Cybersecurity

REVIEW **Open Access**

A survey on lattice-based digital signature

Fengxia Liu[1,2], Zhiyong Zheng[3,4], Zixian Gong[3,4*], Kun Tian[3,4*], Yi Zhang[3,4*], Zhe Hu[3,4], Jia Li[3,4] and Qun Xu[3,4]

Abstract

Lattice-based digital signature has become one of the widely recognized post-quantum algorithms because of its simple algebraic operation, rich mathematical foundation and worst-case security, and also an important tool for constructing cryptography. This survey explores lattice-based digital signatures, a promising post-quantum resistant alternative to traditional schemes relying on factoring or discrete logarithm problems, which face increasing risks from quantum computing. The study covers conventional paradigms like Hash-and-Sign and Fiat-Shamir, as well as specialized applications including group, ring, blind, and proxy signatures. It analyzes the versatility and security strengths of lattice-based schemes, providing practical insights. Each chapter summarizes advancements in schemes, identifying emerging trends. We also pinpoint future directions to deploy lattice-based digital signatures including quantum cryptography.

Keywords Post-quantum cryptography, Lattice-based cryptography, Lattice-based digital signatures

Introduction

As the advent of quantum computers looms ever closer, the super computing power it provides would cause threats on the security of universally used cryptographic schemes in various application fields by the Shor's algorithm (Shor 1999), this is based on a polynomial-time quantum algorithm proposed by Shor which can be used to factor large integers and solve discrete logarithm problem. Thus, the schemes based on the number-theoretic hard problems and discrete logarithm problem tend to be vulnerable which cover almost all public-key encryption wildly used on the Internet including RSA (Rivest et al. 1978), DSA (National Institute of Standards and Technology 2009), and elliptic-curve cryptography (Breuil and Diamond 2001). For 30 years, Shor's algorithm has been an example of the promise of quantum computers. Until Oded Regev, recently proposes a scheme (Regev 2023) that drastically reduces the number of gates or logical steps needed to factor extremely large numbers, which is the first substantial improvement of Shor's algorithm in 30 years. In principle, it could allow a smaller quantum computer to figure out the encryption key, or a larger machine to decode the encryption key more quickly. On the other hand, his work means that the age of quantum computers may come sooner. This has sparked a frenzy of research into post-quantum cryptography (PQC), among the four main areas in post-quantum research (Multivariate, code-based, hash-based, and lattice-based), lattice-based cryptography is undoubtedly the most concerned because it is based on the mathematically rigorous computational problems which lead to reliable and verifiable. The computational problems CVP and SVP show the quantum resistance (Ajtai et al. 2001; Dinur et al. 1998) which makes lattice-based cryptography a promise in post-quantum era.

In recent years, the field of lattice-based cryptography has experienced significant growth in theory. NIST

*Correspondence:
Zixian Gong
gzx@ruc.edu.cn
Kun Tian
tkun19891208@ruc.edu.cn
Yi Zhang
ethanzhang@ruc.edu.cn
[1] Institute of Artificial Intelligence, Beihang University, Beijing 100191, People's Republic of China
[2] Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing, Beijing, People's Republic of China
[3] Engineering Research Center of Ministry of Education for Financial Computing and Digital Engineering, Renmin University of China, Beijing 100872, People's Republic of China
[4] School of Mathematics, Renmin University of China, Beijing 100872, People's Republic of China

(National Institute of Standards and Technology) initiated the Post-Quantum Cryptography Standardization Process, in which lattice-based cryptography plays a highly significant role. The emergence of some lattice-based cryptographic schemes here demonstrates higher efficiency compared to traditional schemes based on RSA. In a more specific context, this implementation surpasses a comparable RSA implementation by an order of magnitude in terms of speed, affords a heightened level of security while demanding fewer device resources. Nonetheless, it will take a while before lattice-based schemes start to replace existing public-key cryptography. For instance, ECC was introduced by Miller (1985) and Koblitz (1987), but it took nearly two decades to become integrated into actual secure systems. While the security analysis of cryptographic schemes is an essential consideration, the paramount challenge for lattice-based cryptography thus far has been its practicality.

The digital signature scheme (DSS) (Diffie and Hellman 2022), also called public key digital signature, is a method of identifying digital information similar to an ordinary physical handwritten signature written on paper, but implemented using techniques from the field of public key cryptography. The basic idea comes from Diffie and Hellman (2022), laterly, Rivest et al. (1978) suggested the basic concept of basic signature scheme. Traditionally, the digital signature technology uses an asymmetric algorithm to encrypt the hash private key (owned only by an individual) of the original text through the hash function to generate a digital signature and send it to the recipient together with the original text. The receiver can decrypt the encrypted message only by using the public key of the sender, and then performs the hash operation on the content to obtain the hash value, and compares it with the hash value of the decrypted digital signature. If the comparison results are consistent, it indicates that the received information is complete and has not been modified during transmission, otherwise the information must have been modified. More generally, each person has a pair of “keys” (digital identity), one of which is known only to her/him (private key) and the other is public (public key). The private key is used for signing and the public key is used for verifying the signature. And because anyone can sign it claiming to be you, the public key must be registered with someone the recipient trusts (an identity authority). After registration, the identity authority will issue you a digital certificate. After signing the document, you send the digital certificate, along with the document and signature, to the recipient, who verifies with the authentication authority that the document was actually issued with your key. Hence, based on the definition of DSS, there are many properties for it: publicly verifiable, transferable, non-repudiation. Precisely because of the properties, they are widely applied in fields such as identity verification, financial transactions, blockchain, and cryptocurrencies, and have been given legal validity in many countries.

In order to achieve the properties of digital signatures and ensure the security of signatures, scholars have proposed many signature schemes in recent years. digital signature algorithms include RSA (Rivest et al. 1978; El Gamal 1985; Fiat and Shamir 1986; Guillou and Quisquater 1990; Ong and Schnorr 1990), Des/DSA (National Institute of Standards and Technology 2009), elliptic curve digital signature algorithm (Washington 2008) and finite automata digital signature algorithm. Special digital signatures include blind signature, proxy signature, group signature, undeniable signature, fair blind signature, threshold signature, and signature with message recovery function, which are closely related to the specific application environmentAccording to the basic construction of the scheme, digital signatures can be divided into two paradigms: Hash-and-Sign (Diffie and Hellman 2022; Fiat and Shamir 1986) where the majority of subsequent schemes are designed based on their basic architectures. Building upon these foundational approaches, schemes are optimized and tailored to evolve into various specialized schemes for specific application scenarios such as group signatures and blind signatures. In this article, we only introduce lattice-based (quantum-resistent) digital signatures.

Outline. The main objective of this survey is to provide a comprehensive classification for lattice-based digital signatures. Indeed, classifying digital signatures solely based on hardness assumptions or construction methods might seem monotonous, especially considering their crucial integration with internet applications within the realm of cryptography. This classification of the article encompasses not only the basic structures of signature schemes but also includes specialized schemes tailored for specific application scenarios. Within this, the article will provide introductions to key schemes under each subcategory. The ultimate goal of this review of lattice-based digital signature is not only to prepare for the arrival of the post-quantum era but also serves as a valuable reference for current research in the theory and application of digital signatures. Sect. Preliminaries briefly gives some theoretical prerequisites. Section Notation discusses the **general** lattice-based schemes. Section Digital signature considers the digital signatures for **specialized** application scenarios. Section Lattice makes a conclusion while Sect. Hardness assumptions outlines prospective research areas crucial for advancing lattice-based digital signature.

Preliminaries

In this section, notation for the whole paper is introduced first, and then some basic concepts for digital signature, lattice and hardness assumption are introduced.

