Sādhanā (2022)47:41
https://doi.org/10.1007/s12046-022-01808-3

A Quantum Resistant Anonymous Poxy Signature Scheme

SWATI RAWAL and SAHADEO PADHYE*

Department of Mathematics, Motilal Nehru National Institute of Technology Allahabad, Prayagraj 211004, India
e-mail: swati.rawal25@gmail.com; sahadeomathrsu@gmail.com

MS received 29 June 2021; revised 5 December 2021; accepted 6 January 2022

Abstract. Proxy signature was first coined by Mambo *et al* to carry out the signing procedure even in the absence of the original signer to sign the required document. Moreover, occasionally anonymity of proxy signers is required so that no one can reveal their identity, including the original signer. The paper thus proposes a quantum-safe anonymous proxy signature, which provides anonymity to the proxy signers based on the worst-case hardness of lattice problems. The construction is proved to be unforgeable against the adaptive chosen message attacks against the hardness of the small integer solution problem.

Keywords. Lattice-based digital signature; proxy signature; anonymous proxy signature.

1. Introduction

As of yet, the security of many cryptosystems is widely based on well-known number-theoretical problems such as factoring and discrete-log problem. For decades, many algorithms were developed to solve these problems, but the fastest algorithms are sub-exponential on classical systems. However, Peter Shor [1, 2] gave an algorithm that can solve these problems in polynomial runtime on quantum computers. This development threatened modern cryptography and gave a new domain of interest *post-quantum* cryptography. Post-quantum cryptography is the area where we develop quantum computer-resistant schemes and can be implemented on our classical computers. It mainly consists of code-based systems, multivariate cryptography, hash-based signatures, and lattice-based schemes.

Lattices are coined as the most exciting feature of modern cryptography. The lattice-based cryptosystems have an upper hand over other areas as the security of these systems can be reduced to worst-case problems, and most of the schemes require simple computations to compute ciphertexts or signatures. Due to the ground-breaking work of Ajtai [3] connecting worst-case problems and average-case problems for lattices, many cryptographers attract to work on lattice-based cryptography. Ajtai proved that certain problems are hard on average if the underlying related problem on lattices is hard in the worst-case scenario. Such results become the foundations for the construction of many cryptographical schemes like digital signature. Digital signature plays a vital role in modern digital communication to verify the sender's authenticity.

Sometimes, suppose the original signer is unable to sign on any document due to his busy schedule or any other unavoidable reason. In that case, he authorizes a trusted proxy signer to sign the document on his behalf using a proxy signature. The concept of proxy signature was first formally presented by Mambo *et al* [4] in 1996. In this scheme, the proxy signer signs the document on behalf of the original signer using a proxy signing key. The proxy signing key is either generated by the original signer or by the proxy signer using his secret key and the delegation sent by the original signer.

Literature review. Many proxy signatures and their variants were proposed [5–8] in classical settings based on integer factoring, discrete log problems, and elliptic curves. Proxy signature based on bilinear pairing [9–12] were also introduced later on. But the advent of quantum computers in the near future threatens the security of all the above schemes. In 2010, Jiang *et al* [13] introduced the first lattice-based proxy signature, offering a quantum secure alternative. But this scheme was proved to be insecure by Tian and Huang [14], where they showed that anyone could forge a proxy signature on any message. Cash *et al* [15] introduced a new insight of using bonsai trees to get such signatures. In 2011, Wang *et al* [16] proposed a proxy signature scheme using the bonsai trees concept. Xia *et al* [17] also gave a proxy signature using the bonsai trees, which security is based on the hardness of average-case SIS and ISIS problems. This scheme was proved to be existentially secure for the chosen-message attack in the random oracle. But both the signature schemes [16, 17] face a drawback that they produce longer signatures, which is inefficient for practical uses. Using fixed dimension basis expansion techniques [18], in 2013, Yu Lei [19] developed

*For correspondence
Published online: 16 February 2022

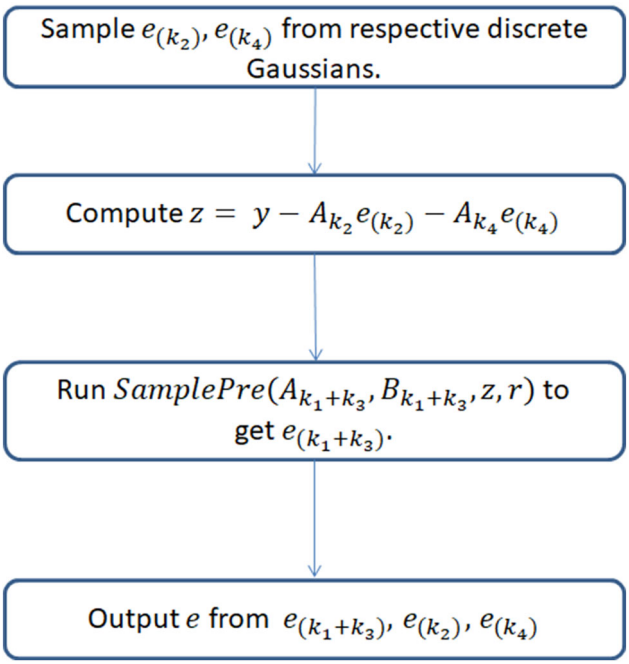

Figure 1. ExtSampPre Algorithm.

more efficient proxy signature. But this signature uses the basis expansion along with two times a pre-image sampling algorithm, which turns out to be time-consuming and not efficient for practical uses. In 2015, extending the concept of signature developed by Lyubashevsky [20], Yang *et al* [21] developed a proxy signature without trapdoor, which generated a shorter signature in comparison to the above schemes, and proved the scheme to be existentially unforgeable in the random oracle.

