An efficient and secure ID-based multi-proxy multi-signature scheme based on lattice

Rahim Toluee[1], Taraneh Eghlidos[2]

[1]Department of Electrical Engineering, Sharif University of Technology, Tehran, Iran

[2]Electronics Research Institute, Sharif University of Technology, Tehran, Iran

[1]rtoluee@ee.sharif.edu, [2]teghlidos@sharif.edu

Abstract

Multi-proxy multi-signature schemes are useful in distributed networks, where a group of users cooperatively could delegate their administrative rights to the users of another group, who are authorized to generate the proxy signatures cooperatively on behalf of the original signers. In this paper, we aim to propose an ID-based lattice-based multi-proxy multi-signature (ILMPMS) scheme, which enjoys security against quantum computers and efficiency due to ID-based framework, linear operations and possibility of parallel computations based on lattices. For this purpose, we first propose an ID-based lattice-based multi-signature scheme, used as the underlying signature in our ILMPMS scheme. We prove existential unforgeability of both schemes against adaptive chosen-message attack in the random oracle model based on the hardness of the learning with errors problem over standard lattices.

Keywords: multi-proxy multi-signature scheme, multi-signature scheme, ID-based signature, lattice-based signature, learning with errors problem.

1 Introduction

Multi-proxy multi-signature schemes are useful in distributed networks, where a group of users could delegate their administrative rights to the users of another group. As another instance consider the case where a large number of users have some complaints against some internet service providers. The users could delegate a group of lawyers to pursue the complaints on their behalf through the multi-proxy multi-signature scheme.

The concept of proxy signature scheme is useful in cases when an original signer wishes to delegate his/her signing rights to the other one, called a proxy signer. The first proxy signature scheme was introduced by Mambo et al. in 1996 [1] and [2]. Several proxy signature schemes and their variants have been proposed using classical methods of cryptography including integer factorization, discrete logarithm and elliptic curve-based methods [3-7]. The advent of quantum computers in the near future threatens

security of the existing public-key cryptosystems such as RSA [8] and ElGamal [9], because of vulnerability of integer factorization and discrete logarithm problems with respect to Shor's polynomial time quantum algorithms [10]. Lattice-based cryptography is one of the important branches of post-quantum cryptography that benefits from provable security based on worst-case intractability of the lattice hard problems and conjectured security against quantum computers [11] and [12], following the pioneering work of Ajtai [13]. Besides, lattice-based algorithms take advantage of simplicity and relatively efficient linear operations and possibility of parallel computations [44]. Since then, there are some lattice-based proxy signature schemes such as lattice-based identity-based (ID-based) proxy signature [14], lattice-based multiple grade proxy signature [15] and lattice-based ID-based proxy blind signature [16].

Proxy signatures can be categorized into three groups including proxy multi-signature, multi-proxy signature and multi-proxy multi-signature, based on the number of original signers and proxy signers involved.

The concept of proxy multi-signature (PMS) scheme is useful in cases when a group of original signers wish cooperatively to delegate their signing rights to a proxy signer. The first proxy multi-signature scheme was introduced by Yi et al. in 2000 [17]. Several proxy multi-signature schemes and their variants have been proposed using classical methods of cryptography [18-20]. Wang and Cao proposed an ID-based proxy multi-signature scheme in 2007 [21] and Shao showed the vulnerability of their scheme [22]. In 2009, Cao and Cao proposed an ID-based proxy multi-signature scheme with formal definition and security model for the first time [23]. In 2012, Anand and Padhye proposed an ID-based proxy multi-signature scheme using random oracle model [24]. However, their scheme is not secure in the security model they used.

Multi-proxy signature (MPS) scheme was first introduced by Hwang and Shi in 2000 [25]. It is useful when a group of proxy signers are authorized to generate the proxy signatures cooperatively on behalf of an original signer. Several multi-proxy signature schemes and their variants have been proposed using classical methods of cryptography [18], [26-28].

The extension of the previous scenarios leads to the concept of multi-proxy multi-signature (MPMS) schemes, where a group of original signers wish to delegate their signing rights to a group of proxy signers. The first multi-proxy multi-signature scheme introduced by Hwang and Chen in 2004 [29]. Several multi-proxy multi-signature schemes and their variants have been proposed using classical methods of cryptography [30-34].

In some multi-proxy multi-signature schemes such as [35-36], the proxy signers should cooperate with the original signers in the multi-delegation generation phase. In our opinion, this extra cooperation reduces the bandwidth efficiency of their scheme and on the other hand it is only expected that the original signers be involved in the multi-delegation generation phase.

Asaar et al., in 2014 proposed an ID-based multi-proxy multi-signature (IMPMS) scheme without bilinear pairings [37]. Besides, they showed that the scheme proposed in [20] and [34] are not secure in the underlying security models. However, the scheme

proposed in [37] could be non-interactive. Anand and Padhye, in 2015 proposed a secure IMPMS scheme in random oracle model [38]. However, it seems that their scheme suffers from the leakage of the original signers' private keys.

In this paper, we focus on the IMPMS, to achieve bandwidth efficiency and avoid the heavy public key infrastructure in real scenarios because of large number of users involved. Hence, we propose a provable secure ID-based lattice-based multi-proxy multi-signature (ILMPMS) scheme in the random oracle model, based on standard assumptions. To the best of our knowledge, the proposed scheme is the first ID-based lattice-based one which enjoys security against quantum computers and efficiency due to ID-based framework, linear operations and possibility of parallel computations based on lattices.

In this paper, we first propose an ID-based lattice-based multi-signature (ILMS) scheme. We use the proposed ILMS scheme as the underlying signature to propose an ILMPMS scheme. The proposed ILMS scheme is based on LWE problem over standard lattices in the random oracle model. In the proposed ILMS scheme, we use Bai-Galbraith's scheme as the underlying signature [39].

We note that, El Bansarkhani and Sturm proposed the first lattice-based multi-signature scheme in 2016 [40]. Their interactive multi-signature scheme is relied on the signature scheme of Güneysu et al. [41]. The proposed scheme in [40] is provable secure in the random oracle model based on ideal lattice problems using Forking Lemma. However, Forking Lemma in general is an obstacle in quantum security proof [42].

Roadmap: The rest of this paper is organized as follows. Section 2 deals with preliminaries. The proposed signature models and security requirements are given in Sections 3 and 4, respectively. Sections 5 and 6 embrace the proposed ILMS scheme and its security analysis, respectively. Section 7 is devoted to our proposed ILMPMS scheme. The security analysis of the proposed ILMPMS scheme is given in Section 8. Finally, Section 9 draws all the points together and gives concluding remarks.

2 Preliminaries

2.1 Notations

The Euclidean norm is denoted by $\|.\|$. We denote by $\|.\|_\infty$ the infinity norm. The ring $\mathbb{Z}_q$, for a positive integer q, represents the set of integers in the interval $[-\frac{q}{2}, \frac{q}{2})$. We use uppercase letters for matrices and by the length of a matrix we mean the largest norm of its columns. A vertical bar is used for horizontal concatenation of vectors and matrices. The notation $\lceil . \rfloor_d$ indicates dropping the d least significant bits and $[c]_{2^d}$ is the unique integer in the set $(-2^{d-1}, 2^{d-1}]$ such that $c \equiv [c]_{2^d} (\, mod\ 2^d)$.

The standard notations $\mathcal{O}(.)$ and $\omega(.)$ used to describe asymptotic growth rates and $\tilde{\mathcal{O}}(.)$ and $\tilde{\omega}(.)$ indicate hiding the logarithmic factors. In a polynomial time algorithm the running time is upper bounded by $\mathcal{O}(l^k)$, where l is the input size of the algorithm and k is a constant value. We represent the negligible function by $negl\ (n)$, where for every $c > 0$ there is an integer n_c such that for all $n > n_c$ the inequality $|negl\ (n)| < n^{-c}$ holds [43].

2.2 Lattices and the hard problems

Definition 1 (lattice) [44]**:** An m-dimensional lattice is generally a subspace of $\mathbb{R}^m$. An integer lattice $\mathcal{L}$ with a basis $B = \{b_1, b_2, \cdots, b_n\} \in \mathbb{Z}_q^{m\times n}$ is a subspace of $\mathbb{Z}^m$ ($n \leq m$), where

$$\mathcal{L}(B) = \mathcal{L}(b_1, \cdots, b_n) = \{Bx | x \in \mathbb{Z}^n\} = \{\sum_{i=1}^{n} x_i b_i : x_i \in \mathbb{Z};\ 1 \leq i \leq n\} \quad (1)$$

The integers m and n are called the dimension and the rank of the lattice, respectively. A lattice basis is not unique and for any unimodular matrix U, $U \in \mathbb{Z}^{n\times n}$ with determinant ± 1, $B.U$ is another basis of $\mathcal{L}(B)$.