Notation

Throughout this paper, the following notation will be used in the following sections, the variations present in certain schemes will be discussed in the subsequent content. All vectors are denoted as bold lowercase letters and are represented as column vectors, while the bold upper case expressing the matrix. The ℓ_p-norm of a vector $\mathbf{b}$ is denoted by $\|\mathbf{b}\|_p$ while the default representation of ℓ_2-norm is denoted by $\|\mathbf{b}\|$. The prime number $q \in \mathbb{N}$ is defined as $q \equiv 1(mod\ 2n)$ where the n is set as $n = 2^k \in \mathbb{N}$ for $k \in \mathbb{N}$. We denoted by $\mathbb{Z}_q$ the finite field $\mathbb{Z}/\mathbb{Z}_q$ where the element is in the range $\left[-\frac{q}{2}, \frac{q}{2}\right)$. We define the ring $\mathcal{R} = \mathbb{Z}[x]/\langle x^n + 1\rangle$ and $\mathcal{R}_q = \mathbb{Z}_q[x]/\langle x^n + 1\rangle$ where all elements can be represented by polynomials of degree $n - 1$. The notation $s \overset{\$}{\leftarrow} \mathcal{S}$ is used to express that an element s is chosen uniformly at random from a set $\mathcal{S}$.

Digital signature

A digital signature system consists of four symbols and three core components, totaling seven parts. For the four symbols, $k \in \mathbb{N}$ is the security parameter of whole DSS, and $\mathcal{M}, \mathcal{S}, \mathcal{H}$ stand for message space, signature space and key space respectively. The core component of DSS is denoted as $\pi = (\mathrm{Gen}, \mathrm{Sign}, \mathrm{Vrfy})$ where the the Gen and Sign are *PPT* (probabilistic polynomial time) algorithms, and Vrfy algorithm is deterministic. For the process of a DSS:

- $(pk, sk) \leftarrow \mathrm{Gen}(1^{\mathrm{k}})$ where the pk, sk represent the public key and secret key respectively.
- $\sigma \leftarrow \mathrm{Sign}(\mathrm{sk}, \mathrm{m})$, $\sigma \in \mathbb{S}$ for m is a message in $\mathcal{M}$. We call the (m, σ) a signature.
- $b \leftarrow \mathrm{Vrfy}(\mathrm{pk}, (\mathrm{m}, \sigma))$, and $b = 1$ or 0. if $b = 1$, we call (m, σ) an efficient signature.

For an adversary, the key aim is to forge a signature with the correct output under the Vrfy algorithm without using the secret key for signing.

In this context, digital signatures are generally categorized into one-time signatures and many-time signatures. As the literal meaning suggests, a one-time signature is designed to perform only a single signing operation, implying that for each signing and verification, a new key pair must be generated. In contrast, many-time signatures allow the usage of the same key pair for signing and verifying multiple messages. One-time signatures are often designed to provide higher security; however, key management poses a challenge compared to many-time signatures.

There are definitions about the properties, we will use at follows, of digital signature:

- Unforgeability: Everyone except the specific participants (proxy signer, group member) can not generate a valid signature.
- Verifiability: The verifier can verify the proxy signature using the verification key of proxy signer.

  And he can know whether the proxy signature is admitted by the original signer.
- Nonrepudiation: The proxy signer can't deny the valid proxy signature signed by him.
- Distinguishability: The proxy signature must distinguishable from the normal signature.
- Non-frameability: An attacker cannot generate the signature used by an opener from a valid signature to expose the identity of an honest signing group member.
- Tracing soundness: The opener reveals the signer of a signature, the attacker cannot generate a signature that belongs to two different group members.
- Identifiability: Anyone can identify the proxy signer from the original singer through a proxy signature.
- Linkability: The ability to anonymously verify whether two signatures havebeen signed by the same signer, and this is one of the most widely used applicationsof ring signatures

Lattice

One of the keys for lattice-based cryptography is the structure for lattice. In this subsection, some basic knowledge and definitions for lattice will be introduced. We can refer Zheng et al. (2023) for more detail of lattice.

A lattice is a discrete additive subgroup of the vector space with a *minimum distance*. Given a set of linearly independent vectors $\mathbf{b_1}, \mathbf{b_2} \ldots \mathbf{b_n} \in \mathbb{R}^m$ as the basis of a lattice $\mathcal{L}$. The lattice $\mathcal{L}$ generated by $\mathbf{b_1}, \mathbf{b_2} \ldots \mathbf{b_n}$ is the set

$$\mathcal{L}(\mathbf{b_1}, \mathbf{b_2} \ldots \mathbf{b_n}) = \{\sum_{i=1}^{n} a_i \mathbf{b_i} : a_i \in \mathbb{Z}\}. \tag{1}$$

The vectors $\mathbf{b_1}, \mathbf{b_2} \ldots \mathbf{b_n}$ can be seen as column vectors, then the basis can be seen as a matrix $\mathbf{B}$ where the integers n and m are the rank and dimension of the lattice. The *minimum distance*λ is defined as the length of the shortest non-zero vector $\mathbf{x}$, ie,

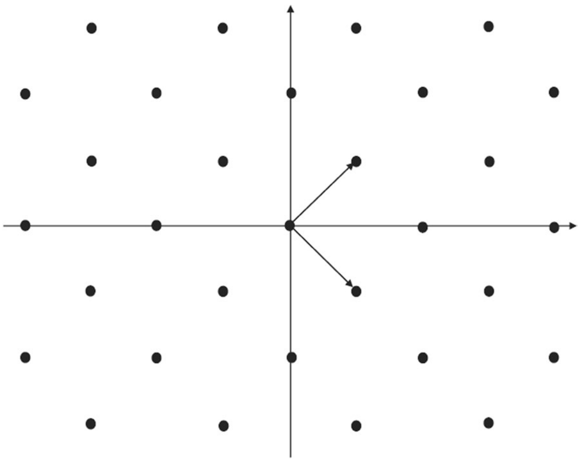


Fig. 1 Lattice in 2-dimension space

$$\lambda = min\{\|x\| | x \in \mathcal{L}, x \neq 0\}. \tag{2}$$

According to the definition, it can be observed that a lattice is an additive subgroup composed of discrete lattice points. For example, a lattice in 2-dimension generated by basis $\{(1,1),(1,-1)\}$ is shown in Fig. 1.

One important thing to note is that a lattice can be generated by two different sets of basis vectors.

In cryptography, besides the standard lattice structures, we often explore schemes based on special lattices such as cyclic lattices, q-ary lattices, ideal lattices, and NTRU lattices (Zheng and Liu 2022). These lattice structures frequently offer stronger security assumptions along with shorter public keys or signatures. For specific details, refer to Zheng et al. (2023).

Hardness assumptions

This section introduces some of the most commonly used hardness assumptions in cryptographic schemes.

Computational problems

SVP − Shortest Vector Problem. Given a lattice basis $\mathbf{B} \in \mathbb{Z}^{m\times n}$, find a non-zero lattice vector $\mathbf{Bx}$ such that $\|\mathbf{Bx}\| \leq \|\mathbf{By}\|$ for any other $\mathbf{y} \in \mathbb{Z}^n \setminus \{0\}$.

CVP − Closest Vector Problem. Given a lattice basis $\mathbf{B} \in \mathbb{Z}^{m\times n}$ and a target vector $\mathbf{t} \in \mathbb{Z}^m$, find the $x \in \mathbb{Z}^n$ such that $\|\mathbf{Bx} - \mathbf{t}\|$ is minimum.

The above two problems also have approximate relaxed versions with a factor γ.

Approximate SVP$_\gamma$. Given a lattice basis $\mathbf{B} \in \mathbb{Z}^{m\times n}$, find a non-zero lattice vector $\mathbf{Bx}$ such that $\|\mathbf{Bx}\| \leq \gamma \cdot \|\mathbf{By}\|$ for any other $\mathbf{y} \in \mathbb{Z}^n \setminus \{0\}$.

Approximate CVP$_\gamma$. Given a lattice basis $\mathbf{B} \in \mathbb{Z}^{m\times n}$ and a target vector $\mathbf{t} \in \mathbb{Z}^m$, find the $x \in \mathbb{Z}^n$ such that $\|\mathbf{Bx} - \mathbf{t}\| \leq \gamma \cdot \|\mathbf{By} - \mathbf{t}\|$ for any other $\mathbf{y} \in \mathbb{Z}^n$.

Apart from the precise and approximate formulations, it is also possible to articulate these problems as promises called **GapSVP$_\gamma$** and **GapCVP$_\gamma$**.

Average-case lattice problems

This section will introduce two main problems, SIS (Short Integer Solution) and LWE (Learning With Errors), along with their specific variants.

