed and desires to obtain the signature.
- *Signer* $\mathcal{S}$: holds the signing key and can sign the message.
- *Random number generator*: used to generate random numbers to ensure the security of the protocol.
- *Verifier*: verifies the validity of the signature.

We use four steps to describe the interaction among these entities:

- *Key Generation* (1^n) given the security parameter n, then generate a key pair (pk,sk), which represents the public key and secret key.
- *Signature Protocol* The message owner $\mathcal{U}$ uses a random number generator to generate a blinding factor that blinds the message $e \in \mathcal{M}$, where $\mathcal{M}$ is the message space. Then the owner sends the blinded message e^* to the signer. Then, the signer $\mathcal{S}$ signs the blinded message with the signing key sk and sends the signed message z^* back to the message owner. Upon receiving z^*, the user $\mathcal{U}$ unblinding the signature z, then outputs an ordered pair (z, e) as the final signature.
- *Verification* The verifier could use the public key pk to verify the validity of the signature.

 doi:10.20944/preprints202509.2568.v1

3. New Blind Signature

3.1. Overview

In this section, we will introduce our blind signature scheme, which has the advantage of being provably secure while avoiding using zero-knowledge proof technology. Additionally, it utilizes a bimodal Gaussian distribution to enhance parameter security. Our main innovation lies in upgrading the BLISS scheme into a blind signature scheme. The first step is to construct a scheme with a trapdoor x to be a blinding and unblinding technique. Then encrypt the message μ with b sending to the signer (v,v'). The reason for resulting two vectors rather than one is because of the encrypting algorithm we use. Recieving a message pair (v,v'), the signer using his secret key S to sign the blinding message,computes $G = Dp + v$ and $g = dp + v'$, where p is a prim. We set $d = Dx \ mod \ 2q$ in the begining.

The signer then uses G, g, and the signing algorithm to compute λ_1 and λ_2. The algorithm includes a bimodal Gaussian. Upon receiving λ_1 and λ_2, the user uses sk x to get one part of the signature z, and H to compute $c = H(Ay \ mod \ 2q, \mu)$, H is a hash function based on the lattice, we will introduce it in detail later. After publishing the signature pair (z, c), the public could verify the signature using the public key A. Then if $z' = (Az + q\mathbf{c} \ mod 2q \ , \mu)$ and $z' = c$, the signature is then proven to be trustworthy.

Our scheme requires only a 20KB public key size, a 99KB private key size, and a 120KB signature size.

The way we use it in the group vision is that we set different private keys for each user. In more detail, our main aim is to ensure that each *Group User* possesses distinct D_i, d_i, x_i and y_i. The *Group Manager*'s method for tracking user trapdoors is y_i. If the algorithm succeeds, it indicates that the user possesses the corresponding y_i. Furthermore, we have also computed the potential space requirements for this scheme. The space needed for the manager to store is 1889KB, and it increases linearly with the number of users in the group. This is because each user has a fixed-size key to store, and as the number of users increases, the total number of keys required also increases.

3.2. New Blind Signature and Verification Algorithms

In this subsection, we denote integers n and m, and a large prime q. Additionally, we model the hash function H as a random oracle.

Key Generation: We sample a matrix $S \leftarrow \mathbb{Z}_{2q}^{m \times n}$, and the public key is made of $A \leftarrow \mathbb{Z}_{2q}^{n \times m}$ such that $AS \equiv q\mathbf{I}_n \pmod{2q}$. This implies that $AS = A(-S) \equiv q\mathbf{I}_n \pmod{2q}$. The detailed steps are shown in Algorithm 2

Algorithm 2 Key Generation

1: $S \leftarrow \mathbb{Z}_{2q}^{m \times n}$
2: $A \leftarrow \mathbb{Z}_{2q}^{n \times m}$
3: $AS \equiv q\mathbf{I}_n \pmod{2q}$
4: $x \leftarrow \{-\gamma, \ldots, \gamma\}^n, \gamma \leftarrow \{-2, -1, 0, 1, 2\}$
5: $D \leftarrow \mathbb{Z}_q^{n \times m}$
6: $d \equiv x^T \cdot D \pmod{q_1}$
7: $pk = (D, d), sk = x$
8: $PK = A, SK = S$
9: **return** $(pk, sk), (PK, SK)$

Blinding algorithm: The user needs to blind the message before sending it to the signer. The user chooses a random vector $r \in \mathbb{Z}^n$ and blinds the message to produce (v, v') and D, d, which will be sent to the signer. The detailed steps are shown in Algorithm 3.