For the rest of this paper we consider integer lattices and use simply "lattice" instead of "integer lattice".

Definition 2 (fundamental parallelepiped) [44]**:** For a lattice with a basis $B = \{b_1, b_2, \cdots, b_n\} \in \mathbb{Z}_q^{m\times n}$, the fundamental parallelepiped is $\mathcal{P}_{1/2}(B) = \{\sum_{i=1}^{n} x_i b_i : -1/2 \leq x_i < 1/2\}$.

Definition 3 (Gram-Schmidt orthogonalization) [44]**:** For a given set of linearly independent vectors $B = \{b_1, \dots, b_n\}$, the corresponding Gram-Schmidt algorithm outputs the orthogonal linearly independent vectors $B^* = \{b_1^*, b_2^*, \dots, b_n^*\}$, where

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{i,j} b_j^*\ ;\ \mu_{i,j} = \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle} \quad 1 \leq i \leq n \quad (2)$$

Definition 4 (q-ary lattice) [11]**:** A lattice $\mathcal{L}$ is called q-ary if $q\mathbb{Z}^n \subseteq \mathcal{L} \subseteq \mathbb{Z}^n$, for some integer q. For a matrix $B \in \mathbb{Z}_q^{m\times n}$ and some integers q, m and n ($n \leq m$), the corresponding q-ary lattices with dimension m are as follows:

$$\mathcal{L}_q(B) = \{y \in \mathbb{Z}^m : y = Bs \bmod q \ for\ some\ s \in \mathbb{Z}^n\} \quad (3)$$

$$\mathcal{L}_q^{\perp}(B) = \{y \in \mathbb{Z}^m : B^T y = 0 \bmod q\} \quad (4)$$

Gaussian heuristic [11]**:** The number of variables in $\mathcal{L}_q^{\perp}(B) \cap [-\alpha, \alpha]^m$ is approximated by the so-called Gaussian heuristic as follows:

$$\left|\mathcal{L}_q^{\perp}(B) \cap [-\alpha, \alpha]^m\right| = \frac{vol\ ([-\alpha, \alpha]^m)}{\det(\mathcal{L}_q^{\perp}(B))} = \frac{(2\alpha + 1)^m}{q^n}$$

Definition 5 (Shortest Vector Problem (SVP) and $GapSVP$) [45]**:** for a given lattice basis B, SVP is the problem of finding the shortest nonzero vector in $\mathcal{L}(B)$. SVP_γ is the problem of finding a nonzero vector $v \in \mathcal{L}(B)$ in the approximation variant of SVP, where $\gamma = \gamma(n) \geq 1$ is the approximation factor, such that

$$\|v\| \leq \gamma \min_{w \in \mathcal{L}(B)\setminus\{0\}} \|w\| \quad (5)$$

Let $\lambda_1(\mathcal{L})$ be the length of the shortest nonzero vector in $\mathcal{L}(B)$. $GapSVP_\gamma$ is the decisional variant of SVP_γ determining either $\lambda_1(\mathcal{L}) \leq r$ or $\lambda_1(\mathcal{L}) > \gamma r$, for $r > 0$ [12].

There is neither classical nor quantum polynomial time algorithm known to approximate the above-mentioned problems to within polynomial approximation factor γ [12] and [46].

Definition 6 (statistical distance) [47]**:** The statistical distance between two distributions A and B over a countable domain D is $\frac{1}{2}\sum_{d\in D}\|\mathrm{A}(d)-\mathrm{B}(d)\|$. Two distributions are statistically close if their statistical distance is negligible.

Definition 7 (discrete Gaussian distribution) [48]**:** The continuous Gaussian distribution over $\mathbb{R}^m$ with mean c and real standard deviation $s>0$ has the following density function

$$\rho_{s,c}^{m}(\mathrm{x})=\left(\frac{1}{\sqrt{2\pi s^2}}\right)^{m} e^{\frac{-\|x-c\|^2}{2s^2}} \tag{6}$$

Therefore, $\rho_{s,c}^{m}(\mathbb{Z}^m)=\sum_{z\in\mathbb{Z}^m}\rho_{s,c}^{m}(z)$. Discrete Gaussian distribution over $\mathbb{Z}^m$ and over a lattice $\mathcal{L}$ are defined as follows, respectively

$$D_{s,c}^{m}(\mathrm{x})=\rho_{s,c}^{m}(\mathrm{x})/\rho_{s,c}^{m}(\mathbb{Z}^m) \tag{7}$$

$$\forall x\in\mathcal{L}, D_{\mathcal{L},s,c}(x)=\rho_{s,c}^{m}(\mathrm{x})/\rho_{s,c}^{m}(\mathcal{L}) \tag{8}$$

Definition 8 (smoothing parameter) [12] and [47]**:** Informally, the smoothing parameter of an m-dimensional lattice $\mathcal{L}$ is the minimum positive s to blur the discreteness of the corresponding lattice, which has the following bound

$$\eta_{\epsilon}(\mathcal{L})\le\min_{B}\|B^*\|\sqrt{\log(2m(1+1/\epsilon))/\pi} \tag{9}$$

Where B is a basis of the lattice $\mathcal{L}$, $\|B^*\|$ is the length of the corresponding Gram-Schmidt orthogonalized matrix, $m\ge 2nlog\ q$ and ϵ is a real positive number. Therefore, there is a negligible $\epsilon(n)$ where

$$\eta_{\epsilon}(\mathcal{L})\le\min_{B}\|B^*\|\,\omega(\sqrt{\log m}) \tag{10}$$

Theorem 1 [47]**:** On inputs a basis $B\in\mathbb{Z}_q^{n\times m}$ of the lattice $\mathcal{L}$, parameters $c\in\mathbb{R}^m$ and a real $r\ge\|B^*\|.\omega(\sqrt{\log m})$, there is a probabilistic polynomial-time (PPT) algorithm that outputs a sample from a distribution statistically close to $D_{\mathcal{L},r,c}$. Besides, for $\mathrm{x}\leftarrow D_{\mathcal{L},r,c}$ the following assertion holds

$$Pr\{\|\mathrm{x}-c\|>r\sqrt{m}\}\le negl(m) \tag{11}$$

Definition 9 (ring-SIS problem) [12]**:** Consider the ring R, we define $R_q=R/qR$. Given an arbitrary vector $a\in R_q^m$ and $\beta>0$, $ring-SIS_{q,m,\beta}$ is to find a non-trivial vector $z\in R^m$ such that $\|z\|\le\beta$ and $a^t.z=0\in R_q$.

Definition 10 (decisional learning with errors (LWE) problem) [12]**:** Let n,m,q be positive integers, $s\in\mathbb{Z}_q^n$, and χ be a discrete Gaussian distribution of width αq for some $\alpha<1$. $A_{s,\chi}$ is the LWE distribution which outputs $(a,<a,s>+\mathrm{e}\ (mod\ q))\in\mathbb{Z}_q^n\times\mathbb{Z}_q$, where $a\overset{R}{\leftarrow}\mathbb{Z}_q^n$ and $\mathrm{e}\leftarrow\chi$. For given arbitrarily many samples from $\mathbb{Z}_q^{n+1}$, the

decisional-LWE problem distinguishes whether the samples are distributed uniformly or from the LWE distribution for some fixed vector s.

The hardness of LWE is maintained even if LWE has short secrets, where the secret vector s is sampled according to the error distribution χ [49]. LWE problem is at least as hard as solving $GapSVP_\gamma$ in the worst case, for $q \geq 2^{n/2}$ and $\gamma = \tilde{O}(n/\alpha)$ [50] and [12].

Definition 11: Let n, m, q be positive integers, $s \in \mathbb{Z}_q^n$, and χ be a discrete Gaussian distribution of width αq for some $\alpha < 1$, $a \xleftarrow{R} \mathbb{Z}_q^n$ and e $\leftarrow \chi$. We say that $\text{LWE}_{n,m,q,\alpha}$ is ϵ-hard, if for any PPT algorithm $\mathcal{A}$, $\Pr\{s \leftarrow \mathcal{A}(a, < a, s > + \text{e } (mod\ q))\} \leq \epsilon$, for any negligible ϵ.

Definition 12 (trapdoor basis) [47]**:** A trapdoor basis T of a lattice for signature generation corresponds to a random basis B (as the public key) from an appropriate distribution. The length of the Gram-Schmidt vectors of the trapdoor basis is relatively short.