SIS. Let n, m and q be positive integers and β be a positive real number smaller than q. $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is a randomly generated matrix following a uniform distribution and formed by m independent vectors $a_i \xleftarrow{\$} \mathbb{Z}_q$. The problem **SIS**$_{n,q,\beta,m}$ asks to find a shortest integer solution $z \in \mathbb{Z}^m$ such that:

$$\mathbf{A}z \equiv 0\ (mod\ q),\ z \neq 0,\ \|z\| \leq \beta. \tag{3}$$

LWE distribution. Let n and q be positive integers and let χ be a distribution over $\mathbb{Z}$. For a fixed secret $\boldsymbol{s} \in \mathbb{Z}_q^n$, the LWE distribution $A_{\boldsymbol{s},\chi} = (\boldsymbol{a}, b)$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is defined with $b = \langle \boldsymbol{a}, \boldsymbol{s}\rangle + e\ mod\ q$ where $\boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n$, and the error (or noise) $e \leftarrow \chi$.

There are two distinct variations of the LWE problem which are Search LWE and Decisional LWE problems. The first ask to find the secret $\boldsymbol{s}$ with high probability while another version asking to distinguish between the LWE distribution and the uniform distribution.

Search LWE. Given m independent samples $(\boldsymbol{a}_i, b_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ from $A_{\boldsymbol{s},\chi}$ and $e_i \leftarrow \chi$ for $1 \leq i \leq m$. The problem $\mathbf{S-LWE}_{n,q,\chi,m}$ asks to obtain the secret $\boldsymbol{s} \in \mathbb{Z}_q^n$ with high probability ($p > 1 - \delta$).

Decisional LWE. Given $\boldsymbol{a} \in \mathbb{Z}_q^n$ and $\boldsymbol{a} \xleftarrow{\$} \mathbb{Z}_q^n, s \in \mathbb{Z}_q^n$ and $e \in \mathbb{Z}_q$ follows the distribution χ. The problem $\mathbf{D-LWE}_{n,q,\chi,m}$ asks to distinguish between $\langle \boldsymbol{a}, \boldsymbol{s}\rangle + e$ and uniform distribution with non-negligible probability.

After the basic definition of SIS and LWE problems, there are module variant for the SIS and LWE problems. The hardness assumptions are done over the ring $\mathcal{R}_q = \mathbb{Z}_q/\langle x^n + 1\rangle$. And the parameters are selected from the $\mathcal{R}_q^d$ and used to generate the **MSIS**$_{d,q,\beta,m}$ and **MLWE**$_{d,q,\chi,m}$ problems. Actually the module problems generalizes plain problems, simply take $n = 1$ and $\mathcal{R} = \mathbb{Z}$. Another special case which is very common in construction of cryptographic scheme where $d = 1$ for module problems, these kind of variants are ring problems denoted by **RSIS**$_{q,\beta,m}$ and **RLWE**$_{q,\chi,m}$ (Lyubashevsky 2009).

Hash function

A **Hash Function** is a pair of probabilistic polynomial-time algorithms (Gen, H) such that (Yung and Katz 2010):

- Gen is a probabilistic algorithm that on input 1^k outputs a key s.
- There exists a polynomial l such that H takes as input a key s and $x \in \{0,1\}^*$, and outputs a string $H_s(x) \in \{0,1\}^{l(k)}$.

If H_s is defined only for inputs $x \in \{0,1\}^{l'(k)}$, where $l'(k) > I(k)$ for all k, then we say that (Gen, H) is a fixed-length hash function for inputs of length l'.

It is worth to say that the property of collision-resistant is very important, and easy to see that collision-resistance implies universal one-wayness.

Conventional lattice-based schemes

For the constructions of lattice-based signatures, there are essentially two paradigms: Fiar-shamir or Hash-and-sign. In this section, the conventional schemes follow the classification. Both paradigms will be discussed.

Hash-and-sign signatures

We will introduce the simplest (and coolest) techniques cryptography: signatures based on hash functions. The definition we have given above, and the most essential property of hash function is collision-resistant, which can satisfy security. Hash signatures are fast and simple, as they only require evaluating the appropriate hash function. From a purely computing cost point of view, hash signatures definitely have the ability to compete with ECDSA, RSA (Rivest et al. 1978), etc., while being very friendly for lightweight devices. But there is a more complex reason for the rise of hash signatures: Most hash signatures are not easily affected by the Shor algorithm. Of course, we're not saying that hash signatures are completely resistant to quantum computing attacks. The most effective quantum attack on hashing is called the Grover algorithm (Nelsen and Chuang 2010), which greatly reduces the security of hashing. However, the security impact of this degree is far less than that of the Shor algorithm (the difference in the cracking time level is between the square and the cube), so the security of the signature can be guaranteed simply by increasing the operation content and output size of the hash function, such as SHA3 (Dworkin 2015).

In 1979, a mathematician Leslie Lamport invented the world's first signature based on a hash function (Lamport 1979). Lamport found that by using simple hash functions, or one-way functions, it was possible to build very powerful digital signature systems. The powerful premise is that the user only needs to do a signature action to ensure security!

We will illustrate it first for the case of signing l-bit messages(SHA256, l=256). Let f be a one-way function. The secret key consists of $2l$ elements $x_{1,0}, x_{1,1}, x_{2,0}, x_{2,1}, , x_{256,0}, x_{256,1}$, in the range of f; Next, to generate the public key, we pass a random string of bits through $H(.)$ Hash operation is performed to obtain the public key $y_{i,0} = H(x_{i,0}), y_{i,1} = H(x_{i,1})$. These keys can be visualized as two-dimensional arrays:

$$sk = \begin{pmatrix} sk_0 \\ sk_1 \end{pmatrix} := \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{256,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{256,1} \end{pmatrix},$$

$$pk = \begin{pmatrix} pk_0 \\ pk_1 \end{pmatrix} := \begin{pmatrix} y_{1,0} & y_{2,0} & \cdots & y_{256,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{256,1} \end{pmatrix}.$$

- Now we can publish the public key(pk_0, pk_1) for everyone. For example, we can send a public key to a friend, embed it in a certificate, or publish it on Keybase.
- We then use the key to sign the l-bit message M. First we have to reproduce the message M as a separate l-bit: $M_1, M_2, \cdots, M_l \in 0, 1$.
- We fetch strings from bits 1 to l of the message M, one by one, corresponding to one of the keys in the key list. The key chosen depends on the value of each bit of the message we want to sign. Specifically, for $i = [1, l]$, if the message bit $M_i = 0$ in bit i, we select the character i $(sk_{i,0})$ from the sk_0 table as part of our signature. If the message bit of bit i is $M_i = 1$, we do the above process from the sk_1 table. After doing this for each message bit, we concatenate the selected string to get a signature.
- When a user (who already knows the public key (pk_0, pk_1) receives the message M and the signature, she can easily verify the signature. We represent the i-th component of the signature as s_i, and the user can examine the corresponding message M_i and calculate the hash value $H(s_i)$. If M_i= 0, the hash must match the elements in the public key pk_0; If $M_i = 1$, the hash must match the elements in public key pk_1. If each element in the signature is hashed to find the corresponding public key for the correct part, we say that the signature is valid.

There are two drawbacks for the Lamport one-time digital signature: The signature and key for the Lamport method is simply too large, about the thousands of bits. What's more, this approach has serious security limitations: each key can only be used to sign one message, so the Lamport method is used here as an example of a “one- time signature”. There have been many subsequent optimizations for Lamport one-time digital signature. To address the inability to sign multiple messages with a single key, Ralph Merkle proposed a new DSS based on Merkle’s tree (Merkle 1980). Roughly speaking, the Merkle method provides a way to collect different values and represent the collected values with a “root” hash. Given this root hash, you can simply “prove” that an element exists in the given hash tree. And the size of the proof is paired with the number of leaf nodes. Merkle’s method transforms a one-time signature into an n-order signature. Constructing this method is still based on some one-time signature method, such as the Lamport method which is still relatively expensive.