 doi:10.20944/preprints202509.2568.v1

Algorithm 3 Blinding algorithm

1: **Input:** Message μ, $pk = (\boldsymbol{D}, \boldsymbol{d})$, $\boldsymbol{r} \in \mathbb{Z}^m$, $\boldsymbol{e}\{-\gamma, \ldots, \gamma\}^n \times \{-\gamma, \ldots, \gamma\}^m, e' \leftarrow \{-\gamma, \ldots, \gamma\}$
2: **Output:** $(\boldsymbol{v}, v')$ and $\boldsymbol{D}, \boldsymbol{d}$ to be sent to the signer.
3: $(\boldsymbol{v}, v') = \text{enc}(pk, \mu) = (\boldsymbol{Dr} + \boldsymbol{e}, \boldsymbol{dr} + e' + \mu)$
4: **return** $(\boldsymbol{v}, v')$ and $\boldsymbol{D}, \boldsymbol{d}$

Signing algorithm: In this phase, when the signer recieves $(\boldsymbol{v}, v')$ and $\boldsymbol{D}, \boldsymbol{d}$, he gengerates (λ_1, λ_2) as the blinding signature. Before sending it back, the signer needs to do a rejection sampling algorithm to protect the secret key S with the accept advantage p_λ. We set M_1 which is defined as follows, as the possibility of rejection sampling.

$$M_1 = \frac{1}{M} \exp\left(-\frac{\|\boldsymbol{Sg}\|}{2\sigma^2}\right)^2 \cosh\left(\frac{\langle \lambda_1, \boldsymbol{Sg} \rangle}{\sigma^2}\right)$$

The detailed steps are shown in Algorithm 4.

Algorithm 4 Signing algorithm

1: **Input:** $\boldsymbol{D}, \boldsymbol{d}$, SK, PK and $(\boldsymbol{v}, v')$
2: **Output:** (λ_1, λ_2)
3: $\boldsymbol{y} \leftarrow \{-\gamma, \ldots, \gamma\}^m \times \{-\gamma, \ldots, \gamma\}^n, y'\{-\gamma, \ldots, \gamma\}$, p is an arbitrary prime. $b_1, b_2 \leftarrow \{0, 1\}$
4: $\boldsymbol{G} = \boldsymbol{D}p + \boldsymbol{v}, \boldsymbol{g} = \boldsymbol{d}p + v'$
5: $\lambda_1 = (-1)^{b_1}\boldsymbol{SG} \mod 2q$, $\lambda_2 = (-1)^{b_2}\boldsymbol{Sg} + y' \mod 2q$
6: continue with posibility M_1.
7: **return** (λ_1, λ_2)

Unblinding algorithm: In this phase, the user implements the unblinding algorithm to generate the signature $\langle \boldsymbol{z}, \boldsymbol{c} \rangle$ with the probability of rejection sampling. We set M_2 as the possibility of rejection sampling.

$$M_2 = \frac{1}{M} \exp\left(-\frac{\|\mu \boldsymbol{S}\|}{2\sigma^2}\right)^2 \cosh\left(\frac{\langle \boldsymbol{z}, \mu \boldsymbol{S} \rangle}{\sigma^2}\right)$$

The detailed steps are shown in Algorithm 5.

Algorithm 5 Unblinding algorithm

1: **Input:** (λ_1, λ_2), $sk : x, \boldsymbol{A}, \boldsymbol{y}$
2: **Output:** $\langle \boldsymbol{z}, \boldsymbol{c} \rangle$
3: $\boldsymbol{z} = x\lambda_2 - \lambda_1 = (-1)^{b_1+b_2}\mu \boldsymbol{S} + \boldsymbol{y} \mod 2q$
4: Perform Rejection sampling on $\boldsymbol{z}$, coutinue with posibility M_2.
5: $\boldsymbol{c} = H(\boldsymbol{Ay} \mod 2q, \mu)$
6: **return** $\langle \boldsymbol{z}, \boldsymbol{c} \rangle$

$(-1)^{b_1+b_2}$ indicates an uncertain value that can be either +1 or -1, where $b_3 \in \{0, 1\}$. However, this does not affect the result because it will be eliminated when we use the rejection sampling algorithm with a bimodal Gaussian distribution. As mentioned earlier, if b_3 is -1, it cleverly turns into a positive value through $\mod 2q$, and the same applies if it is 1.

Verify algorithm: When the signature is published, the verifier can implement the following algorithm to check its validity. We set $\boldsymbol{T} = q\boldsymbol{I}_n$ as in Section 3 The detailed steps are shown in Algorithm 6.

 doi:10.20944/preprints202509.2568.v1

Algorithm 6 Verify algorithm

1: **Input:** Message μ, Public Key $PK : \boldsymbol{A}$, Blind Signature $\langle \boldsymbol{z}, \boldsymbol{c} \rangle$
2: **Output:** Reject or accept
3: **if** $\|\boldsymbol{z}\| > \frac{q}{4}$ **then**
4: **return** Reject;
5: **else if** $\|\boldsymbol{z}\| > \boldsymbol{B}_2$ **then**
6: **return** Reject;
7: **else if** $\boldsymbol{z}' = H(\boldsymbol{A}\boldsymbol{z} + \boldsymbol{T}\mu \mod 2q, \mu)$ and $\boldsymbol{z}' = \boldsymbol{c}$. **then**
8: **return** Accept;
9: **end if**