There are efficient PPT algorithms $TrapGen(1^n)$ that output a basis $B \in \mathbb{Z}_q^{n \times m}$ statistically close to the uniform and a trapdoor basis $T \in \mathbb{Z}_q^{m \times m}$ for $\mathcal{L}_q^\perp(B)$, on inputs positive integers $n, q \geq 2$ and $m = \mathcal{O}(n \log q)$ [51] and [52].

Definition 13 (preimage-samplable trapdoor functions (PSFs)) [12] and [47]**:** PSFs include the following PPT algorithms:

- $(B, T) \leftarrow TrapGen(1^n)$, where B is used to compute efficiently $f_B: D_n \longrightarrow R_n$, and T is used as a trapdoor.
- $DomSample\ (1^n)$ chooses a point x from D_n such that the distribution of $f_B(x)$ is uniformly over R_n.
- $PreSample\ (B, T, y)$ computes a preimage $x \leftarrow f_B^{-1}(y)$, given $f_B(x) = y$ for any y chosen uniformly from R_n.

Micciancio and Peikert proposed a new method for trapdoors generation [53], which is very simple and fast in the generation phase, also parallel, mostly offline and practical in the inversion phase. Compared to [47] and [51-52], their scheme enjoys from smaller and tighter parameters m and r, and smaller key size. They use a fixed, structured and public matrix $G \in \mathbb{Z}_q^{n \times m_1}$, nominated as "gadget matrix" for which solving the LWE problem is easy. The matrix G is randomized with a unimodular matrix to generate a matrix $A \in \mathbb{Z}_q^{n \times m}$, statistically close to the uniform. Computing f_A^{-1} is reduced to f_G^{-1} with the trapdoor matrix T along with pre-/post-processing.

Theorem 2 [53]**:** Given positive integers $n, q \geq 2$, $m_1 = n \log q$, $m_2 \geq n \log q$, $m = m_1 + m_2$ and a matrix $\bar{A} \in \mathbb{Z}_q^{n \times m_2}$, there is an efficient PPT algorithm $TrapGen(\bar{A})$ which outputs a basis $A \in \mathbb{Z}_q^{n \times m}$ statistically close to the uniform, and a trapdoor basis $T \in \mathbb{Z}_q^{m_2 \times m_1}$, where:

$$A = [\bar{A}|G] \begin{bmatrix} I & -T \\ 0 & I \end{bmatrix} = [\bar{A}|G - \bar{A}T] \tag{12}$$

$TrapGen(1^n)$ could be used when $\bar{A}$ is chosen randomly from uniform distribution.

Theorem 3 [53]**:** Let $s(T)$ be the largest singular value of the matrix T, $s' = \sqrt{s(T)^2 + 1}$ and $f_G(s, e) = Gs + e \bmod q$, where G is a gadget matrix. Consider that the algorithm correctly computes $f_G^{-1}(s', e')$ for any $e' \in \mathcal{P}_{1/2}(qB^{-t})$, for some B. Let $b = f_A(s, e)$ for any s and e $\leftarrow D_{\mathbb{Z}^m, \alpha q}$, where $1/\alpha \geq 2\|B\|s'.\omega(\sqrt{\log n})$. There is a PPT algorithm $Invert\ (A, T, b)$ that outputs s and e, on inputs a basis $A \in \mathbb{Z}_q^{n \times m}$, a trapdoor basis $T \in \mathbb{Z}_q^{m_2 \times m_1}$ for A and b with overwhelming probability, where $m_1 = n \log q, m_2 \geq n \log q, m = m_1 + m_2$.

Definition 14 (the $Check$ (.) algorithm) [54]**:** For the given E, consider E_r as the r^{th} row of the matrix E. The function $\max_k(E_r)$ outputs the k^{th} largest element of the given vector. Output of the $Check\ (E)$ algorithm is false if for any row of E, $\sum_{k=1}^{\omega} \max_k(E_r)$ is greater than some bound L, otherwise the output is true.

3 The proposed signature models

3.1 Model of ID-based lattice-based multi-signature (ILMS) schemes

Consider there are N signers with identity set $ID_S = \{ID_{S1}, \dots, ID_{SN}\}$. An ILMS scheme consists of the following algorithms.

Table 1. Algorithms of ILMS scheme

Algorithm	Input(s)	Output(s)
Setup	the system security parameter	system parameters and master private/public key pair
Key Extraction	the system parameters, the master private key, the master public key and a user identity ID_i	user's private key sk_i
MS Generation	the system parameters, the master public key, a message μ, the signers' identity set ID_S, the signers' private keys $sk_i, i \in \{1, \dots, N\}$, and the partial signature of the co-signers* *This is an interactive algorithm between signers to sign the message μ.	multi-signature σ_s on μ
MS Verification	the system parameters, the master public key, the signers' identity set ID_S and their multi-signature σ_s on μ	"accept" if σ_s is valid, and "reject" otherwise

3.2 Model of ID-based lattice-based multi-proxy multi-signature (ILMPMS) schemes

Consider there are M original signers and N proxy signers with identity sets $ID_O = \{ID_{O1}, \dots, ID_{OM}\}$ and $ID_P = \{ID_{P1}, \dots, ID_{PN}\}$, respectively. An ILMPMS scheme consists of the following algorithms.

Table 2. Algorithms of ILMPMS scheme

Algorithm	Input(s)	Output(s)
Setup	the system security parameter	system parameters and master private/public key pair
Key Extraction	the system parameters, the master private key, the master public key and a user identity ID_i	user's private key sk_i
MD Generation	the system parameters, the master public key, a warrant w, the original signers' identity set ID_O, the original signers' private keys $sk_i, 1 \leq i \leq M$, and the partial signature of co-original signers* *This is an interactive algorithm between original signers to sign the warrant w.	multi-delegation signature σ_w on w
MD Verification	the system parameters, the master public key, the original signers' identity set ID_O and multi-delegation signature σ_w on w	"accept" if σ_w is valid, and "reject" otherwise
ILMPMS Generation	the system parameters, the master public key, a message μ, the warrant w, the proxy signers' identity set ID_P, the original signers' identity set ID_O, the proxy signers' private keys $sk_i, i \in \{1, \dots, N\}$, multi-delegation signature σ_w on w, and the partial signature of co-proxy signers* *This is an interactive algorithm between proxy signers to sign the message μ.	ILMPMS σ on μ
ILMPMS Verification	the system parameters, the master public key, the proxy signers' identity set ID_P, the original signers' identity set ID_O, the warrant w and ILMPMS σ on μ	"accept" if σ is valid, and "reject" otherwise

4 Security requirements

4.1 Existential unforgeability of ILMS schemes

In the security model, it is assumed w.l.o.g. that there is only one honest signer. Existential unforgeability of ILMS schemes requires that forging a valid multi-signature on a chosen message by an adversary be difficult, even if the adversary has obtained the private keys of the signers except for the honest signer, and some other valid multi-signatures on its chosen messages. Consider the following game for a formal definition of existential unforgeability against a PPT adversary in an ILMS scheme.

1. Let l be the game parameter. The system parameters, the master private/public key pair and users' private keys are generated. Let the identities of the signers, the system parameters and the master public key are given to the adversary.

2. Throughout the entire game, the adversary is able to make ILMS generation queries of the form (t, ID_S, μ), where t is the index of an honest signer such that $ID_{S,t} \in ID_S$

and μ is the message to be signed. A challenger simulates a valid $\sigma_s \leftarrow Sig(sk_{S,t}, \mu, ID_S)$.

3. The adversary has also access to a corrupt oracle $Corrupt(.)$, which on input $ID_{S,i}$ returns $sk_{S,i}$.

4. The adversary Outputs $(\mu^*, \sigma_{\mu^*}, ID_{S^*})$ and succeeds if the following conditions are satisfied:

- It never queried (t, ID_{S^*}, μ^*), for any t.
- One of the identities in ID_{S^*} is not in the set of the corrupted users.
- $Vrfy(\mu^*, \sigma_{\mu^*}, ID_{S^*}) = 1$.

Definition 15. We say that an ILMS scheme is existential unforgeable against adaptive chosen-message attack if no PPT adversary has a non-negligible advantage in the above game.

4.2 Existential unforgeability of ILMPMS schemes

In the security model, it is assumed w.l.o.g. that there is only one honest signer. Existential unforgeability of ILMPMS schemes requires that forging a valid multi-proxy multi-signature on a chosen message by an adversary be difficult, even if the adversary has obtained the private keys of the signers except for the honest signer, and some other valid multi-proxy multi-signatures on its chosen messages. To discuss the unforgeability of ILMPMS schemes, we categorize the adversaries into three types according to different resources they can get.

Type1: The adversary has only identities of the original signers and proxy signers.

Type2: The adversary has private keys of the original signers and proxy signers except for the honest proxy signer, besides identities of the original signers and proxy signers.