Later, Robert Winternitz proposed a further upgrade DSS (Winternitz 1984) based on the Merkle method described above. In practice, this approach reduces the signature and public key size by a factor of four to eight, at the cost of increasing the time it takes to sign and verify. Winternitz’s idea came from a technique called time-space tradeoff, which could reduce space requirements at the expense of increasing computing time (and vice versa).

sOne limitation to all of the above methods is that they require signers to maintain state between signatures. In 1980s, Goldreich and Levin (1989) pointed out that there is a way to create a signature that does not need to be maintained. Generating a short “verification tree” of one-time public keys instead of all the keys up front. Each key can sign additional one-time public key at the bottom of the tree. If a single seed is used to generate all the private keys, it means that the full Merkle tree does not need to exist at key generation, but can be built on demand when new keys are generated. Each signature contains a “verification chain” of signatures and public keys. From the root node to the key pair that the leaf node is actually used to sign. This technique allows us to build exponential numbers of keys in very “deep” Merkle trees (Bernstein et al. 2015). It is worth mentioning that Melissa et al. proposed a completely different idea of Picnic (Chase et al. 2017), based on a new non-interactive zero-knowledge proof system technology called ZKBoo, which is a new ZK proof system based on “MPC in the mind” that lets prover self-prove using multi-party copmputations.

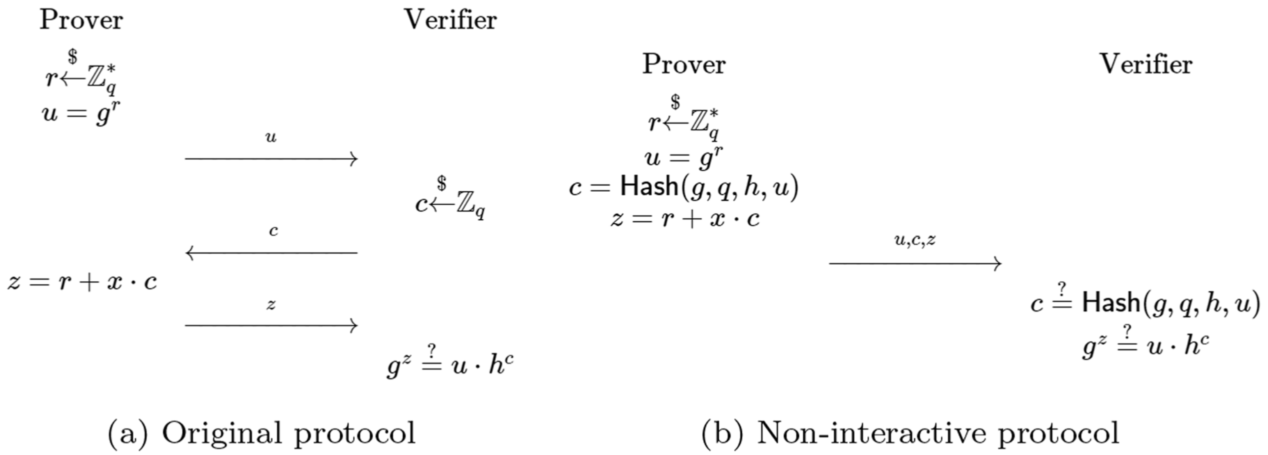
At STOC 2008, Gentry et al. (2008) rectified a flawed signing procedure, introducing the GPV framework for secure lattice-based hash-and-sign signatures. Stehlé and Steinfeld (2011) later enhanced this paradigm by merging the GPV framework with NTRU lattices. In a practical application, Ducas et al. (2014) instantiated the IBE part of the GPV framework over NTRU lattices. The 2019 Falcon scheme, a leading candidate in NIST’s Post-Quantum Cryptography Standardization Process, builds on these foundations, incorporating NTRU lattice (Stehlé and Steinfeld 2011) and Fast Fourier sampling (Ducas and Prest 2016) for impressive efficiency and security.

Fiat-shamir signatures

Instead of using the Hash and Sign signature approach, an alternative method to construct a digital signature scheme involves transforming a specific type of identification scheme into a signature scheme through the Fiat-Shamir transformation (Abdalla et al. 2002; Fiat and Shamir 1986), first introduced in Shamir (1985). The Fiat-Shamir transformation allows a typical authentication system with passive security can be transformed into a signature system under a random model. This transformation is employed to convert a zero-knowledge protocol into a digital signature scheme. In zero-knowledge protocols, a prover aims to convince a verifier of their identity without revealing any specific information. This interactive process involves the verifier repeatedly challenging the prover until convinced. However, this interactivity poses a problem, as bystanders cannot ensure there is no collusion between the parties in advance. To address this, the Fiat-Shamir technique enables the transformation of the interactive protocol into a non-interactive one. It achieves this by allowing the prover to compute a value using a random function (like a cryptographic hash function) instead of relying on the verifier to send a random challenge value.

Schnorr’s identification protocol (Schnorr 1990) is the simplest example of a zero-knowledge protocol which is aimed at convincing verifier that the prover knows the discrete logarithm x of some value $h = g^x$ without revealing x. The steps are listed as Fig. 2. The hidden theory is: $g^z = g^{r+x\cdot c} = g^r gx \cdot c = u \cdot h^c$. For the non-interactive protocol, the above process is reduced to just two steps, the challenge c is now created by hashing all the public values $\{g, q, h, u\}$. The above two schemes are illustrated in Fig. 2.

After the concept of Random Oracles is proposed (Bellare and Rogaway 1993), the verifier in the identification scheme can be replaced by a random oracle. Although the Fiat-shamir transform was proposed earlier, the lattice-based fiat-shamir scheme (Lyubashevsky 2009) was not proposed until the safety and complexity of some related concepts were discussed (Goldwasser et al. 1989; Chase and Lysyanskaya 2006). Most lattice-based Fiat-shamir signatures follow Lyubashevsky’s “Fiat-Shamir with aborts” paradigm (Lyubashevsky 2009), which ensures that the identification scheme used by Fiat-shamir transformation achieves honest-verifier zero-knowledge by rejecting sampling. The Lyubashevsky


Prover
Verifier
$r \xleftarrow{\$} \mathbb{Z}_q^*$
$u = g^r$
u
$c \xleftarrow{\$} \mathbb{Z}_q$
c
$z = r + x \cdot c$
z
$g^z \overset{?}{=} u \cdot h^c$
Prover
Verifier
$r \xleftarrow{\$} \mathbb{Z}_q^*$
$u = g^r$
$c = \mathsf{Hash}(g, q, h, u)$
$z = r + x \cdot c$
u,c,z
$c \overset{?}{=} \mathsf{Hash}(g, q, h, u)$
$g^z \overset{?}{=} u \cdot h^c$

(a) Original protocol

(b) Non-interactive protocol

Fig. 2 Schnorr's identification protocol

signature scheme constructs an identity-based signature scheme on the lattice, based on the SIS on a lattice, Lyubashevsky et al. gave a quantum reduction from the approximate SVP (worst-case) on an ideal lattice in R to the search version of R-LWE. Compared with other effective schemes, the proposed scheme has advantages in computational complexity and security. The practicality of a digital signature scheme is crucial. Lyubashevsky's subsequent improvements (Lyubashevsky 2012) focus on two key areas: Firstly, the hardness assumption transitions from single ring-SIS to a combination of Ring-SIS and Ring-LWE(Once proposed, RLWE has become a frequent visitor in the construction of public key cryptosystems, and the most common is the construction of full-homomorphic encryption). This change drastically reduces the size of public keys and signatures, leading to a notable efficiency boost. Secondly, the signing procedure now requires a more intricate rejection sampling, ensuring the independence of signatures from the secret. However, due to the high precision demanded by this process, which may be challenging to support in hardware, both schemes require optimization for practical implementation. They tend to be surpassed by a series of highly effective and practical schemes like GLP, BLISS, and ring-TESLA (Güneysu et al. 2012; Ducas et al. 2013; Akleylek et al. 2016).

Since the introduction of cyclic and ideal lattices (Micciancio 2007), along with related computationally hard problems like Ring-SIS (Lyubashevsky and Micciancio 2006; Peikert and Rosen 2006) and Ring-LWE (Lyubashevsky et al. 2010), lattice-based signature schemes have struck a favorable balance between signature and key sizes, as well as security. This work (Güneysu et al. 2012) presents a provably secure digital signature scheme based on ideal lattices and a variant of decisional Ring-LWE called decisional compact knapsack (DCK) problem which means that the adversary needs to distinguish between the uniform random distribution over $\mathcal{R}_q \times \mathcal{R}_q$ and the LWE distribution $(\mathbf{a}, \mathbf{as_1} + \mathbf{s_2})$ where the $\mathbf{a}$ is selected from $\mathcal{R}_q$ uniformly and the $\mathbf{s_1}, \mathbf{s_2}$ are chosen uniformly from $\mathcal{R}_{q,k}$ which is expanded from $\left[-\frac{q}{2}, \frac{q}{2}\right)$ to $[-k, k)$. The security level which was claimed in this work about 100-bits, but it was estimated to be around 80 bits actually in Ducas et al. (2013).