Proxy signatures with additional features were also proposed as per the requirement. The lattice-based ID-based proxy signature was first proposed by Zhang *et al* [22] using the bonsai tree, which is proved to have a unforgeability proxy key, revocability of proxy signature as well as existential unforgeable. But this signature scheme was not proxy protected. Kim *et al* [23] constructed the first ID-based proxy signature scheme with proxy protection in the random oracle model. ID-based proxy signature in the standard model [24] was also developed utilizing the lattice-based delegation techniques [18] and lattice-based signing. Zhang *et al* [25] used the concept of blind signature and gave the ID-based proxy blind signature, but Rawal *et al* [26] carried an attack over this scheme exposing the secret master key of the scheme. Lattice-based multigrade proxy signature [27] was also proposed by Zhang *et al* in 2013 based on SIS and ISIS hardness assumptions. In 2018, Faguo Wu *et al* proposed an ID-based proxy signature [28], but based on NTRU lattice in the random oracle model.

Consider a scenario where an entity delegates his signing capability to many proxy signers, and any of the proxy signers can perform the signing operation on behalf of the original signer. In some applications, anonymity is required, and proxy signers want nobody to reveal their identity, even the original signer. For example, consider the case where an authorized journalist is supposed to publish an article on some issue on behalf of the editor, but he needs courage and assurance to do this honestly. Therefore, he needs his identity to be anonymous, and this could be achieved by the concept of an anonymous proxy signature. This concept was first introduced in 2003 by Zhang *et al* [29] and then again in 2009 by Yu *et al* [30] with provable security under the random oracle model. But, later, Chou *et al* [31] proved their scheme to lack anonymity. Also, these schemes were based on classical methods, which lack security in the presence of quantum computers.

Our contribution- In this paper, we propose a lattice-based quantum-proof anonymous proxy signature, which allows intractability to the proxy signers. To offer anonymity to proxy signers, we use the concept of ring signature. We prove that the constructed scheme is adaptively secure against the chosen message attacks against the solidity of the small integer solution problem. This scheme is the first lattice-based anonymous proxy signature scheme to the best of our knowledge.

Organization- The paper proceeds as follows, Sectons 2 and 3 deal with required preliminaries, algorithms, and the security requirements for the scheme. Section 4 is devoted to the proposed scheme, and section 5 analyzes the security requirements for our proposed scheme. The last section compiles the paper with a conclusion.

2. Preliminaries

2.1 *Notation*

Unless specified, $\|.\|$ denotes euclidean norm of vector, and the bold case alphabets denote the matrices. The vertical bar $|$ denotes the concatenation of matrices and vectors. For any random variables U and V, the statistical distance between them over a discrete domain D is defined as $\Delta(U,V) = \frac{1}{2}\Sigma_{t\in D}(Prob(U=t) - Prob(V=t))$. The set $\{1,\ldots,k\}$ is denoted by $[k]$.

The standard asymptotic growth rates notations $\mathcal{O}()$ and $\omega()$ are used and the symbol $\sim$ implies that logarithmic factors are ignored.

2.2 *Lattice background*

Definition 1 An $n-dimensional$ lattice is a full-rank discrete subgroup of $\mathbb{R}^n$. For a set $\{\mathbf{b}_1,\ldots\mathbf{b}_n\}$ with n linearly independent vectors, an n-dimensional lattice $\mathcal{L}$ using this set is defined as $\mathcal{L} = \{\Sigma_{i=1}^{n}\mathbf{b}_i\alpha_i : \alpha_i \in \mathbb{Z}\}$. This set $\{\mathbf{b}_1,\ldots\mathbf{b}_n\}$ is known as a basis of the lattice $\mathcal{L}(\mathbf{B})$.

Definition 2 [32] For some $q, n, m \in \mathbb{Z}$ and a given matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, we define following

1. $\mathcal{L}^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{Ax} : \mathbf{0} \bmod \mathbf{q}\}$
2. $\mathcal{L}_y^{\perp}(\mathbf{A}) := \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{Ax} : \mathbf{y} \bmod \mathbf{q}\}$

Note that as $\mathcal{L}_y^{\perp}(\mathbf{A}) = u + \mathcal{L}^{\perp}(\mathbf{A})$ where u is an arbitrary solution (over $\mathbb{Z}^m$) of the equation $Au = y \bmod q$, $\mathcal{L}_y^{\perp}(\mathbf{A})$ forms a coset of $\mathcal{L}^{\perp}(\mathbf{A})$.

The lattice problems on which our scheme is based on introduced by Ajtai [3] which connect the average-case hardness to the worst-case hardness of lattice problems [33], are as below.

Definition 3 (SIS-Shortest Integer Solution Problem) Here the problem is to find a non-zero integer $\mathbf{z}$ such that $\mathbf{Az} = 0 \bmod q$ and $\|\mathbf{z}\| \leq t$, for a positive integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and a real t.

A slight variant of the above problem, where we are expected to solve a random inhomogeneous system, is defined as below.

Definition 4 (ISIS-Inhomogeneous Shortest Integer Solution) Here the problem is to find a non-zero integer $\mathbf{z}$ such that $\mathbf{Az} = \mathbf{y} \bmod q$ and $\|\mathbf{z}\| \leq t$, for a positive integer q, a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, a real t, and a syndrome $\mathbf{y} \in \mathbb{Z}_q^n$.

2.3 *Discrete Gaussian over lattices*

Probability distributions plays an important role in lattice cryptography specifically discrete gaussian, below they are discussed briefly.

Definition 5 Gaussian function: For any standard deviation $v > 0$, a Gaussian function can be defined on $\mathbb{R}^n$ centred at c as .

$$\rho_{c,v}(\mathbf{x}) = \exp\Big(-\pi\frac{\|\mathbf{x}-c\|}{v}\Big), \mathbf{x} \in \mathbb{R}^n$$

Definition 6 Discrete Gaussian distribution: For any n-dimensional lattice $\mathcal{L}$, a Discrete Gaussian function can be defined as

$$D_{\mathcal{L}_{c,v}}(\mathbf{x}) = \frac{\rho_{c,v}(\mathbf{x})}{\rho_{c,v}(\mathcal{L})}, \forall x \in \mathcal{L}.$$

where $\rho_{c,v}(\mathcal{L}) = \Sigma_{x\in\mathcal{L}}\rho_{c,v}(\mathbf{x})$.