Type3: The adversary has private keys of the proxy signers and original signers except for the honest original signer, besides identities of the original signers and proxy signers.

It can be found that if an ILMPMS scheme is existential unforgeable against Type2 and Type3 adversaries, it is also existential unforgeable against Type1 adversary.

a. Existential unforgeability against Type2 adversary

By existential unforgeability against Type2 adversary of ILMPMS schemes, we mean that it is difficult for an adversary to forge a valid ILMPMS on a message of its choice, even if it has obtained the private keys of the original signers and proxy signers except for the honest proxy signer, and some other valid multi-proxy multi-signatures on its chosen messages. Consider the following game for a formal definition of existential unforgeability against a PPT Type2 adversary in an ILMPMS scheme.

1. Let l be the game parameter. The system parameters, master private/public key pair and users' private keys are generated. Then the adversary is provided with identities of the original signers and proxy signers, the system parameters, the master public key and the original signers' private keys.

2. Throughout the entire game, the adversary is able to make ILMPMS generation queries of the form $(h, ID_P, \sigma_w, ID_O, m)$, where h is the index of an honest proxy signer such that $ID_{P,h} \in ID_P$, σ_w is a multi-delegation signature generated by the users with ID_O and m is the message to be signed. The challenger simulates a valid multi-proxy multi-signature $\sigma \leftarrow Sig(sk_{P,h}, \sigma_w, m, ID_O, ID_P)$.

3. The adversary has also access to a corrupt oracle $Corrupt(.)$, which on input $ID_{P,i}$, returns $sk_{P,i}$.

4. The adversary Outputs $(w^*, m^*, \sigma^*, ID_{O^*}, ID_{P^*})$ and succeeds if the following conditions are satisfied:

- It never queried $(h, ID_{P^*}, \sigma_{w^*}, ID_{O^*}, m^*)$, for any h.
- One of the identities in ID_{P^*} is not in the set of the corrupted users.
- $Vrfy(w^*, m^*, \sigma^*, ID_{O^*}, ID_{P^*}) = 1$.

Definition 16. We say that an ILMPMS scheme is secure against Type2 adversary if no PPT adversary has a non-negligible advantage in the above game.

b. **Existential unforgeability against Type3 adversary**

By existential unforgeability against Type3 adversary of ILMPMS schemes, we mean that it is difficult for an adversary to forge a valid multi-delegation signature on a warrant of its choice, even if it has obtained the private keys of the proxy signers and original signers except for the honest original signer, and some other valid multi-delegation signatures on its chosen warrants. Consider the following game for a formal definition of existential unforgeability against a PPT Type3 adversary in an ILMPMS scheme.

1. Let l be the game parameter. The system parameters, master private/public key pair and users' private keys are generated. Then the adversary is provided with identities of the original signers and proxy signers, the system parameters, the master public key and the proxy signers' private keys.

2. Throughout the entire game, the adversary is able to make multi-delegation generation queries of the form (h, ID_O, w), where h is index of an honest original signer such that $ID_{O,h} \in ID_O$ and w is the warrant to be signed. The challenger simulates a valid delegation signature $\sigma_w \leftarrow Sig(sk_{O,h}, w, ID_O)$.

3. The adversary has also access to a corrupt oracle $Corrupt(.)$, which on input $ID_{O,i}$, returns $sk_{O,i}$.

4. The adversary Outputs $(w^*, \sigma_{w^*}, ID_{O^*})$ and succeeds if the following conditions are satisfied:

- It never queried (h, ID_{O^*}, w^*), for any h.
- One of the identities in ID_{O^*} is not in the set of the corrupted users.
- $Vrfy(w^*, \sigma_{w^*}, ID_{O^*}) = 1$.

Definition 17. We say that an ILMPMS scheme is secure against Type3 adversary if no PPT adversary has a non-negligible advantage in the above game.

Definition 18. We say that an ILMPMS scheme is existential unforgeable against adaptive chosen-message attack if it is secure against both Type2 and Type3 adversaries.

5 ILMS scheme

Here, we propose an ILMS scheme, which enjoys security against quantum computers and efficiency due to ID-based framework, linear operations and possibility of parallel computations based on lattices. We use the proposed ILMS scheme as the underlying signature in our ILMPMS scheme in Section 7. Our ILMS scheme consists of the following algorithms, as mentioned in Section 3.1.

5.1 Setup

Consider a set of N signers with identity set $ID = \{ID_1, \dots, ID_N\}$. Let $\alpha, k, d, q, n, m = n \log q$ be positive integers, $H_1: \{0,1\}^* \to \mathbb{Z}_q^{m \times n}$ and $H: \{0,1\}^* \to \{0,1\}^k$ be as random oracles and $F: \{0,1\}^k \to V_{n,\omega}$, where $V_{n,\omega}$ denotes the set of binary vectors of length n and Hamming weight ω. The key distribution center (KDC) chooses $A_0 \in \mathbb{Z}_q^{(m+n)\times n}$ and generates the corresponding trapdoor basis T_0. KDC sets T_0 as the master private key and generates the master public key $A = A_0' \in \mathbb{Z}_q^{m \times n}$ using the following lemma.

Lemma 1 : Let $\boldsymbol{b = As + e\ (mod\ q)}$, where $\boldsymbol{A} \in \mathbb{Z}_{\boldsymbol{q}}^{(\boldsymbol{m+n})\times \boldsymbol{n}}, \boldsymbol{s} \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{n}}, \boldsymbol{e} \in \boldsymbol{\chi}^{\boldsymbol{m+n}}$ and $\boldsymbol{b} \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{m+n}}$. We have the following trapdoor for LWE with short secrets.

Proof: First, we use the trapdoor basis of $\boldsymbol{A}$ to invert $\boldsymbol{b}$. With overwhelming probability, $\boldsymbol{A}$ has rank $\boldsymbol{n}$ and by swapping rows of $\boldsymbol{A}$, if necessary, we have $\boldsymbol{A_1} \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{n}\times \boldsymbol{n}}$ as an invertible matrix and $\boldsymbol{A_2} \in \mathbb{Z}_{\boldsymbol{q}}^{\boldsymbol{m}\times \boldsymbol{n}}$, therefore

$$A = \begin{pmatrix} A_1 \\ A_2 \end{pmatrix}, b = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, e = \begin{pmatrix} e_1 \\ e_2 \end{pmatrix}$$

$$\Longrightarrow b_1 = A_1 s + e_1\ (mod\ q), b_2 = A_2 s + e_2\ (mod\ q)$$

$$\Longrightarrow b_2 = A_2 A_1^{-1}(b_1 - e_1) + e_2\ (mod\ q)$$

$$\Longrightarrow b_2 - A_2 A_1^{-1} b_1 = (-A_2 A_1^{-1}) e_1 + e_2\ (mod\ q)$$

$$h = A's' + e', where \begin{cases} h = b_2 - A_2 A_1^{-1} b_1 \in \mathbb{Z}_q^m \\ A' = -A_2 A_1^{-1} \in \mathbb{Z}_q^{m \times n} \\ s' = e_1 \in \mathbb{Z}_q^n \\ e' = e_2 \in \mathbb{Z}_q^m \end{cases}$$

■

5.2 Key Extraction

For each signer $ID_i \in \{ID_1, \dots, ID_N\}$, KDC computes $S_i \in D_\alpha^{n \times n}$ and $E_i \in D_\alpha^{m \times n}$ such that $AS_i + E_i = H_1(ID_i)(mod\ q)$. If $Check\ (E) = 0$, as mentioned in the preliminary, then the algorithm restarts. Otherwise, it outputs the private key S_i to the signer ID_i.

5.3 MS Generation

Let μ denotes a message to be signed by the signers from the identity set $ID = \{ID_1, \dots, ID_N\}$.

- The signer ID_i chooses $y_i \xleftarrow{R} [-\beta, \beta]^n$, where β is obtained from Theorem 4, then computes $v_i = Ay_i \ (mod\ q)$ and broadcasts v_i to the co-signers.
- The signer ID_i, computes:

$$v = \sum_{j=1}^{N} v_j \ (mod\ q)$$

$$c = H(\lceil v \rfloor_d, \mu, ID)$$

$$C = F(c)$$

$$z_i = S_i C + y_i$$

$$w = Az_i - H_1(ID_i)C \ (mod\ q) \tag{13}$$

$$if \ \left|[w_i]_{2^d}\right| > 2^{d-1} - \ell \ , then\ restart. \text{ (for } 1 \le i \le m)$$

Otherwise, the signer ID_i broadcasts z_i to the co-signers with probability $\min\{\frac{D_y^n(z_i)}{N.D_{y,SC}^n(z_i)}, 1\}$.