Due to the absence of the algorithm for sampling from Gaussian distribution without requiring a large look-up table, the Gaussian distribution was usually avoided for lattice-based schemes leading to less compact as they could be in theory (Güneysu et al. 2012). Thus, the BLISS scheme (Ducas et al. 2013) made a modification in the rejection sampling stage which is seen as the core part of Lyubashevsky's scheme (Lyubashevsky 2012) and GLP scheme (Güneysu et al. 2012) which changed the sample method from the discrete Gaussian distribution and uniform random to a bimodal Gaussian distribution while the hardness assumption of the scheme is Ring-SIS problem. For an adversary who need to forge a signature, it is hard to obtain the secret key $\mathbf{S}$ from public parameter where $\mathbf{AS} = q\mathbf{I}\ (mod\ 2q)$ because of the Ring-SIS problem. However, despite the advantages offered by the Gaussian distribution, there are notable drawbacks. Firstly, the scheme incurs high computational costs due to intricate operations like exponential functions. Secondly, the Gaussian sampling process is assumed to be susceptible to timing attacks (Bos et al. 2015; Dagdelen et al. 2014).

Many practical schemes enhance performance at the cost of security, resulting in a non-tight security reduction. Before ring-TESLA (Akleylek et al. 2016), predecessors like TESLA (Alkim et al. 2015) improved Bai and Galbraith's work (Bai and Galbraith 2014) by tightening the security reduction process. TESLA (Alkim et al.

2015) introduced a standard-lattice based signature scheme grounded in the decisional LWE problem with a tight security reduction. The forking lemma (Pointcheval and Stern 2000), introduced by Pointcheval and Stern, provides either a genuine or fabricated public key for a hypothetical adversary. While a powerful tool for proving signature security, it has drawbacks: it leads to a non-tight security reduction and doesn't address situations involving quantum adversaries. To bypass these issues, schemes like Alkim et al. (2015) and Abdalla et al. (2015) avoid the forking lemma and use a different proof idea from Katz and Wang (2003). Both schemes perform worse in terms of running time and key sizes compared to BLISS and GLP. Ring-TESLA is poised to improve these aspects. The scheme ring-TESLA is based on the Ring-LWE problem and has a good performance with provable security instantiation.

The three schemes mentioned above can be considered the most efficient and practical lattice-based Fiat-Shamir signatures over the past decade. In order to address the challenge of efficiently and securely implementing the Gaussian distribution, the NIST candidate scheme Dilithium (Ducas et al. 2018) adopts a uniform distribution. This enhancement reduces the public key size by a factor of 2.5 compared to previously efficient lattice-based schemes using a uniform distribution, all while maintaining the same security level and signature size. The main architecture of this scheme follows the modified version of the scheme (Bai and Galbraith 2014). The hardness assumptions of the scheme are MLWE and MSIS lattice problems. Besides, in order to reduce the running time of the procedure, small element such as x will not be stored during the calculation process like $r + x$, to achieve this goal, some auxiliary tools such as Decompose_q, HighBits_q and LowBits_q will be used to obtain the High/Low order bits of parameters.

As the most practical and reasonably secure schemes, they have high-practicability in various fields such as FPGAs, reconfigurable hardware, CPUs and microcontroller. The Table 1 concludes the security level and rough performance (the table is concluded from the work (Ducas et al. 2013; Akleylek et al. 2016), The size column was benchmarked under different hardware environments, it should only be considered as rough suggestion) for the Fiat-shamir schemes mentioned above.

Table 1 Scheme overview table

Scheme	Assumption	Security	pk+sig size
GLP	DCK	80-bits	21.5 kb
BLISS-I	R-SIS	128-bits	12.6 kb
BLISS-II	R-SIS	128-bits	12 kb
BLISS-III	R-SIS	160-bits	13 kb
BLISS-IV	R-SIS	192-bits	13.5 kb
ring-TESLA-I	R-LWE	80-bits	36.5 kb
ring-TESLA-II	R-LWE	128-bits	36 kb
Dilithium	MLWE, MSIS	128-bits	15 kb

Based on the development of schemes in this section, we can draw a rough conclusion: there exists a transition from constructing schemes based on SIS to those based on LWE under certain hard assumptions. Additionally, the underlying hard assumptions progress from standard lattice problems to ring-based problems, and ultimately to generalized module lattice problems. However, throughout, the common objective of all these schemes is to strike a balance between security and efficiency in order to construct a practical, efficient, and secure digital signature scheme.

Specialized lattice-based schemes

Digital signatures have a wide range of applications, which has led to the emergence of specific types of digital signature schemes for particular scenarios. This section introduces some types of digital signatures tailored for specific contexts, which may draw inspiration from or incorporate constructs from Conventional digital signature schemes.

Group signatures and ring signatures

The group signature is a specialized digitial signature scheme first proposed by Chaum and Van Heyst at the Eurocrypt conference in 1991 (Chaum and Van Heyst 1991). A group signature is a type of digital signature where each member of the group can sign on behalf of the entire group in an anonymous manner. Group signatures possess two fundamental properties: anonymity, and traceability. Anonymity means that anyone receiving a signed message can verify that comes from a member of the group without knowing the specific identity of the signer. Traceability signifies that the group manager can, when necessary, reveal the specific identity of the member who generated a signature. The security of schemes mentioned in Chaum and Van Heyst (1991) are based on the difficulty of factoring and discrete logarithm problems for large integers which seems a bit weak in the post quantum era.

The group signature scheme, after being proposed, experienced rapid development. In 1995, a group signature scheme that allows the dynamic addition of new members after the setup phase named partially dynamic group signatures was introduced (Chen and Pedersen 1994). However, in the provided schemes, both the public key size and the signature size are directly proportional to the number of members within the group, which is highly disadvantageous for groups with a large number of members. Therefore, in 1997, a CS97 group signature scheme was proposed, which is independent of both signature and group public key size with respect to the number of group members (Camenisch and Stadler 1997), along with the ACJT group signature scheme introduced in 2000 (Camenisch and Stadler 1997; Ateniese et al. 2000), still rely on traditional classical number theory problems. However, in 2000, reference Kim et al. (2001) first introduced a fully dynamic group signature where group members can actively choose to leave the group or group administrators can choose to revoke group members and then in 2003, the BMW model was introduced (Bellare et al. 2003), providing a theoretical definition for static group signatures. Until 2010, Gordon and Katz, among others, introduced the first lattice-based group signature scheme (Gordon et al. 2010). This marked the fusion of group signatures with lattice theory. The scheme was built upon the BMW model and further integrated zero-knowledge proof techniques and lattice theory. However, this scheme had long key and signature lengths. Subsequently, many efforts were made to reduce the key and signature lengths, but most of these schemes lacked mechanisms for adding or revoking members. It wasn't until 2016 when Bootle et al. proposed a fully dynamic signature scheme with strict security definitions (Bootle et al. 2016). However, this scheme was not based on lattice-based group signatures. Also in 2016, another paper (Libert et al. 2016) constructed a lattice-based group signature scheme with an adding mechanism, but the joining process was overly complex and time-consuming, and it did not support the revocation of group members. In 2017, reference Ling et al. (2017) constructed a lattice-based fully dynamic group signature with both adding and revocation mechanisms using a Merkle's hash tree. However, it suffered from long update times. Subsequent research papers still did not fully address the issues of complexity and lengthy update times in the joining and revocation processes. Therefore, lattice-based fully dynamic group signatures continue to hold research value.

We selected a range of lattice-based group signature schemes, some of which are static, some partially dynamic, and others fully dynamic. We compared their adherence to the signature size, group public key size, and secret key size in Table 2 as well as security properties mentioned above together with blind signatures and proxy signatures in Table 4 in the Conclusion section.