Note that σ and c are 1 and 0 respectively if it is not mentioned in the equation.

Definition 7 Statistical distance [34] **:** The statistical distance between two distribution U and V over a countable domain D is defined as $\Delta(U,V) = \frac{1}{2}\Sigma_{x\in D}\|U(x) - V(x)\|$. If the statistical distance $\Delta(U,V)$ is negligible in k, then we say the two distributions (two ensembles $\{U_k\}_{k\in\mathbb{N}}$ and $\{V_k\}_{k\in\mathbb{N}}$ indexed by k) are statistically close.

Theorem 1 [34] *Let $n, q > 0$ with q a prime, and $m > 2n\log q$. Then for all $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ (except a $2q^{-n}$ fractions of all $\mathbf{A}$'s), any $\sigma > \omega(\sqrt{\log m})$ and for given $\mathbf{e} \leftarrow D_\sigma^m$, the distribution of $\mathbf{y} = \mathbf{Ae} \bmod q$ is statistically close to the uniform distribution over $\mathbb{Z}_q^n$.*

Theorem 2 [34] *There is a PPT (probabilistic polynomial time) algorithm that returns a sample from a distribution statistically close to $D_{\mathcal{L},\sigma,c}$ on input a basis $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ of the lattice $\mathcal{L}$, a center $c \in \mathbb{R}^m$, and a parameter $\sigma \geq \|\tilde{\mathbf{B}}\|\omega(\sqrt{\log m})$. Moreover, for any $\mathbf{x} \leftarrow D_{\mathcal{L},\sigma,c}$*

$$prob\{\|\mathbf{x} - c\| \geq \sigma\sqrt{m}\} \leq negl(m)\,.$$

.

Theorem 3 [34, 35] *For the given positive integers $n, q \geq 2$ and $m = O(n\log q)$, there is an efficient PPT algorithm $TrapGen(1^n)$ that returns an $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ statistically close to uniform and the trapdoor basis $\mathbf{T} \in \mathbb{Z}^{m\times m}$ for $\mathcal{L}^{\perp}(\mathbf{A})$.*

Definition 8 Pre-image sampleable functions (PSF): The PSF's are determined by three PPT algorithms *TrapGen*, *SampleDom* and *SamplePre*

- $TrapGen(1^n)$: This generates a pair $(\mathbf{A}, \mathbf{T})$, which efficiently defines a function $f_{\mathbf{A}} : D_n = \{\mathbf{e} \in \mathbb{Z}^m : \|\mathbf{e}\| \leq s\sqrt{m}\} \longrightarrow R_n = \mathbb{Z}_q^n$ as $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{Ae} \bmod q$ and $\mathbf{T}$ act as a trapdoor.
- $SampleDom(1^n)$: This samples a $\mathbf{e}$ from the input distribution D_n such that $f_{\mathbf{A}}(\mathbf{e})$ is uniform over the range R_n.
- $SamplePre(\mathbf{A}, \mathbf{T}, \mathbf{y})$: Returns the preimage $\mathbf{e}$ for $\mathbf{y}$, such that $f_{\mathbf{A}}(\mathbf{e}) = \mathbf{y}$ for any uniformly chosen $\mathbf{y}$ from the range R_n.

2.4 *Pre-image sampling for extended lattice [36]*

For some $k, k_1, k_2, k_3, k_4 \in \mathbb{Z}_{>0}$ with $k = k_1 + k_2 + k_3 + k_4$, let $\mathbf{A}_k = [\mathbf{A}_{k_1}, \mathbf{A}_{k_2}, \mathbf{A}_{k_3}, \mathbf{A}_{k_4}] \in \mathbb{Z}_q^{n\times km}$, where $\mathbf{A}_{k_i} \in \mathbb{Z}_q^{n\times k_i m}$, $i \in [4]$. Consider $\mathbf{A}_{k_1+k_3} = [\mathbf{A}_{k_1}|\mathbf{A}_{k_3}] \in \mathbb{Z}_q^{n\times(k_1+k_3)m}$. Let us suppose we have short basis $\mathbf{B}_{k_1+k_3}$ of the lattice $\mathcal{L}^{\perp}(\mathbf{A}_{k_1+k_3})$ and given an integer $r \geq \|\overline{\mathbf{B}}_{k_1+k_3}\|\omega(\sqrt{\log n})$, the *ExtSampPre* algorithm samples a preimage of the function $f_{\mathbf{A}_k}(\mathbf{e}) = \mathbf{A}_k\mathbf{e} \bmod q$. $ExtSampPre(\mathbf{A}_{\mathbf{k}}, \mathbf{A}_{k_1+k_3}, \mathbf{B}_{k_1+k_3}, \mathbf{y}, r)$ runs with the following steps :