The correctness of the proposed scheme needs to be verified. We assume that the verifier receives the signature $\langle \boldsymbol{z}, \boldsymbol{c} \rangle$. The verifier then runs the Algorithm 6 to determine its legality. We assume $\|\boldsymbol{z}\| \leq \frac{q}{4}$ and $\|\boldsymbol{z}\| \leq \boldsymbol{B}_2$. If these conditions are not met, the verifier rejects it. The verifier then uses the public key to execute the algorithm, and the detailed steps are as follows:

$$\begin{aligned} \mathbf{z}' &= H(\boldsymbol{A}\boldsymbol{z} + \boldsymbol{T}\mu \mod 2q, \mu) \\ &= H((-1)^{b_3}\mu\boldsymbol{A}\boldsymbol{S} + \boldsymbol{A}\boldsymbol{y} + \boldsymbol{T}\mu \mod 2q, \mu) \\ &= H(\boldsymbol{A}\boldsymbol{y} \mod 2q, \mu) \\ &= \mathbf{c} \end{aligned} \tag{1}$$

As we know $\boldsymbol{A}\boldsymbol{S} = q\boldsymbol{I}_n$, so if we set $b_3 = 1$, $-\mu\boldsymbol{A}\boldsymbol{S} + \boldsymbol{T}\mu \mod 2q = \mathbf{0}$. If $b_3 = 0$, $\mu\boldsymbol{A}\boldsymbol{S} + q\boldsymbol{I}_n\mu \mod 2q = 2q\mu \mod 2q = \mathbf{0}$. Therefore, we can verify the correctness of the scheme.

4. Conclusion

In this work, we proposed a lattice-based blind signature scheme derived from the BLISS framework. By leveraging bimodal Gaussian distributions and rejection sampling techniques, our scheme provides provable security against quantum adversaries while ensuring the essential properties of blindness and one-more unforgeability. A notable advantage of the construction is its round-optimal design, requiring only two communication rounds, which significantly improves efficiency compared to previous lattice-based blind signature schemes.

Our parameter analysis further demonstrates that the scheme achieves a favorable balance between security and practicality. With a public key size of about 20KB and a signature size of 120KB, the scheme is compact enough for real-world deployment. These properties make it a promising candidate for applications in blockchain, electronic voting, and anonymous payment systems, where both privacy protection and post-quantum security are critical.

References

1. D. Chaum, "Blind signatures for untraceable payments," in *Advances in Cryptology: Proceedings of Crypto 82*. Springer, 1983, pp. 199–203.
2. A. H. Eid and A. Ismail, "An analytical review on lattice-based cryptography," in *Journal of Physics: Conference Series*, vol. 3075, no. 1. IOP Publishing, 2025, p. 012013.
3. V. Lyubashevsky and D. Micciancio, "Asymptotically efficient lattice-based digital signatures," in *Theory of Cryptography: Fifth Theory of Cryptography Conference, TCC 2008, New York, USA, March 19-21, 2008. Proceedings 5*. Springer, 2008, pp. 37–54.
4. V. Lyubashevsky, "Fiat-shamir with aborts: Applications to lattice and factoring-based signatures," in *Advances in Cryptology–ASIACRYPT 2009: 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings 15*. Springer, 2009, pp. 598–616.
5. K. de Boer and W. van Woerden, "Lattice-based cryptography: A survey on the security of the lattice-based nist finalists," 2025.
6. L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal gaussians," in *Advances in Cryptology–CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*. Springer, 2013, pp. 40–56.

 doi:10.20944/preprints202509.2568.v1

7. V. Lyubashevsky, N. K. Nguyen, M. Plancon, and G. Seiler, "Shorter lattice-based group signatures via "almost free" encryption and other optimizations," in *Advances in Cryptology–ASIACRYPT 2021: 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6–10, 2021, Proceedings, Part IV 27*. Springer, 2021, pp. 218–248.
8. S. Bouaziz-Ermann, S. Canard, G. Eberhart, G. Kaim, A. Roux-Langlois, and J. Traoré, "Lattice-based (partially) blind signature without restart," *Cryptology ePrint Archive*, 2020.
9. N. Alkeilani Alkadri, R. El Bansarkhani, and J. Buchmann, "Blaze: practical lattice-based blind signatures for privacy-preserving applications," in *Financial Cryptography and Data Security: 24th International Conference, FC 2020, Kota Kinabalu, Malaysia, February 10–14, 2020 Revised Selected Papers 24*. Springer, 2020, pp. 484–502.
10. C. Popescu, "A secure and efficient group blind signature scheme," *Studies in Informatics and Control*, vol. 12, no. 4, pp. 269–276, 2003.
11. W. Kong, J. Shen, P. Vijayakumar, Y. Cho, and V. Chang, "A practical group blind signature scheme for privacy protection in smart grid," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 29–39, 2020.
12. R. Xu, L. Huang, W. Yang, and L. He, "Quantum group blind signature scheme without entanglement," *Optics Communications*, vol. 284, no. 14, pp. 3654–3658, 2011.