- When all the partial signatures are valid, the multi-signature of the message μ w.r.t. the identity set ID is obtained as $\sigma_{MS} = (z = \sum_{j=1}^{N} z_j\ , c)$.

5.4 MS Verification

Upon receiving $(ID, \mu, \sigma_{MS} = (z, c))$, the verifier computes:

$$C = F(c)$$

$$w' = Az - \sum_{i=1}^{N} H_1(ID_i)\, C \ (mod\ q) \tag{14}$$

$$c' = H(\lceil w' \rfloor_d, \mu, ID)$$

The multi-signature σ_{MS} is accepted if the following relations are satisfied. Otherwise, it is rejected.

$$\|z\|_\infty \le N\beta$$

$$c' = c$$

6 Security analysis of the proposed ILMS

In the security proof, it is assumed w.l.o.g. that there is only one honest signer. Here, we consider an adversary faced with either a valid public key of our ILMS scheme or a

random one and show that those keys cannot be distinguished with non-negligible probability. In Theorem 4 we show that our ILMS scheme is unforgeable based on decisional LWE problem in the random oracle model. We consider adaptive chosen-message attack scenario, where an adversary $\mathcal{A}$ is allowed to make arbitrary many multi-signature queries to the honest signer on the messages of its choice. The adversary $\mathcal{A}$ is provided with the private keys of all signers but the honest signer.

Theorem 4: If $\boldsymbol{LWE_{n,m,q,\alpha}}$ is $\boldsymbol{\epsilon}$-hard, our ILMS scheme is $\boldsymbol{\epsilon'}$-unforgeable against adaptive chosen-message attacks in the random oracle model, where at most $\boldsymbol{N}$ users are involved and $\boldsymbol{\mathcal{A}}$ makes at most $\boldsymbol{q_0}$ key extraction queries, at most $\boldsymbol{q_1}$ hash queries of oracle $\boldsymbol{H}(.)$ and at most $\boldsymbol{q_2}$ signing queries.

Before proving this theorem, it is needed to state the following lemmas.

Lemma 2: For $S \in [-\beta, \beta]^{n\times n}, E \in [-\beta, \beta]^{m\times n}$ and $A, H_1 \overset{R}{\leftarrow} \mathbb{Z}_q^{m\times n}$, we have

$$\Pr\{(S,E)|\, AS + E = H_1\} \leq \frac{(2\beta+1)^{mn+n^2}}{q^{mn}}$$

Proof: Using the conditional probability definition, we have

$$\Pr\{(S,E)|\, AS + E = H_1\} = \Pr\{(S,E), AS + E = H_1\}/\Pr\{AS + E = H_1\}$$

$$\leq \frac{|\{S \in [-\beta,\beta]^{n\times n}\}|.|\{E \in [-\beta,\beta]^{m\times n}\}|}{\left|\{H_1 \in \mathbb{Z}_q^{m\times n}\}\right|} = \frac{(2\beta+1)^{n^2}.(2\beta+1)^{mn})}{q^{mn}}$$

$$= \frac{(2\beta+1)^{mn+n^2}}{q^{mn}} \blacksquare$$

Lemma 3: For $z \in [-\alpha, \alpha]^n, y \overset{R}{\leftarrow} [-\beta, \beta]^n, C \overset{R}{\leftarrow} \mathcal{B}_{n,\omega}$ and $\{A, H_1\} \overset{R}{\leftarrow} \mathbb{Z}_q^{m\times n}$, we have

$$\Pr\{z \mid \lceil Ay\ (mod\ q)\rfloor_d = \lceil Az - H_1 C\ (mod\ q)\rfloor_d\} \leq \frac{2^{dn}(2\alpha+1)^n}{q^m}$$

Proof: Using the notation $\lceil . \rfloor_d$, we have

$$\Pr\{z|\, \lceil Ay\ (mod\ q)\rfloor_d = \lceil Az - H_1 C\ (mod\ q)\rfloor_d\}$$
$$= \Pr\{z|\, Ay = Az - H_1 C\ (mod\ q)\}.2^{dn}$$

Therefore, it remains to prove that

$$\Pr\{z|\, Az = Ay + H_1 C\ (mod\ q)\} \leq \frac{(2\alpha+1)^n}{q^m}$$

For using Lemma 1, we rewrite $A = \binom{A_1'}{A_2'}$, where $A_1' \in \mathbb{Z}_q^{n\times n}$ is an invertible matrix and $A_2' \in \mathbb{Z}_q^{(m-n)\times n}$. Let

$$u = Az = Ay + H_1 C\ (mod\ q) = \binom{u_1}{u_2}$$

$$\Rightarrow \begin{cases} A_1' z = u_1 \in \mathbb{Z}_q^n \quad (mod\ q)\ (I) \\ A_2' z = u_2 \in \mathbb{Z}_q^{m-n}\ (mod\ q)\ (II) \end{cases}$$

First, we compute the number of variables z' satisfying (I). Then, we give the probability of satisfying z' in (II).

(I) : Using Gaussian heuristic, stated in Section 2.2, the number of variables in $\mathcal{L}_{u_1,q}^{\perp}(A_1') \cap [-\alpha, \alpha]^n$ is $\frac{(2\alpha+1)^n}{q^n}$.

(II): Assume that $A_1' z' = u_1\ (mod\ q)$, the probability that z' satisfies the second equation for $u_2 \in \mathbb{Z}_q^{m-n}$ is $\frac{1}{q^{m-n}}$.■

Lemma 4 [39]: For $A \xleftarrow{R} \mathbb{Z}_q^{m\times n}$, we have

$$\Pr\{\lfloor Ay_1\ (mod\ q)\rceil_d = \lfloor Ay_2\ (mod\ q)\rceil_d \mid y_1, y_2 \xleftarrow{R} [-\beta, \beta]^n\} \leq \frac{2^{(d+1)m}/q^{m-n}}{(2\beta+1)^n}$$

Proof of Theorem 4: Consider an adversary $\mathcal{A}$ that makes q_1 hash queries and q_2 signing queries and outputs a valid forgery with probability ϵ', involving at most N users. We show that a challenger $\mathcal{C}$ could use $\mathcal{A}$ and solve the $LWE_{n,m,q,\alpha}$ problem with probability ϵ.

Assume that on input (A, T), the challenger $\mathcal{C}$ uses $\mathcal{A}$ to decide whether T is of the form $T = AS + E$ for some $S \xleftarrow{R} D_\alpha^{n\times n}$ and $E \xleftarrow{R} D_\alpha^{m\times n}$ ($\mathcal{C}$ outputs 1) or it is sampled uniformly from $\mathbb{Z}_q^{m\times n}$ ($\mathcal{C}$ outputs 0). The challenger $\mathcal{C}$ initializes empty lists $R_1[.]$ and $R[.]$ and answers the queries as follows.

- $\boldsymbol{H_1(ID_u)}$ **queries:** Let ID_1 be the identity of the honest signer and $R(ID_1) = (*,*,T)$. If $R(ID_u) = (S_u, E_u, T_u)$ then $\mathcal{C}$ returns T_u, otherwise it chooses $S_u \xleftarrow{R} D_\alpha^{n\times n}$ and $E_u \xleftarrow{R} D_\alpha^{m\times n}$ and sets $T_u = AS_u + E_u$ and returns T_u to $\mathcal{A}$.
- $\boldsymbol{H(Q)}$ **queries:** If $R_1(Q)$ is already filled, then $\mathcal{C}$ returns it, otherwise $\mathcal{C}$ chooses $R_1(Q) \xleftarrow{R} \{0,1\}^k$ and returns it to $\mathcal{A}$.
- $\boldsymbol{Corrupt(ID_u)}$ **queries:** If $R(ID_u) = (S_u, E_u, T_u)$ then $\mathcal{C}$ returns S_u, otherwise it queries $H_1(ID_u)$ and returns S_u to $\mathcal{A}$. In the case of $u = 1$, $\mathcal{C}$ aborts.
- **MS Generation queries:** On input message μ and identity set ID including ID_1, $\mathcal{C}$ chooses $c \xleftarrow{R} \{0,1\}^k$ and $z_1 \xleftarrow{R} [-\beta, \beta]^n$, and computes

$$C = F(c), w = Az_1 - TC$$
$$if\ \left|[w_i]_{2^d}\right| > 2^{d-1} - \ell\ then\ restart.$$

Then $\mathcal{C}$ broadcasts $v_1 = \lfloor w \rceil_d$. At the same time $\mathcal{C}$ receives v_i from the corrupted signers and computes $v = \sum_{i=1}^{N} v_i\ (mod\ q)$. If $H(\lfloor v \rceil_d, \mu, ID)$ was queried before, then $\mathcal{C}$ aborts. Otherwise, it broadcasts z_1, corresponding to the honest signer, while receiving z_i from the corrupted signers and outputs $(z = \sum_{j=1}^{N} z_j, c)$ as the multi-signature.