1. For $D_{\mathbb{Z}^{k_2 m},r}$ and $D_{\mathbb{Z}^{k_4 m},r}$, sample[1] $\mathbf{e}_{(k_2)} \in \mathbb{Z}^{k_2 m}$ and $\mathbf{e}_{(k_4)} \in \mathbb{Z}^{k_4 m}$. Write $\mathbf{e}_{(k_2)}$ as $[\mathbf{e}_{k_1+1}, \ldots, \mathbf{e}_{k_1+k_2}] \in \mathbb{Z}^{k_2 m}$ and $\mathbf{e}_{(k_4)}$ as $[\mathbf{e}_{k-k_4+1}, \ldots, \mathbf{e}_k] \in \mathbb{Z}^{k_4 m}$.
2. Construct $\mathbf{z} = \mathbf{y} - \mathbf{A}_{k_2}\mathbf{e}_{(k_2)} - \mathbf{A}_{k_4}\mathbf{e}_{(k_4)} \bmod q$. Run $SamplePre(\mathbf{A}_{k_1+k_3}, \mathbf{B}_{k_1+k_3}, \mathbf{z}, r)$(from [34]) to obtain $\mathbf{e}_{(k_1+k_3)} \in \mathbb{Z}^{(k_1+k_3)m}$ from $D_{\mathcal{L}^{\perp}_{\mathbf{y}}(\mathbf{A_k}),r}$. Write $\mathbf{e}_{(k_1+k_3)} = [\mathbf{e}_1, \ldots, \mathbf{e}_{k_1}, \mathbf{e}_{k_1+k_2+1}, \ldots, \mathbf{e}_{k-k_4}] \in \mathbb{Z}^{(k_1+k_3)m}$, and let $\mathbf{e}_{(k_1)} = [\mathbf{e}_1, \ldots, \mathbf{e}_{k_1}] \in \mathbb{Z}^{k_1 m}$, $\mathbf{e}_{(k_3)} = [\mathbf{e}_{k_1+k_2+1}, \ldots, \mathbf{e}_{k-k_4}] \in \mathbb{Z}^{k_3 m}$.
3. Yielding $\mathbf{e} = \{\mathbf{e}_{(k_1)}, \mathbf{e}_{(k_2)}, \mathbf{e}_{(k_3)}, \mathbf{e}_{(k_4)}\} = [\mathbf{e}_1, \ldots \mathbf{e}_k] \in \mathbb{Z}^{km}$.

Remark 1 According to construction, we have $\mathbf{A}_{k_1}\mathbf{e}_{(k_1)} + \mathbf{A}_{k_3}\mathbf{e}_{(k_3)} = \mathbf{A}_{k_1+k_3}\mathbf{e}_{(k_1+k_3)} = \mathbf{z} \bmod q$. Therefore, $\mathbf{A}_k\mathbf{e} = \Sigma_{i=1}^{4}\mathbf{A}_i\mathbf{e}_{(k_i)} = \mathbf{y} \bmod q$, and the output $\mathbf{e}$ belongs to $\mathcal{L}^{\perp}_{\mathbf{y}}(\mathbf{A}_k)$. From the Theorem 3.4 in [37] , $\mathbf{e}$ is within negligible statistical distance of $D_{\mathcal{L}_{\mathbf{y}}{}^{\perp}(\mathbf{A}_k),r}$.

3. Anonymous proxy signature : formal structure and security requirements

The anonymous proxy signature with warrant works with the subsequent algorithms,

- *Setup* : It takes security parameter as input and returns the system parameters as output.
- *KeyGen* : On receiving the system parameters as input, the algorithm generates the public/private keys of original signer and the proxy signers.
- *DelGen* : This algorithm generates the delegation on the warrant using the private key of the original signer and the system parameters.
- *DelVef* : Using the system parameters and original signer's public key, the proxy signers verify the delegation on the provided warrant. This algorithm accepts the delegation if valid else rejects it.
- *PSign* : On receiving the system parameters, the message to be signed, delegation warrant, public keys of proxy signers, and a private key of one of the proxy signer. This algorithm returns the proxy signature on the given message.
- *PVerify* : On receiving the proxy signature it returns accept if the signature is proved to be valid using the public keys of proxy and original signer, else it rejects the signature.

[1] $\mathbf{e}_{(k_i)}$'s is just used to differentiate them from $\mathbf{e}_{k_i}$, as both of them are distinct. $\mathbf{e}_{(k_i)}$ belongs to $\mathbb{Z}^{k_i m}$ and $\mathbf{e}_{k_i} \in \mathbb{Z}^m$ is a k_ith vector of $\mathbf{e}_{(k_i)}$.

3.1 *Security requisites*

3.1.1 *Existential unforgeability* Unforgeability of the proposed scheme is discussed under the following three type of adversaries.

- **Type 1 :** The adversary here have the public and private key pair of original signer and public keys of proxy signers.
- **Type 2 :** The adversary here have the public keys of original and proxy signers, and private keys of some of the proxy signers.
- **Type 3 :** The adversary only have access to the public keys of both original and proxy signer.

Definition 9 Existential unforgeability adverse to Type 1 adversary: The anonymous proxy signature is said to unforgeable against Type 1 probabilistic polynomial time adversary if the probability of successfully executing the following game is non-negligible.

The game works as follows :

Let l be the number of proxy signers (or the game parameter). Then $\{pk_i, sk_i\}_{i=1}^{l}, \{pk_O, sk_O\}$ are generated for the proxy signers and the original signer respectively. $\{pk_i, sk_i\}_{i=1}^{l}$ are given to the adversary along with all the public parameters. During the entire game, adversary is empowered to make proxy signer queries of the form (i, s_w, msg, R) and corruption query of the form $\{i\}$. The challenger then returns signature s and sk_i respectively for the above queries.

Finally, the adversary returns a forgery $(s^{\star}, msg^{\star}, s_w^{\star}, R^{\star})$ such that

- $(i, msg^{\star}, s_w^{\star}, R^{\star})$ is not queried for any i.
- $R^{\star}$ doesn't contain any corrupted user.
- It satisfies the verification equation.

If the above holds, he wins the game.

Definition 10 Existential unforgeability adverse to Type 2 adversary: The anonymous proxy signature is said to unforgeable against probabilistic polynomial time Type 2 adversary if the probability of successfully executing the following game is non-negligible.

This game works as follows :

Let l be the number of proxy signers (or the game parameter). Then $\{pk_i, sk_i\}_{i=1}^{l}, \{pk_O, sk_O\}$ are generated for all signers as in previous game. The adversary will have $\{pk_O, sk_O\}$, and all the public parameters. Throughout the game, the adversary is allowed to have delegation sign queries of the form $\{w\}$, and the challenger returns s_w using the private key of the original signer.

Finally, the adversary will return the delegation forgery $(w^{\star}, s^{\star})$. It will be accounted as a valid forgery if $w^{\star}$ is not queried before and it satisfies the delegation verification equation, and he wins the game.

Definition 11 Anonymity: The proposed signature is said to be anonymous if there exists no adversary who can successfully execute the following game with non-negligible probability.