For the static group signature scheme, the first proposal for lattice-based group signatures, was introduced (Gordon et al. 2010) in 2010. It is based on the hard problem of LWE and provides security properties such as Anonymity and Traceability. The signature size and the number of group members are linearly related, with the signature size being $O(\lambda^2 N)$, the Group Public-key size being $O(\lambda^2 N)$, and the Signing-key size being $O(\lambda^2)$. In reference Laguillaumie et al. (2013), improvements were made to the signature size, constraining the relationship between signature size and the number of group members to logarithmic terms. Specifically, the signature size is $O(\lambda logN)$, the Group Public-key size is $O(\lambda^2 logN)$, and the Signing-key size is $O(\lambda^2)$. This scheme is based on the hard problems of LWE and SIS and provides security properties of full anonymity and traceability. Furthermore, in the paper from 2020, denoted as Luo and Jiang (2020), a scheme based on the RLWE and RSIS hard problems was introduced. It still maintains security properties like Anonymity and Traceability. In terms of signature size, significant improvements were made to achieve constant relationships. The corresponding sizes are $O(\lambda log^3 N)$ for the signature size, $O(\lambda log^2 N)$ for the Group Public-key size, and $O(\lambda log^2 N)$ for the Signing-key size.

In 2016, Libert et al. constructed a Lattice-based partially dynamic group signature (Libert et al. 2016) based on the LWE and SIS problems. However, in terms of security, it only satisfies anonymity and does not meet the requirements for traceability and non-frameability. Concerning the relationship between signature size and the number of group members, it follows a logarithmic pattern. The signature size is $O(\lambda logN)$, the group public-key

Table 2 The signature size, key sizes and Relationship between signature and *N* for schemes

Scheme	Relationship	sig size	gpk size	sk size
Gordon et al. (2010)	Linear	$O(\lambda^2 N)$	$O(\lambda^2 N)$	$O(\lambda^2)$
Laguillaumie et al. (2013)	Logarithmic	$O(\lambda logN)$	$O(\lambda^2 logN)$	$O(\lambda^2)$
Luo and Jiang (2020)	Constant	$O(\lambda log^3 N)$	$O(\lambda log^2 N)$	$O(\lambda log^2 N)$
Libert et al. (2016)	Logarithmic	$O(\lambda logN)$	$O(\lambda^2 logN)$	$O(\lambda)$
Ling et al. (2018)	Constant	$O(\lambda)$	$O(\lambda)$	$O(\lambda)$
Xie et al. (2019)	Linear	$O(N)$	$O(N)$	$O(\lambda)$
Sun et al. (2019)	Logarithmic	$O(\lambda + log\lambda logN)$	$O(\lambda + log\lambda logN)$	$O(\lambda + log\lambda logN)$

size is $O(\lambda^2 N)$, and the signing-key size is $O(\lambda)$. In 2018, a lattice-based partially dynamic signature scheme based on RLWE and RSIS was proposed (Ling et al. 2018). This scheme achieves full anonymity, traceability, and non-frameability, with both signature size and key size being constant. All three sizes are $O(\lambda)$.Regarding lattice-based fully dynamic group signatures.Based on the LWE and SIS, one scheme was proposed (Xie et al. 2019) that achieves full anonymity, traceability, and non-frameability. However, it does not satisfy tracing soundness, and the signature size increases linearly with the number of group members. Another article based on RLWE and RSIS improved upon this (Sun et al. 2019), and it also satisfies tracing soundness in terms of security. The sizes follow a logarithmic relationship, all being $O(\lambda + log\lambda logN)$. In a reference from 2021 (Abhilash and Amberker 2021), a scheme based on LWE and SIS was proposed that improved the size to constant terms, namely $O(\lambda)$, $O(\lambda^2)$, and $O(\lambda)$ respectively. However, it does not meet the requirement of tracing soundness in terms of security. We can observe that subsequent schemes have consistently aimed to reduce the size of both group signatures and group keys. This reduction has progressed from linear relationships to logarithmic ones, and in some cases, even to constant sizes. Some schemes may compromise certain security attributes, while others manage to strike a balance. Therefore, the challenge of minimizing the size of group signatures and keys while maintaining security remains an important area of research for the future.

Ring signature, as a special form of group signature, was proposed by Rivest and others in 2001 (Rivest et al. 2001), addressing the issue of achieving anonymous digital signatures. What sets it apart from group signatures is that in ring signatures, there is no group manager. Verification of the signature does not disclose the specific members' identities. As the combination of ring signatures and threshold signatures which means a signature can only be generated only when the number of cooperating members in the signing process reaches a threshold value. In 2002, Bresson et al. introduced the first threshold ring signature based on threshold concepts (Bresson et al. 2002). In 2005, Awasthi et al. proposed identity-based ring signatures and proxy ring signature schemes (Awasthi and Lal 2005). In 2008, a weakly linkable ring signature scheme that allows for selective linkability was introduced (Jeong et al. 2008). Subsequently, the number of ring signature schemes in post-quantum cryptography, resistant to quantum attacks, started to increase. In 2012, the first threshold ring signature scheme based on multivariate cryptography was introduced by Petzoldt et al. (2013). In 2018, Baum et al. proposed a linkable ring signature scheme based on the SIS and LWE problems (Baum et al. 2018). In 2021, a lattice-based and identity-based linkable ring signature scheme utilizing trapdoors and rejection sampling techniques was introduced, reducing time overhead (Tang et al. 2021).

As ring signatures are a special form of group signature, their definitions and security properties are essentially consistent with the aforementioned content. Linkability is the opposite of unlinkability, refers to the ability to anonymously verify whether two signatures have been signed by the same signer, and this is one of the most widely used applications of ring signatures which establish connections between different signatures, enabling them to be audited or traced when necessary. Scheme (Baum et al. 2018) is based on the lattice-based RSIS hard problem, while reference Tang et al. (2021) is based on the NTRU SIS problem. Ring signatures can be applied in various fields such as vehicular networks, medical data sharing, anonymous voting, and many others. Lattice-based ring signatures that are resistant to quantum attacks are still in the developmental stage. Furthermore, efficiency issues arise when the group size becomes too large. Constructing more efficient ring signature schemes remains a challenge.

Blind signatures

In order to improve the lack of security in automatic payment systems, Chaum (1983) proposed a new cryptographic concept, blind signature, in 1982. Blind signature scheme consists of the interaction process between a user and a signer, that is, the user first performs a blind transformation to mask the original message, and then sends the transformed message to the signer to sign with the public key. In the end, the user performs a reverse transformation to obtain the signature corresponding to the original message. This signature scheme ensures that the signer does not know which messages have been signed, and the signer cannot track which signature was obtained by which signing process.

As a result, blind signature, by virtue of its blindness and unforgeability, is widely used in fields such as e-voting (Shao et al. 2021; Cruz and Kaji 2017), e-cash (Li et al. 2017; Aboud and Al-Fayoumi 2007), and so on, where the privacy of the message provider needs to be protected. Taking the goal first envisioned by Chaum (1983) for automated payment systems as an example, a blind signature scheme enables a payment system to have the following properties: Inability of third parties to determine payee, time or amount of payments made by an individual; Ability of individuals to provide proof of payment, or to determine the identity of the payee under exceptional circumstances; Ability to stop using of payments media reported stolen.

In 1994, Camenisch et al. (1995) first proposed a blind signature scheme based on the discrete logarithm problem. The paper presents two completely new schemes, one derived from a variant of DSA (Wang and Hou 2019) and the other based on the Nyberg Rueppel's signature scheme (Nayak et al. 2017). Due to the early introduction of this scheme, its accuracy and efficiency have not been estimated and analyzed in the paper. But since then, many blind signature schemes based on discrete logarithm problem or integer factorization problem have emerged. For example, in 1995, Harn (1995) also gave a blind signature scheme based on the discrete logarithm problem, and proposed the definition of strong blind signature, which led to further discussion and development of blind signature schemes. Meanwhile, the formal security definition of blind signature was proposed by Pointcheval and Stern (1996) in 1996, which states that the security of blind signature includes blindness and one-more unforgeability.