$\mathcal{A}$ finally outputs a forgery (z', c') on a non-queried message. If it outputs a valid forgery, then $\mathcal{C}$ outputs 1. Otherwise, it outputs 0. We have:

$$\epsilon = |\Pr\{(S,E): \mathcal{C}(A, AS+E) = 1\} - \Pr\{T \xleftarrow{R} \mathbb{Z}_q^{m\times n}: \mathcal{C}(A,T) = 1\}|$$

Where, $\mathcal{C}(A, AS+E) = 1$ means the correct output 1 in case of $T = AS + E$ and $\mathcal{C}(A,T) = 1$ means the false output 1 in case of $T \xleftarrow{R} \mathbb{Z}_q^{m\times n}$. Now, we compute the probability of correct 'output 1' in case of $T = AS + E$ and the probability of false 'output 1' in case of $T \xleftarrow{R} \mathbb{Z}_q^{m\times n}$:

- **The case of $T = AS + E$:** Success is achieved in this case, when $\mathcal{C}$ does not abort during *MS Generation queries* and *Corruption queries*, and $\mathcal{A}$ does not fail. Using Lemma 4 and hybrid argument [55], the probability of abortion during the *MS Generation queries* is bounded by $q_2(q_1+q_2)\frac{2^{(d+1)m}/q^{m-n}}{(2\beta+1)^n}$. It remains to compute the probability that $\mathcal{C}$ does not abort during *Corruption queries*. The honest signer is considered to be uniformly chosen among N users. The probability that $\mathcal{C}$ does not abort after c corruption queries is $1/(N-c)$. Consider that $\mathcal{A}$ queries at most q_0 corruption queries. The probability that $\mathcal{C}$ does not abort during *Corruption queries* is:

  $$\left(1-\frac{1}{N}\right)\left(1-\frac{1}{N-1}\right)\ldots\left(1-\frac{1}{N-(q_0-1)}\right) = \frac{N-q_0}{N}$$

  So, we have:

$$\Pr\{\mathcal{C}(A, AS+E) = 1\} \geq \left(\tfrac{N-q_0}{N}\right)\left(1 - q_2(q_1+q_2)\frac{2^{(d+1)m}/q^{m-n}}{(2\beta+1)^n}\right)\epsilon' \qquad (15)$$

- **The case of $T \xleftarrow{R} \mathbb{Z}_q^{m\times n}$:** For falsely 'output 1' in this case, we have scenarios of Lemma 2 and Lemma 3. Based on Lemma 2, for $S \in [-\beta,\beta]^{n\times n}$ and $E \in [-\beta,\beta]^{m\times n}$, we have:

$$\Pr\{(S,E) | AS + E = T\} \leq \frac{(2\beta+1)^{mn+n^2}}{q^{mn}} \qquad (16)$$

Note that the entries of S and E are bounded by $\beta = 7\alpha$, with high probability.

Based on Lemma 3, for $z \in [-N\beta, N\beta]^n$, $C \xleftarrow{R} \mathcal{B}_{n,\omega}$ and $\{A, H_1\} \xleftarrow{R} \mathbb{Z}_q^{m\times n}$, we have

$$\Pr\{z | \lceil Ay \ (mod\ q)\rfloor_d =$$

$$\lceil Az - (T + \textstyle\sum_{i=2}^{N} H_1(ID_i))C \ (mod\ q)\rfloor_d\} \leq \frac{2^{dn}(2N\beta+1)^n}{q^m} \qquad (17)$$

$$(16), (17) \Longrightarrow \Pr\{\mathcal{C}(A,T) = 1\} \leq \frac{(2\beta+1)^{mn+n^2}}{q^{mn}} + q_1\frac{2^{dn}(2N\beta+1)^n}{q^m} \qquad (18)$$

Eventually, from (15), (18) we have:

$$\epsilon \approx \left(\frac{N-q_0}{N}\right)\left(1-q_2(q_1+q_2)\frac{\frac{2^{(d+1)m}}{q^{m-n}}}{(2\beta+1)^n}\right)\epsilon' - \left(\frac{(2\beta+1)^{mn+n^2}}{q^{mn}} + q_1\frac{2^{dn}(2N\beta+1)^n}{q^m}\right) \quad (19)$$

7 ILMPMS scheme

Here, we propose an ILMPMS scheme usable in real scenarios, which enjoys security against quantum computers and efficiency due to ID-based framework, linear operations and possibility of parallel computations based on lattices. Our ILMPMS scheme consists of the following algorithms, as mentioned in Section 0.

7.1 Setup

There are M original signers and N proxy signers with identity sets $ID_O = \{ID_{O1}, \dots, ID_{OM}\}$ and $ID_P = \{ID_{P1}, \dots, ID_{PN}\}$, respectively. Let $\alpha, k, d, q, n, m = n\log q$ be positive integers, $F: \{0,1\}^k \to V_{n,\omega}, H_1: \{0,1\}^* \to \mathbb{Z}_q^{m\times n}$ and $H: \{0,1\}^* \to \{0,1\}^k$ be random oracles. KDC chooses $A_0 \in \mathbb{Z}_q^{(m+n)\times n}$ and generates the corresponding trapdoor basis T_0. KDC sets T_0 as the master private key and generates the master public key $A = A_0' \in \mathbb{Z}_q^{m\times n}$ using Lemma 1.

7.2 Key Extraction

For each signer $ID_i \in ID_O \cup ID_P$, KDC computes $S_i \in D_\alpha^{n\times n}$ and $E_i \in D_\alpha^{m\times n}$ such that $AS_i + E_i = H_1(ID_i)(mod\ q)$. If $Check\ (E) = 1$, then the algorithm outputs the private key S_i to the signer ID_i. Otherwise, the algorithm is restarted.

7.3 MD Generation

Let w denotes a warrant to be signed by the original signers $ID_O = \{ID_{O1}, \dots, ID_{OM}\}$.

- For $1 \le i \le M$, the original signer ID_{Oi} chooses $y_i \xleftarrow{R} [-\beta, \beta]^n$, computes $v_i = Ay_i\ (mod\ q)$ and broadcasts v_i to co-original signers.
- For $1 \le i \le M$, the original signer ID_{Oi}, computes:

$$v_O = \sum_{j=1}^{M} v_j\ (mod\ q)$$

$$c_O = H(\lceil v_O \rfloor_d, w, ID_O)$$

$$C_O = F(c_O)$$

$$z_i = S_i C_O + y_i$$

$$u_O = Az_i - H_1(ID_{Oi})C_O\ (mod\ q) \quad (20)$$

$$if\ \left|[u_{Oi}]_{2^d}\right| > 2^{d-1} - \ell\ then\ restart.\ (\text{for } 1 \le i \le m)$$

and broadcasts z_i to the co-original signers with probability $\min\{\frac{D_y^n(z_i)}{M.D_{y,SC}^n(z_i)}, 1\}$.

- When all the partial signatures are valid, the multi-delegation signature σ_w on w w.r.t. ID_O is $\sigma_w = (z_O = \sum_{j=1}^{M} z_j , c_O)$.

7.4 MD Verification

Upon receiving $(ID_O, w, \sigma_w = (z_O, c_O))$, the verifier computes:

$$C_O = F(c_O)$$
$$u'_O = Az_O - \sum_{i=1}^{M} H_1(ID_{Oi})\, C_O \ (mod\ q) \tag{21}$$
$$c'_O = H(\lceil u'_O \rfloor_d, w, ID_O)$$

The multi-delegation signature σ_w is accepted if the following relations are satisfied. Otherwise, it is rejected.

$$\|z_O\|_\infty \leq M\beta$$
$$c'_O = c_O$$

7.5 ILMPMS Generation

Let μ denotes a message to be signed by the proxy signers $ID_P = \{ID_{P1}, \dots, ID_{PN}\}$.

- For $i \in \{1, \dots, N\}$, the proxy signer ID_{Pi} chooses $y_i \xleftarrow{R} [-\beta, \beta]^n$, computes $v_i = Ay_i \ (mod\ q)$ and broadcasts v_i to co-proxy signers.
- For $i \in \{1, \dots, N\}$, the proxy signer ID_{Pi} computes:

$$v_P = \sum_{j=1}^{N} v_j \ (mod\ q)$$
$$u'_O = Az_O - \sum_{i=1}^{N} H_1(ID_{Oi})\, C_O \ (mod\ q)$$
$$c_p = H(\lceil u'_O + v_P \rfloor_d, w, \mu, ID_O, ID_P)$$
$$C_P = F(c_P)$$
$$z_i = S_i C_P + y_i$$
$$u_P = Az_i - H_1(ID_{Pi}) C_P \ (mod\ q) \tag{22}$$
$$if\ \ \left|[u_{Pi}]_{2^d}\right| > 2^{d-1} - \ell\ \ then\ restart. \text{ (for } 1 \leq i \leq m)$$

and broadcasts z_i to the co-proxy signers with probability $\min\{\frac{D_y^n(z_i)}{N.D_{y,SC}^n(z_i)}, 1\}$.