The game works as follows :

Let l be the number of proxy signers (or the game parameter). Then $\{pk_i, sk_i\}_{i=1}^{l}, \{pk_O, sk_O\}$ are generated for the proxy and original signers respectively. $\{pk_i\}_{i=1}^{l}$ are given to the adversary.

During the entire game the adversary can ask for proxy signer queries of the form (i, s_w, msg, R) and challenger returns signature s to the adversary.

Then adversary pleas a challenge by sending the value (s_w, i_0, i_1, R, msg), where i_0, i_1 are the indices for the public key pk_{i_0}, pk_{i_1} for the members of the ring R. $\mathcal{C}$ randomly selects $b \in \{0,1\}$ and returns the proxy signature σ on $H(\sigma_w, R, msg)$ using the keys (pk_b, sk_b). Finally adversary returns the guess b' corresponding to b. The adversary is successful if the guess $b' = b$.

4. Proposed Construction

The proposed construction works with the following algorithms,

- *Setup* : Positive integers n, m, d, q, N such that $q \geq 2$ and $m \geq n \log q$. The scheme consists of parameter functions $\tilde{L} \geq O(\sqrt{n \log n})$ and $\beta \geq \tilde{L}.\omega(\sqrt{\log n})$ as defined in [38]. System parameters also consist of $d+1$ independent matrices $\mathbf{U}_0, \mathbf{U}_1, \ldots, \mathbf{U}_d$ and a cryptographic hash function $H : \{0,1\}^{\star} \longrightarrow \{0,1\}^d$.
- *KeyGen* : Original signer and proxy signers run the $TrapGen(1^n)$ to get $(\mathbf{A}_O, \mathbf{T}_O)$ and $(\mathbf{A}_i, \mathbf{T}_i)$, $i = 1, \ldots, N$ as their public and private key respectively.
- *DelGen* : Original Signer generates the signature on the warrant $w = (w_1, \ldots, w_d) \in \{0,1\}^d$ which contains the original signer's public key and validity of warrant as follows :
  - First compute $\mathbf{U}_w = \mathbf{U}_0 + \Sigma_{i=1}^{d}(-1)^{w_i}\mathbf{U}_i \bmod q$ and $\mathbf{A}_w = [\mathbf{A}_O|\mathbf{U}_w] \in \mathbb{Z}_q^{n \times 2m}$.
  - Then, original signer samples $s_w \leftarrow ExtSampPre(\mathbf{A}_w, \mathbf{T}_O, \beta)$ and sends this s_w to the proxy signers.
- *DelVef* : After receiving this warrant (w, s_w) from the original signer, proxy signers accepts the warrant if the following relation hold

$$\|s_w\| \leq \beta\sqrt{2m},$$
$$\mathbf{A}_w s_w = 0 \bmod q.$$

As $\mathbf{U}_0, \mathbf{U}_1, \ldots, \mathbf{U}_d$ are public parameters, proxy signers can compute $\mathbf{A}_w$.

- *PSign* : The proxy signer with $(\mathbf{A}_i, \mathbf{T}_i)$, from a ring R of a proxy signers, such that $|R| = l$, generates the signature on the message $msg \in \{0,1\}^{\star}$ as follows,
  - First, he computes $M = H(msg, w, R)$ and $\mathbf{U}_M = \mathbf{U}_0 + \Sigma_{i=1}^{d}(-1)^{M_i}\mathbf{U}_i \bmod q$, where M_i is the ith bit of $M \in \{0,1\}^d$.
  - Then he obtains $\mathbf{A}_R = [\mathbf{A}_1|\ldots|\mathbf{A}_l|\mathbf{U}_M]$ and samples $s \leftarrow ExtSampPre(\mathbf{A}_R, \mathbf{T}_i, \beta)$. Then he publishes (s, msg, s_w, w) as a warrant of the proxy signature on the message msg.
- *PVerify* : After the proxy signature is published, the verifier confirms its validity if,

$$\|s\| \leq \beta\sqrt{(l+1)m}, \|s_w\| \leq \beta\sqrt{2m},$$
$$\mathbf{A}_R s = 0 \bmod q, and \mathbf{A}_w s_w = 0 \bmod q.$$

5. Security Analysis

This section deals with the analysis of the proposed scheme. First, the unforgeability of the scheme is proved under the hardness of the short integer solution problem, for all possible types of adversaries.

5.1 *Unforgeability*

Theorem 4 *The proposed construction is secure against Type 1 adversary under the event that underlying hash H is collision-resistant, and SIS is hard.*

Proof 1 Here, Type 1 adversary can lead in two different ways. First, where he issues two pairs (msg, R) and (msg', R') such that $H(msg, w, R) = H(msg', w, R')$. Second, where he doesn't attack the underlying hash but returns a forged signature. This proof shows that there exists a challenger $\mathcal{C}$ that can challenge the complexity assumptions in both the cases.

Case 1: First, let us suppose that $\mathcal{C}$ wants a collision for underlying hash H.

For l proxy signers of ring R and original signer, Challenger $\mathcal{C}$ runs the *Setup* and *KeyGen* to obtain the public and private keys for all users. Then $\mathcal{C}$ sends public parameter, the proxy public key and original signer's keys (both public and private) to the adversary.

Initially, $\mathcal{C}$ initializes the set of corrupted users $C \leftarrow \phi$. The adversary $\mathcal{A}$ makes the following queries to $\mathcal{C}$,

- *Proxy Sign Query :* $\mathcal{A}$ gives (i, s_w, msg, R) as an input where i is the signer with keys (pk_i, sk_i) and $\mathcal{C}$ returns s as a signature for the message msg with warrant w.
- *Corruption Query :* $\mathcal{A}$ gives the input i and then $\mathcal{C}$ returns sk_i and stores pk_i to C.

Finally, $\mathcal{A}$ returns $(s^\star, msg^\star, s_w^\star, R^\star)$ as a forgery, since it is a valid forgery, it satisfies all the verification equations and $R^\star$ doesn't have any corrupted user. Moreover, $(s_w^\star, msg^\star, R^\star)$ is not queried before.