With the emergence and development of quantum computers, the security of blind signature schemes based on classical number theory problems is significantly reduced, which brings great challenges to this field. However, among the post-quantum cryptosystems, lattice-based cryptosystems have unique advantages. Ajtai (1996) once pointed out that the random instances of lattice problem have the same difficulty as the worst-case instances, which is also the biggest advantage of lattice-based cryptosystems compared with other cryptosystems. Moreover, there is no quantum algorithm that can solve the lattice problem, so lattice-based cryptography has a broad application prospect. Due to the above theoretical advantages of lattice-based cryptosystems, scholars at home and abroad have begun to study lattice-based blind signature schemes to defend against quantum attacks.

In 2010, Rückert (2010) proposed the first lattice-based blind signature scheme, which introduced Lyubashevsky's filtering technique (Lyubashevsky 2009), and also adopted the reject sampling algorithm based on the Fiat-Shamir construction to terminate the signing process when the output may leak the private key or the initial message. It has quasi-linear complexity, security and unforgeability in random oracle model depending on ISVP problem. In the same year, Wang et al. (2010) optimized the blind signature algorithm using a preimage sampling function, so that the blind signature scheme can be implemented through only two rounds of interactions, which performs better than Rückert's scheme (Rückert 2010) and satisfies both blindness and unforgeability. In 2012, Gu et al. (2012) devised an ID-based signature scheme from lattices and gave its blind signature version, which ensures that the scheme has unforgeability and blindness in the random oracle model, while generating shorter private keys and signatures. In 2017, Gao et al. (2017) proposed two ID-based blind signature schemes from lattices, which were built in the random oracle model and the standard model respectively. Both signature construction schemes were proved to be unforgeable and unconditionally blind against selective identity and chosen message attack (SID-CMA). In the same year, Tang et al. (2017) also proposed an ID-based blind signature scheme in the standard model. In this scheme, the basis delegation algorithm is used to generate the corresponding private key according to the user identity, and the forward sampling algorithm is used to sign the message. The scheme satisfies one-more unforgeability and security depending on SIS problem. In 2018, Zhu et al. (2018) proposed an ID-based blind signature scheme on NTRU lattice, which mainly uses a reject sampling theorem instead of constructing a trapdoor, as a way to ensure that the scheme has security in the random oracle model with the advantages of confidentiality, integrity and non-repudiation. However, a security vulnerability was found in this scheme by Singh and Padhye (2020) in 2020 and an improved scheme was given. Later in 2021, Li et al. (2021) proposed a lattice-based blind signature scheme on blockchain system, which uses bimodal Gaussian distribution and reject sampling to sign, which has blindness and one-more unforgeability in the random oracle model and improves the probability of successful signing. In 2022, Lyubashevsky et al. (2022) proposed a two-round optimal lattice-based blind signature scheme. The scheme used Gaussian-generated secret keys and a one-time signature system, which can generates signatures with the length of 150 KB. The scheme seems to be the most efficient blind signature candidate at present.

With the continuous development of blind signature technology, its related extension concepts and composite technical schemes have been widely promoted. In 1996, Abe and Fujisaki introduced the concept of partially blind signature (Abe and Fujisaki 1996). Partially blind signature allows the signer to embed public information in the signature that has been negotiated with the user in advance and that cannot be removed or illegally modified. Therefore, partially blind signature can be regarded as a general form of blind signature. Due to the broad application prospects of partially blind signature in the fields of e-cash and e-voting, it has been widely concerned by scholars. In 1998, Lysyanskaya and Ramzan (1998) proposed the concept of group blind signature, which skillfully combined blind signature with group signature, and could be applied to the scenarios such as multi-bank development of e-cash. In 2000, Lin and Jan (2000) proposed proxy blind signature for the first time by combining proxy signature and blind signature. These

Table 3 The signature size, security model and move for schemes

Scheme	sig size	Security Model	Move	unforgeability
Rückert (2010) (n=2048)	$(n+m)logq$	Random Oracle	4	YES
Wang et al. (2010)	$mlogq$	Random Oracle	2	YES
Gao et al. (2017)	$mlogq$	Standard Model	2	YES
Tang et al. (2017)	$mlogq$	Standard Model	2	YES

concepts have enriched the usage scenarios of blind signature and made blind signature play an important role.

Many landmark schemes have emerged during the development of blind signatures, and the following is a detailed description of blind signature schemes, taking the (Rückert 2010) scheme, which first proposed the concept of lattice-based blind signature, and the scheme designed by Wang et al. (2010) as examples. In Rückert (2010), the time complexity and space complexity of this scheme on the ideal lattice are both close to the current optimal, which are $O(n)$. It also shows that the execution time of each algorithm step of the proposed scheme is shorter when the lattice dimension is higher, and it is even and significantly less than the running time of the other two schemes. From the aspect of security, the scheme is statistically blind and that it is one-more unforgeability unless the collision problem $Col(H(R, m), D)$ is easy.

Subsequently, Wang et al. (2010) constructed a 2-round lattice-based blind signature scheme, using the preimage sampling function proposed by Gentry et al. (2008), which is a further optimization of R$\ddot{u}$ckert's scheme. In terms of efficiency, the results show that this scheme outperforms R$\ddot{u}$ckert's scheme in the number of interactions rounds and the size of the signature. In addition, R$\ddot{u}$ckert's scheme uses commitment to ensure that the message is blind to the signer when the signature fails, whereas the proposed scheme can effectively prevent the signature from failing, thus allowing the adoption of a secure hash function instead of commitment to further simplify user operations. As for the security, the proposed blind signature scheme is blind and unforgeable under the SIS problem, and relevant proof is given.

There is a table conclude the basic information for four lattice-based blind signature schemes (Table 3).

Proxy signatures

The concept of proxy signature was first introduced by Mambo et al. (1996) in 1996. The motivation of the proposal of proxy signature is to implement secure delegation of signature authority, that is, by introducing a proxy signer that can sign on behalf of the original signer, and the proxy cannot forge the signature of the original signer. According to the degree of authorization of signature, proxy signature can be classified into fully authorized (Kim et al. 2001), partial proxy and proxy with certificates. In the fully authorized mode, the original signer directly gives the secret key used for signing to the proxy signer, and the proxy signer uses the secret key to sign messages. However, since the original signature and the proxy signature cannot be distinguished, the signature scheme does not satisfy the non-repudiation.

In 2002, Shum and Wei (2002) proposed a proxy signature scheme based on the discrete logarithm problem, in which the identity of the proxy signer is hidden by alias, and only the alias authority can reveal his identity. In addition, there are many proxy signature schemes based on traditional mathematical problems, such as schemes based on the discrete logarithm problem (Li et al. 2003; Hwang and Chen 2003) and schemes based on the integer factorization problem (Shao 2003), both released in 2003.

In the post-quantum era, the focus has shifted towards research on quantum-secure proxy signature schemes, as traditional public key cryptosystems are now vulnerable. In 2010, Jiang et al. (2010) introduced a lattice-based proxy signature scheme using the bonsai tree model (Cash et al. 2012). It builds upon the GPV signature scheme by Gentry et al. (2008), which relies on a set of preimage sampleable trapdoor functions. However, a drawback of this scheme is that it leaves the proxy unprotected, allowing the original signer to forge the proxy signer's signature. In response, Xia et al. (2011) proposed a lattice-based proxy signature scheme in 2011, utilizing trapdoor functions with preimage sampling and the bonsai tree model. Its security is based on the complexity of the average-case small integer solution and inhomogeneous small integer solution. While the public and secret keys in this scheme are larger compared to those based on factoring or discrete logarithm problems, it only requires linear operations on small integers. To address the issue of varying key sizes in proxy signature schemes based on the Bonsai tree principle, Yu (2013) introduced a scheme in 2013 with controllable signature length. This scheme employs a fixed-dimension lattice-based delegation algorithm to generate the proxy key and utilizes a preimage sampling function to construct the proxy signature scheme. Its security is founded on the difficulty of the small integer solution problem and the shortest vector problem from lattices. In the same year, Kim et al. (2013) similarly developed a provably-secure ID-based proxy signature scheme based on lattice problems, employing a fixed-dimensional lattice-based delegation technique. Notably, this scheme is the first to offer protection for the proxy in the adaptive security model. In 2014, Li et al. (2014) put forward a lattice-based proxy signature scheme that is provably secure in the standard model. It primarily relies on the preimage sampling algorithm, with existential unforgeability proven under adaptive chosen message attack based on the small integer solution (SIS) problem in the standard model. Also in 2014, Jiang et al. (2014) constructed a proxy signature scheme using trapdoor-free signature and small-norm matrix transfer technology, relying on the small integer solution problem for security. While this scheme reduces the size of the secret key and proxy signature, it does not provide a proof of public verifiability for its proxy authorization. To address this, Lu et al. (2016) introduced the concept of authorization certificates in 2016 to enhance the scheme proposed by Jiang et al. (2014). They added a revocation list to enable the revocation of proxy authorization within its validity period. Experimental results demonstrate that the scheme improves both efficiency and security compared to the original one. Later, based on the rejection sampling technique of Lyu12 signature, Yang et al. (2015) proposed a lattice-based proxy signature scheme without a trapdoor, providing a formal security proof of unforgeability in the random oracle model.