- When all the partial signatures are valid, the ILMPMS signature σ on μ w.r.t. ID_P is $\sigma = (z_P = z_O + \sum_{j=1}^{N} z_j , c_O, c_P)$.

7.6 ILMPMS Verification

Upon receiving $(ID_O, ID_P, \mu, \sigma = (z_P, c_O, c_P))$, the verifier computes:

$$C_O = F(c_O)$$

$$C_P = F(c_P)$$

$$u'_p = Az_P - \sum_{i=1}^{M} H_1(ID_{Oi})\, C_O - \sum_{i=1}^{N} H_1(ID_{Pi})\, C_P \ (mod\ q) \tag{23}$$

$$c'_P = H\left(\lceil u'_p \rfloor_d, w, \mu, ID_O, ID_P\right)$$

The ILMPMS signature σ is accepted if the following relations are satisfied. Otherwise, it is rejected.

$$\|z_p\|_\infty \le N\beta$$

$$c'_P = c_P$$

8 Security analysis of the proposed ILMPMS

The proposed scheme in Section 8 is warrant-based, in which the delegation is the original signer's signature on a warrant. The warrant includes proxy signers' public key, the validity duration and the restrictions on the messages that the proxy signer can sign. The following properties originate from warrant that is preventing misuse of a delegation, distinguishability from normal signatures and undeniability [5]. In this section we mainly analyze the existential unforgeability of the proposed scheme by Theorem 5, in details.

Theorem 5. If $LWE_{n,m,q,\alpha}$ is ϵ-hard, our ILMPMS is ϵ'-unforgeable against adaptive chosen-message attacks in the random oracle model where at most *M* original signers and *N* proxy signers are involved and $\mathcal{A}$ makes at most q_e *key extraction* queries, at most q_h hash queries of oracle $H(.)$, at most q_d *MD Generation* queries, and at most q_s *MPMS Generation* queries.

Proof. We need to show that our proposed ILMPMS is secure against Type2 and Type3 adversaries. For this purpose, we consider the following cases I and II. Security proofs of both cases can be achieved using Theorem 4. It is assumed w.l.o.g. that there is only one honest signer.

Case I. In this case, we consider adversaries of Type2, where we have only one honest proxy signer.

Proof. In this case, the adversary can make *MPMS Generation* queries. Therefore, in the proof of Theorem 4 we substitute *MS Generation* queries oracle with *MPMS Generation* queries oracle. In this case, there is no need to make *MD Generation* queries, because Type2 adversary has private keys of all original signers. Therefore, from equation (19) we have:

$$\epsilon \approx \left(\frac{N-q_e}{N}\right)\left(1 - q_s(q_h + q_s)\frac{\frac{2^{(d+1)m}}{q^{m-n}}}{(2\beta+1)^n}\right)\epsilon'_{Type2} - \frac{(2\beta+1)^{mn+n^2}}{q^{mn}} - q_h\frac{2^{dn}(2N\beta+1)^n}{q^m} \tag{24}$$

Case II. In this case, we consider adversaries of type3, where we have only one honest original signer.

Proof. In this case, the adversary can make *MD Generation* queries. Therefore, in the proof of Theorem 4 we substitute *MS Generation* queries oracle with *MD Generation* queries oracle. In this case, there is no need to make *MPMS Generation* queries, because Type3 adversary has private keys of all proxy signers. Therefore, from equation (19) we have:

$$\epsilon \approx \left(\frac{M-q_e}{M}\right)\left(1-q_d(q_h+q_d)\frac{\frac{2^{(d+1)m}}{q^{m-n}}}{(2\beta+1)^n}\right)\epsilon'_{Type3}-\frac{(2\beta+1)^{mn+n^2}}{q^{mn}}-q_h\frac{2^{dn}(2N\beta+1)^n}{q^m} \quad (25)$$

In Table 3, we compare our proposed ILMPMS scheme with the existing ones from the view of the underlying hard problems and the security flaws.

Table 3: security comparison between the proposed scheme and the existing IMPMS schemes

Scheme	Security basis	Post-quantum security	Lattice-based	ID-based
Lattice-based multi-signature scheme [40]	R-SIS	×[2]	✓	×
Proposed ILMS scheme	LWE	✓	✓	✓
IMPMS [38]	CDH[1]	×	×	✓
IMPMS [37]	RSA	×	×	✓
Proposed ILMPMS scheme	LWE	✓	✓	✓

[1] Computational Diffie-Hellman
[2] Due to using Forking Lemma

9 Conclusions

Multi-proxy multi-signature schemes are useful when a group of original signers cooperatively delegate their signing rights to a group of proxy signers, who are authorized to generate the proxy signatures cooperatively on behalf of the original signers. For realizing this application, in this paper, we have proposed an ID-based lattice-based multi-proxy multi-signature (ILMPMS) scheme, which enjoys security against quantum computers and efficiency due to ID-based framework, linear operations and possibility of parallel computations based on lattices. For this purpose, we have first proposed an ID-based lattice-based multi-signature (ILMS) scheme, used as the underlying signature in our ILMPMS scheme. To the best of our knowledge, these schemes are the first lattice-based ones, which benefit from provable security based on worst-case intractability of the lattice hard problems. For the security analysis, we have proved that the proposed schemes are existential unforgeable against adaptive chosen-message attack in the random oracle model based on the hardness of LWE problem over standard lattices.

References

[1] Mambo, Masahiro, Keisuke Usuda, and Eiji Okamoto. "Proxy signatures for delegating signing operation." In Proceedings of the 3rd ACM conference on Computer and communications security, pp. 48-57. ACM, 1996.

[2] Mambo, Masahiro, Keisuke Usuda, and Eiji Okamoto. "Proxy signatures: delegation of the power to sign messages." IEICE transactions on fundamentals of electronics, communications and computer sciences 79, no. 9 (1996): 1338-1354.

[3] Awasthi, Amit K., and Sunder Lal. "ID-based ring signature and proxy ring signature schemes from bilinear pairings." arXiv preprint cs/0504097 (2005).

[4] Wei, Baodian, Fangguo Zhang, and Xiaofeng Chen. "Ring proxy signatures." Journal of Electronics (China) 25, no. 1 (2008): 108-114.

[5] Sun, Ying, Chunxiang Xu, Yong Yu, and Yi Mu. "Strongly unforgeable proxy signature scheme secure in the standard model." Journal of Systems and Software 84, no. 9 (2011): 1471-1479.

[6] Xu, Shengmin, Guomin Yang, Yi Mu, and Sha Ma. "Proxy Signature with Revocation." In Australasian Conference on Information Security and Privacy, pp. 21-36. Springer International Publishing, 2016.

[7] El-Kamchouchi, H., Heba Gaber, Fatma Ahmed, and Dalia H. El-Kamchouchi. "Secure Proxy Signature Based on Factoring and Discrete Logarithm." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 10, no. 7 (2016): 1196-1199.

[8] Rivest, Ronald L., Adi Shamir, and Len Adleman. "A method for obtaining digital signatures and public-key cryptosystems." Communications of the ACM 21, no. 2 (1978): 120-126.

[9] ElGamal, Taher. "A public key cryptosystem and a signature scheme based on discrete logarithms." In Advances in cryptology, pp. 10-18. Springer Berlin Heidelberg, 1985.

[10] Shor, Peter W. "Algorithms for quantum computation: Discrete logarithms and factoring." In Foundations of Computer Science, 1994 Proceedings, 35th Annual Symposium on, pp. 124-134. IEEE, 1994.

[11] Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmen, eds. Post-quantum cryptography. Springer Science & Business Media, 2009.

[12] Peikert, Chris. Decade of Lattice Cryptography. World Scientific, 2016.

[13] Ajtai, Miklós. "Generating hard instances of lattice problems." In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 99-108. ACM, 1996.

[14] Lili, Zhang, and Yongxuan Sang. "A Lattice-based Identity-based Proxy Signature from Bonsai Trees." International Journal of Advancements in Computing Technology 4, no. 20 (2012).

[15] Lili, Zhang, Ma Yanqin, and Yongxuan Sang. "A Lattice-based Multiple Grade Proxy Signature in the Standard Model." International Journal of Advancements in Computing Technology 5, no. 9 (2013).