Now, $\mathcal{C}$ keeps the pair $(msg^\star, R^\star)$, if this attack is carried out, there will be two pairs (msg, R) , (msg', R') such that $H(msg, w, R) = H(msg', w, R')$. Therefore, $\mathcal{C}$ can get a collision whenever $\mathcal{A}$ returns a valid forgery. Thus, we can conclude that advantage of the adversary in unforgeability is less than or equal to the advantage of the challenger in getting the collisions.

Case 2: Now, suppose that the challenger wants to attack the underlying signature scheme (Boyen's Signature) for the public key $\mathbf{A} \in \mathbb{Z}_q^{n\times rm}$.

The challenger $\mathcal{C}$ works with $d+1$ independent matrices $\mathbf{U}_0, \mathbf{U}_1, \ldots, \mathbf{U}_d$ and generates the user keys as follows :

- $\mathcal{C}$ picks indices $R_t = \{t_1, t_2, \ldots, t_r\} \subseteq \{1, 2, \ldots, l\}$. For original signer and for each $i \notin R_t$, he runs the *KeyGen* algorithm. For $i \in R_t$, $\mathcal{C}$ separates $\mathbf{A}$ as $pk_i = \mathbf{A}_i \in \mathbb{Z}_q^{n\times m}$. Then he sends the public parameter, public keys $\{pk_i\}_{i=1}^l$ and original signer's key to the adversary $\mathcal{A}$.
- $\mathcal{C}$ initializes the set of corrupted users $C \leftarrow \phi$.

Now, $\mathcal{A}$ makes corruption and proxy sign queries.

- *Corruption Query :* $\mathcal{A}$ gives the input i, and then $\mathcal{C}$ returns sk_i and stores pk_i to C.
- *Proxy Sign Query :* $\mathcal{A}$ gives (j, s_w, msg, R) where $R \in \{1, 2, \ldots, l\}$ and let $|R| = r'$. If $j \notin R_t$ then $\mathcal{C}$ returns s from the *PSign* algorithm. If $j \in R_t$, first it runs the Boyen's signing oracle for the signature on $M = H(msg, R, w)$, where $\mathbf{A} \in \mathbb{Z}_q^{n\times rm}$ is the public key. The Boyen's signing oracle returns $\tilde{s} \leftarrow ExtSampPre(\mathbf{A}_R, \mathbf{T}, \beta)$, where $\mathbf{A}_R = [\mathbf{A}|\mathbf{U}_M] \in \mathbb{Z}_q^{n\times(l+1)m}$ and $\mathbf{U}_M = \mathbf{U}_0 + \Sigma_{i=1}^d (-1)^{M_i}\mathbf{U}_i \bmod q \in \mathbb{Z}_q^{n\times m}$.

$\mathcal{C}$ can separate $\mathbf{A}$ as $[\mathbf{A}_j|\mathbf{A}'] \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n\times(r-1)m}$ and R as $[\mathbf{A}_j|R'] \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^{n\times(r'-1)m}$. Thus,

$$\tilde{s} = (\tilde{s}_1, \tilde{s}_2, \tilde{s}_3) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^{(r-1)m} \times \mathbb{Z}_q^m,$$

$$\mathbf{A}_R\tilde{\sigma} = [\mathbf{A}_j|\mathbf{A}'|\mathbf{U}_M]\begin{bmatrix}\tilde{s}_1\\ \tilde{s}_2\\ \tilde{s}_3\end{bmatrix} = 0.$$

If $R = \mathbf{A}$ then $\mathcal{C}$ returns $\tilde{s}$ to the adversary as the proxy signature. Else, there must exist a user $j \notin R_t$, but $pk_j \in R'$ then the challenger $\mathcal{C}$ computes $s' \leftarrow SampPre(R', \mathbf{T}_j, \mathbf{A}'s_2, \beta)$, and then

$$\hat{s} = (\tilde{s}_1, s', \tilde{s}_3),$$

$$[R|\mathbf{U}_M]\begin{bmatrix}\tilde{s}_1\\ s'\\ \tilde{s}_3\end{bmatrix} = [\mathbf{A}_i|R'|\mathbf{U}_M]\begin{bmatrix}\tilde{s}_1\\ s'\\ \tilde{s}_3\end{bmatrix} = 0.$$

Now, finally $\mathcal{A}$ returns $(s_w^\star, msg^\star, R^\star, s^\star)$ as a forgery.

If $R^\star = \mathbf{A}$ then $s^\star$ is a valid signature of Boyen's signature scheme on $H(R^\star, w, M^\star)$. If $R^\star$ is a submatrix of $\mathbf{A}$ then $\mathcal{C}$ can get a valid signature on $H(R^\star, w, M^\star)$ just by padding zero. Else if $R^\star$ is not even a submatrix of $\mathbf{A}$ then $\mathcal{C}$ aborts. □

Theorem 5 *The Proposed signature scheme is secured against Type 3 adversary under the hardness of SIS problem.*

Proof 2 Let us suppose there exist a challenger $\mathcal{C}$ who wants to solve the *SIS* problem for the matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and interacts with an adversary $\mathcal{A}$ to obtain a non-zero vector $\mathbf{v}$ such that $\mathbf{A}\mathbf{v} = 0 \bmod q$, $\|\mathbf{v}\| \le \mu$.

The challenger $\mathcal{C}$ works with n, m, d, q, N parameters. Then he fixes the public key of original signer as $pk_O = \mathbf{A}$ and runs the *KeyGen* algorithm to generate the key pair $(pk_i, sk_i)_{i=1}^l$ for proxy signers. He then runs the *KeyGen* algorithm once more to generate a $\mathbf{B} \in \mathbb{Z}_q^{n\times m}$ and corresponding basis $\mathbf{T}_B \in \mathbb{Z}_q^{m\times m}$.