[16] Zhang, Lili, and Yanqin Ma. "A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model." Mathematical Problems in Engineering 2014 (2014).

[17] Yi, Lijang, Guoqiang Bai, and Guozhen Xiao. "Proxy multi-signature scheme: a new type of proxy signature scheme." Electronics Letters 36, no. 6 (2000): 527-528.
[18] Li, Xiangxue, Kefei Chen, and Shiqun Li. "Multi-proxy signature and proxy multi-signature schemes from bilinear pairings." In Parallel and Distributed Computing: Applications and Technologies, pp. 591-595. Springer, Berlin, Heidelberg, 2004.
[19] Chun-xiang, Gu, Pan Heng, and Zhu Yue-fei. "A new ID-based proxy multi-signature scheme from bilinear pairings." Wuhan University Journal of Natural Sciences 11, no. 1 (2006): 193-197.
[20] Tiwari, Namita, and Sahadeo Padhye. "An ID-based proxy multi signature scheme without bilinear pairings." In Security Aspects in Information Technology, pp. 83-92. Springer, Berlin, Heidelberg, 2011.
[21] Wang, Qin, and Zhenfu Cao. "Identity based proxy multi-signature." Journal of Systems and Software 80, no. 7 (2007): 1023-1029.
[22] Shao, Zuhua. "Improvement of identity-based proxy multi-signature scheme." Journal of Systems and Software 82, no. 5 (2009): 794-800.
[23] Cao, Feng, and Zhenfu Cao. "A secure identity-based proxy multi-signature scheme." Information Sciences 179, no. 3 (2009): 292-302.
[24] Sahu, Rajeev Anand, and Sahadeo Padhye. "Efficient ID-based proxy multi-signature scheme secure in random oracle." Frontiers of Computer Science 6, no. 4 (2012): 421-428.
[25] S.J. Hwang, C.H. Shi, A simple multi-proxy signature scheme for electronic commerce, in: Proceedings of the 10th National Conference on Information Security, Hualien Taiwan, ROC, 2000, pp. 134–138.
[26] Chen, Xiaofeng, Fangguo Zhang, and Kwangjo Kim. "ID-based multi-proxy signature and blind multisignature from bilinear pairings." Proceedings of KIISC 3 (2003): 11-19.
[27] Cao, Feng, and Zhenfu Cao. "A secure identity-based multi-proxy signature scheme." Computers & Electrical Engineering 35, no. 1 (2009): 86-95.
[28] Wang, Qin, Zhenfu Cao, and Shengbao Wang. "Formalized security model of multi-proxy signature schemes." In Computer and Information Technology, 2005. CIT 2005. The Fifth International Conference on, pp. 668-672. IEEE, 2005.
[29] Shin-Jia, Hwang, and Chen Chiu-Chin. "New multi-proxy multi-signature schemes." Applied Mathematics and Computation 147, no. 1 (2004): 57-67.
[30] Tzeng, Shiang-Feng, Cheng-Ying Yang, and Min-Shiang Hwang. "A nonrepudiable threshold multi-proxy multi-signature scheme with shared verification." Future Generation Computer Systems 20, no. 5 (2004): 887-893.
[31] Sahu, Rajeev Anand, and Sahadeo Padhye. "Efficient ID-based multi-proxy multi-signature scheme based on CDHP." Journal of Applied Mathemtics and Informatics 5, no. 4 (2011): 275-282.
[32] Sahu, Rajeev Anand, and Sahadeo Padhye. "An ID-based multi-proxy multi-signature scheme." In Computer and Communication Technology (ICCCT), 2010 International Conference on, pp. 60-63. IEEE, 2010.
[33] Guo, Sheng, Zhenfu Cao, and Rongxing Lu. "An efficient ID-based multi-proxy multi-signature scheme." In Computer and Computational Sciences, 2006. IMSCCS'06. First International Multi-Symposiums on, vol. 2, pp. 81-88. IEEE, 2006.
[34] Tiwari, Namita, Sahadeo Padhye, and Debiao He. "Efficient ID-based multiproxy multisignature without bilinear maps in ROM." Annals of Telecommunications-Annales des télécommunications 68, no. 3-4 (2013): 231-237.

[35] Li, Xiangxue, and Kefei Chen. "ID-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings." Applied Mathematics and Computation 169, no. 1 (2005): 437-450.
[36] Chang, Ya-Fen, and Chin-Chen Chang. "Efficient multi-proxy multi-signature schemes based on DLP." IJCSNS 6, no. 2B (2006): 152.
[37] Asaar, Maryam Rajabzadeh, Mahmoud Salmasizadeh, and Willy Susilo. "An identity-based multi-proxy multi-signature scheme without bilinear pairings and its variants." The Computer Journal 58, no. 4 (2014): 1021-1039.
[38] Sahu, Rajeev Anand, and Sahadeo Padhye. "Identity- based multi- proxy multi-signature scheme provably secure in random oracle model." Transactions on Emerging Telecommunications Technologies 26, no. 4 (2015): 547-558.
[39] Bai, Shi, and Steven D. Galbraith. "An improved compression technique for signatures based on learning with errors." In Cryptographers' Track at the RSA Conference, pp. 28-47. Springer International Publishing, 2014.
[40] El Bansarkhani, Rachid, and Jan Sturm. "An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins." In International Conference on Cryptology and Network Security, pp. 140-155. Springer International Publishing, 2016.
[41] Güneysu, Tim, Vadim Lyubashevsky, and Thomas Pöppelmann. "Practical lattice-based cryptography: A signature scheme for embedded systems." In International Workshop on Cryptographic Hardware and Embedded Systems, pp. 530-547. Springer Berlin Heidelberg, 2012.
[42] Alkim, Erdem, Nina Bindel, Johannes Buchmann, Özgür Dagdelen, and Peter Schwabe. Tesla: tightly-secure efficient signatures from standard lattices. Cryptology ePrint Archive, Report 2015/755, 2015.
[43] Goldreich, Oded. Foundations of cryptography: vol. 2, basic applications. Cambridge university press, 2009.
[44] Micciancio, Daniele, and Shafi Goldwasser. Complexity of Lattice Problems: A Cryptographic Perspective. vol. 671, Springer Science & Business Media, 2002.
[45] Micciancio, Daniele, and Oded Regev. "Lattice-based cryptography." In Post-quantum cryptography, pp. 147-191. Springer Berlin Heidelberg, 2009.
[46] Gama, Nicolas, and Phong Q. Nguyen. "Predicting lattice reduction." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 31-51. Springer Berlin Heidelberg, 2008.
[47] Gentry, Craig, Chris Peikert, and Vinod Vaikuntanathan. "Trapdoors for hard lattices and new cryptographic constructions." In Proceedings of the fortieth annual ACM symposium on Theory of computing, pp. 197-206. ACM, 2008.
[48] Lyubashevsky, Vadim. "Fiat-Shamir with aborts: Applications to lattice and factoring-based signatures." In Advances in Cryptology-ASIACRYPT 2009, pp. 598-616. Springer Berlin Heidelberg, 2009.
[49] Micciancio, Daniele, and Chris Peikert. "Hardness of SIS and LWE with small parameters." In Advances in Cryptology–CRYPTO 2013, pp. 21-39. Springer Berlin Heidelberg, 2013.
[50] Peikert, Chris. "Public-key cryptosystems from the worst-case shortest vector problem." In Proceedings of the forty-first annual ACM symposium on Theory of computing, pp. 333-342. ACM, 2009.
[51] Ajtai, Miklós. "Generating hard instances of the short basis problem." InInternational Colloquium on Automata, Languages, and Programming, pp. 1-9. Springer Berlin Heidelberg, 1999.

[52] Alwen, Joël, and Chris Peikert. "Generating shorter bases for hard random lattices." Theory of Computing Systems 48, no. 3 (2011): 535-553.

[53] Micciancio, Daniele, and Chris Peikert. "Trapdoors for lattices: Simpler, tighter, faster, smaller." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 700-718. Springer Berlin Heidelberg, 2012.

[54] Özgür Dagdelen, Rachid El Bansarkhani, Florian Göpfert, Tim Güneysu, Tobias Oder, Thomas Pöppelmann, Ana Helena Sanchez, and Peter Schwabe. "High-speed signatures from standard lattices." In Diego F. Aranha and Alfred Menezes, editors, Progress in Cryptology-LATINCRYPT 2014, vol. 8895, pp. 84-103, LNCS, Springer, 2015.

[55] Lyubashevsky, Vadim. "Lattice signatures without trapdoors." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 738-755. Springer Berlin Heidelberg, 2012.