Moreover, he selects $d+1$ short random matrices $\mathbf{C}_0, \mathbf{C}_1, \ldots, \mathbf{C}_d \in \mathbb{Z}_q^{m\times m}$ and d uniformly random $\mathbf{t}_1, \ldots, \mathbf{t}_d \in \mathbb{Z}_q$ and fixes $\mathbf{t}_0 = 1$. Then computes the public parameter as

$$\mathbf{U}_i = \mathbf{A}\mathbf{R}_i + \mathbf{t}_i\mathbf{B}, 0 \le i \le d$$

Then, he sends the public parameters, the public key of the original signer, public keys of proxy signers and some of the secret keys of proxy signers to the adversary $\mathcal{A}$. Now the adversary $\mathcal{A}$ and the challenger $\mathcal{C}$ works with the delegation queries as follows,

- When the adversary $\mathcal{A}$ asks for the delegation query for the warrant $w \in \{0,1\}^d$, the challenger works as follows,
  - First he computes,

$$\mathbf{R}_w = \Sigma_{i=1}^d (-1)^{w_i}\mathbf{R}_i, \mathbf{t}_w = \Sigma_{i=1}^d (-1)^{w_i}\mathbf{t}_i.$$

  If $\mathbf{t}_w = 0 \bmod q$, then $\mathcal{C}$ returns failure and aborts. Else, he computes

$$\mathbf{G} = [\mathbf{A}|\mathbf{A}\mathbf{R}_w + \mathbf{t}_w\mathbf{B}] \in \mathbb{Z}_q^{n\times 2m},$$

  and samples $s_w \leftarrow ExtSampPre(\mathbf{G}, \mathbf{T}_B, \beta)$ and sends this to the adversary $\mathcal{A}$.

Finally, the adversary $\mathcal{A}$ returns a delegation forgery $(w^\star, s_{w^\star})$. Since it is a valid forgery thus $w^\star$ is not queried before, and if $\mathbf{t}_w \neq 0 \bmod q$ then $\mathcal{C}$ aborts and declares

failure. Else he will work for the solution for *SIS* problem as follows,

Since, $s_{w^\star} = (s_1^\star, s_2^\star) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$, $\mathcal{C}$ computes

$$\mathbf{v} = s_1^\star + \mathbf{R}_w^\star s_2^\star \in \mathbb{Z}_q^m,$$

and then $\mathbf{Av} = \mathbf{A}(s_1^\star + \mathbf{R}_w^\star s_2^\star) = [\mathbf{A}|\mathbf{AR}_w^\star + \mathbf{t}_w^\star \mathbf{B}] \begin{bmatrix} s_1^\star \\ s_2^\star \end{bmatrix} = 0 \bmod q$ □

Thus, $\mathbf{v}$ is valid solution for $SIS_{q,m,\mu}$ problem where $\mu = (1 + \sqrt{(d+1)m}\,\omega(\sqrt{m}))\sqrt{2m}\beta$.

5.2 *Anonymity*

Theorem 6 *For $q \geq 2$ and $m \geq 2n \log q$ the proposed signature scheme is anonymous under the hardness of SIS problem.*

Proof 3 Let there be l ring members and suppose there exist a challenger $\mathcal{C}$ who follows the *Setup* algorithm and runs the *KeyGen* algorithm. He runs the *KeyGen* algorithm $l+1$ times with a random input b_i and obtain (pk_0, sk_0) as the keys of original signer and $(pk_i, sk_i)_{i=1}^{l}$ as the keys of proxy signers. During the anonymity game, the challenger responds to the proxy sign query (s, ws_w, R, msg). Finally, the adversary $\mathcal{A}$ sends the challenger the challenge value (s_w, i_0, i_1, R, msg) where i_0, i_1 are the indices for the public key pk_{i_0}, pk_{i_1} for the members of the ring R. Challenger $\mathcal{C}$ selects a random value $b \in \{0, 1\}$ and returns the proxy signature s on $H(s_w, R, msg)$ using the keys (pk_b, sk_b). Finally adversary returns the guess b' for b. If the guess is correct then $\mathcal{C}$ returns 1 else he outputs 0.

Since preimage sampling is used while generating the proxy signature, the signature s_{i_0}, s_{i_1} are computationally indistinguishable as $SIS_{q,(l+1)m,\beta\sqrt{(l+1)m}}$ is hard and the statistical distance between the vectors from the distribution $D^{\perp}_{\mathcal{L}_q(\mathbf{A}_R),\beta}$ is negligible. Hence our scheme has no overwhelming probability in winning the above game, making the scheme to attain anonymity under the hardness of *SIS* problem. □

6. Conclusion

The paper introduces a provable secure lattice-based anonymous proxy signature scheme. The proposed signature works when one out of a number of proxy signers sign messages with unconditional anonymity on behalf of the original signer. In contrast, nobody can open the proxy signer's identities, including the original signer. This scheme is the first lattice-based anonymous proxy signature scheme to the best of our knowledge. The scheme benefits from provable security based on the worst-case intractability of the lattice hard problems and security against quantum computers. We have proved that our scheme is anonymous and existential unforgeable against adaptive chosen-message attack based on the hardness of the short integer solution problem in lattices for the security analysis. The proposed signature scheme uses the concept of pre-image sampling, which can be a limitation, and one can work towards eliminating it to improve efficiency. Future direction in this area can focus on providing anonymity independent of ring setting to improve the signature scheme as well.

References

[1] Shor P 2006 Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal of Comput.* 26: 1484–1509

[2] Shor P 1994 Algorithms for Quantum Computation: Discrete Logarithms and Factoring. In: *Proceedings of 35th Annual IEEE Symposium on Foundations of Computer Scienc*e, IEEE Press, Piscataway, 124–134

[3] Ajtai M 1996 Generating hard instances of lattice problems (extended abstract). In: *Proceeding of 28th Annual ACM Symposium on the Theory of Comput.–STOC* 96: 99–108

[4] Mambo M, Usuda K, Okamoto E 1996 Proxy signatures: delegation of the power to sign messages. *IEICE Transactions Fundamentals* 9: 1338–1353

[5] Kim S, Park S and Won D 1997 Proxy signatures, revisited. In: *Proceedings of ICICS,* Springer-Verlag LNCS 1334: 223–232

[6] Okamoto T, Tada M and Okamoto E 1999 Extended proxy signatures for smart cards. In: *Proceedings of Information Security*, Springer-Verlag LNCS 1729: 247–258

[7] Lee B, Kim H and Kim K 2001 Secure mobile agent using strong non-designated proxy signature. In: *Proceedings of ACISP*, Springer-Verlag LNCS 2119: 474–486

[8] Wang G , Bao F, Zhou J and Deng R H 2004 Security analysis of some proxy signatures. In: *Proceedings of ICISC*, LNCS 2971: 305–319

[9] Okamoto T, Inomata A and Okamoto E 2005 A proposal of short proxy signature using pairing. In: *Proceedings of International Conference on Information Technology: Coding and Computing (ITCC)*, 631–635

[10] Xu J, Zhang Z and Feng D 2005 ID-based proxy signature using bilinear pairings. In: *Proceedings of ISPA*, LNCS 3759: 359–367

[11] Namita Tiwari, Sahadeo Padhye 2013 Provable secure proxy signature scheme without bilinear pairings. *International Journal of Communication Systems*, 26(5): 644–650

[12] Rajeev Anand Sahu, Sahadeo Padhye 2015 Provable secure identity-based multi-proxy signature scheme. *International Journal of Communication Systems* 28(3): 497–512

[13] Jiang Y, Kong F, JU X 2010 Lattice-based Proxy Signature. In: *Proceeding of Computational Intelligence and Security (CIS)*, 382–385

[14] Tian M, HUANG L 2012 Breaking A Proxy Signature Scheme from Lattices. *Int. J. Netw. Secur.* 14(6): 320–323

[15] Cash D, Hofheinz D, Kiltz E, Peikert C 2010 Bonsai Trees, or How to Delegate a Lattice Basis. In: *Proceeding of the Eurocrypt 2010,* LNCS 6110: 553–572

[16] Wang C, QI M 2011 Lattice-based Proxy Signature Scheme. *Journal of Information and Computational Science*, 8(12): 2451–2458

[17] Xia F, Yang B, Ma Sh 2011 Lattice-based Proxy Signature Scheme. *Journal of Hunan University (Natural Sciences)*, 38(6): 84–88

[18] Agrawal S , Boneh D, Boyen X 2010 Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE. In: *CRYPTO 2010, Advances in Cryptology*, 98–115

[19] YU L 2013 A Lattice-based Proxy Signature Scheme. *Computer Engineering*, 39(0): 1–5

[20] Lyubashevsky V 2012 Lattice signatures without trapdoors. In: *EUROCRYPT 2012, Springer-Verlag LNCS* 7237: 738–755

[21] Yang C, Qiu P, Zheng S, Wang L 2015 An Efficient Lattice-Based Proxy Signature Scheme without Trapdoor. In: *Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 189–194

[22] Zhang L and Sang Y 2012 A Lattice-based Identity-based Proxy Signature from Bonsai Trees. *International Journal of Advancements in Computing Technology* 4(20): 99–104

[23] Kim K S, Hong D, Jeong I R 2013 Identity-based proxy signature from lattices. *Communications and Networks* 15(1): 17

[24] Li W 2016 An Identity-Based Proxy Signature Scheme from Lattices in the Standard Model. In: *Proceedings International Conference on Intelligent Networking and Collaborative Systems* 167–172

[25] Zhang L, Ma Y 2014 A Lattice-Based Identity-Based Proxy Blind Signature Scheme in the Standard Model. *Mathematical Problems in Engineering*, Article ID 307637, 6 pages.

[26] Rawal S, Padhye S 2020 Cryptanalysis of ID based Proxy-Blind signature scheme over lattice. *ICT Express* 6 (1): 20–22

[27] Zhang L, Ma Y and Sang Y 2013 A Lattice-based Multiple Grade Proxy Signature in the Standard Model. *International Journal of Advancements in Computing Technology* 5(9), Article 108

[28] Wu F, Wang Y, Zhang X, Wang W, Zheng Z 2018 Identity-based proxy signature over NTRU lattice.*International Journal of Communication Systems*,Vol 32, Issue 3

[29] Zhang F, Safavinaini R, Lin C 2003 New Proxy Signature, Proxy Blind Signature and Proxy Ring Signature Schemes from Bilinear Pairings. *IACR Cryptology* ePrint Archive: Report 2003/104.

[30] Yu, Yong, Xu C, Huang X, Yi Mu 2009 An efficient anonymous proxy signature scheme with provable security. *Computer Standards & Interfaces* 31(2): 348–353

[31] Chou J S, Hung S C and Chen Y 2011 An Efficient Secure Anonymous Proxy Signature Scheme. *IACR Cryptology* ePrint Archive: Report 2011/498

[32] Ajtai M 1999 Generating hard instances of the short basis problem. In: *Proceeding of ICALP* 1–9

[33] Micciancio D and Regev O 2007 Worst-case to average-case reductions based on Gaussian measures. *SIAM J. Comput*., 37(1): 267–302

[34] Gentry C, Peikert C, Vaikuntanathan V 2008 Trapdoors for hard lattices and new cryptographic constructions. In: *Proceedings of the fortieth annual ACM symposium on Theory of computing* 2008, 197–206

[35] Peikert C 2014 A Decade of Lattice Cryptography. *Foundations and Trends in Theoretical Computer Science* World Scientific, vol. 10(4): 283–424

[36] Wang J and Sun B 2011 Ring Signature Scheme from Lattice Basis Delegation. In: *Proceeding of International Conference on Information and Communications Security (ICICS*), SPringer-Verlag LNCS Vol. 7043: 15–28

[37] Cash D, Hofheinz D, Kiltz E 2009 How to Delegate a Lattice Basis. *IACR Cryptology Eprint-Archive*: Report 2009/351

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