Since proxy signature can realize secure signature delegation, it has a wide range of application scenarios, such as the signing of certificates in e-commerce, the distribution of e-checks or e-cash, and so on. With the development of technology, according to different requirements, people combine the advantages of proxy signature and other several types of signature system, and construct many new signatures, such as proxy multi-signature, blind proxy signature, proxy blind signature, threshold proxy signature, proxy signature with forward security, identity-based proxy signature, designated-verifier proxy signature and so on. Among them there is a mobile proxy signature, which can move autonomously in different execution environments. Therefore, it can be utilized for online sales in e-commerce.

In 1997, Kim, Park and Won revisited proxy signature and proposed two new types of proxy signature, called partial delegation with warrant and threshold delegation (Kim et al. 2013), where the partial delegation has fast processing speed and is appropriate for the restricting documents to be signed. In 2014, Zhang and Ma (2014) proposed an identity-based proxy blind signature from lattices by combining proxy signature with blind signature. Proxy blind signature scheme is a special form of blind signature that allows the proxy signer to sign on behalf of the original signer without knowing the content of the message.The new scheme is proved to be strongly unforgeable under the standard hardness assumption of the short integer solution problem (SIS) and the inhomogeneous small integer solution problem (ISIS). In 2018, Zhu et al. (2018) proposed an identity-based proxy signature scheme based on number theorem research unit (NTRU) lattice, which is proved secure in the random oracle. In comparison, the size of signature and key generated by this scheme are small. In 2021, Xie et al. (2021) proposed a forward-secure lattice-based proxy signature scheme. As the name implies, the scheme has forward security, but the scheme needs to improve its security at the cost of efficiency.

Overview

The overview Table 4 we provided for lattice-based digital signatures offers a visual comparison of different scheme properties. It's a valuable reference for researchers and practitioners to select the right scheme for specific scenarios. Proxy signature schemes, designed for delegation, may trade off some security properties like unforgeability. This emphasizes the importance of a balanced approach between security and practicality in their design. In essence, this table serves as a helpful guide for understanding and applying lattice-based digital signatures effectively.

According to the performance of the scheme mentioned in table, the schemes with the highest performance and optimal behavior have been summarized without considering property constraints. In static group signatures, Ling et al. (2019) achieves the smallest signature and public key sizes and exhibits the best performance. Simultaneously, in partially dynamic group signatures, Kansal et al. (2020) achieves the best performance by sacrificing anonymity properties. As for more practical full dynamic group signatures, Sun and Liu (2020) enhances the work of Sun et al. (2019), reaching the optimal performance level. Regarding blind signatures, Tang et al. (2017) and Wang et al. (2010) respectively serve as the optimal solutions under the Standard Model and Random Oracle. The recently introduced Xie et al. (2021) in 2021 also theoretically demonstrates the best performance in proxy signature.

Conclusion

This survey systematically explores the digital signature technology based on lattice cryptography. It introduces key schemes within the two paradigms of Hash-and-sign in traditional digital signatures, while also covering specialized digital signatures such as group signatures, ring signatures, blind signatures, and proxy signatures, along with their specific use cases in practical applications.

Firstly, group signatures and ring signatures offer significant advantages in protecting the privacy of group members. They allow group members to remain anonymous when signing documents while ensuring the validity of

Table 4 Group, ring, blind, proxy signature overview

Type	Scheme	Anonymity	Traceablity	TS	NF	Linkability	Unforgeability	Blindness	Nonrepudiation	Verifiability	PP	Size
Static group signature	Gordon et al. (2010)	Yes	Yes	No	No	No	Yes	No	Yes	Yes	No	Small
	Laguillaumie et al. (2013); Luo and Jiang (2020); Ling et al. (2019)	Full	Yes	No	No	No	Yes	No	Yes	Yes	No	Small
Partially dynamic group signature	Libert et al. (2016)	Yes	No	No	No	No	Yes	No	Yes	Yes	No	Controllable
	Ling et al. (2018)	Full	Yes	No	Yes	No	Yes	No	Yes	Yes	No	Controllable
	Kansal et al. (2020)	No	Yes	No	No	No	Yes	No	Yes	Yes	No	Controllable
Fully dynamic group signature	Xie et al. (2019)	Full	Yes	No	Yes	No	Yes	No	Yes	Yes	No	Controllable
	Sun et al. (2019); Sun and Liu (2020)	Full	Yes	Yes	Yes	No	Yes	No	Yes	Yes	No	Controllable
Ring signature	Baum et al. (2018); Tang et al. (2021)	Yes	Yes	No	No	Yes	Yes	No	Yes	Yes	No	Big
Blind signature	Rückert (2010); Wang et al. (2010); Gao et al. (2017); Tang et al. (2017)	No	No	No	No	No	Yes	Yes	Yes	Yes	No	Small
Proxy signature	Jiang et al. (2010)	No	No	No	No	No	No	No	No	No	No	Uncontrollable
	Xia et al. (2011)	No	No	No	No	No	No	No	No	No	No	Uncontrollable
	Yu (2013)	No	No	No	No	No	Yes	No	Yes	No	No	Controllable
	Kim et al. (2013); Li et al. (2014); Kim et al. (1997); Zhang and Ma (2014)	No	No	No	No	No	Yes	No	No	Yes	Yes	Big
	Jiang et al. (2014)	No	No	No	No	No	Yes	No	No	No	Yes	Small
	Lu et al. (2016); Zhu et al. (2018); Xie et al. (2021)	No	No	No	No	No	Yes	No	Yes	Yes	Yes	Small

Here PP is a shorthand for Proxy Protect the signature. This technology plays a crucial role in scenarios such as internal corporate decision-making and online voting. Ring signatures find widespread use in blockchain applications, ensuring transaction anonymity and traceability. Blind signature technology has unique advantages in information transmission and authentication. It permits the sender to obtain a signature without revealing their identity, which is of practical significance in scenarios like online voting and digital cash. Proxy signatures are a special form of signature that allows one entity to sign a document on behalf of another entity while maintaining the validity of the signature. They are essential in authorization and legal document scenarios.

In addition to these focal areas of research, there exist other specialized signature schemes for specific application requirements, such as multi-signatures, timed signatures, and aggregate signatures. However, these, along with the aforementioned specialized digital signature schemes, are constructed based on the two paradigms mentioned in the paper. The evolution of these two paradigms exhibits a trend shifting from standard lattices to cyclic lattices, ideal lattices, and the hardness assumptions transitioning from standard SIS and LWE to Ring-SIS and Ring-LWE, and further evolving towards more flexible module problems.

As mentioned earlier, one of the primary challenges faced by lattice-based digital signature schemes is how to enhance their usability without compromising security. This is a central consideration in many schemes discussed earlier. In addition, the lack of unified standards hinders the widespread adoption of these schemes. The Post-Quantum Cryptography Standardization Process conducted by NIST has made significant progress in this regard, with Falcon (Fouque et al. 2018) and Dilithium (Ducas et al. 2018), mentioned in the document, being two of the three ongoing standardization candidates. Furthermore, among the seven cryptographic candidates proposed by NIST, five are based on lattice cryptography. This underscores the paramount importance of lattice cryptography in the post-quantum cryptography era. With the development of quantum computing technology, traditional cryptographic algorithms face severe challenges. However, lattice-based schemes exhibit strong resistance to quantum computing, providing a reliable solution for future digital security. It demonstrates immense potential and prospects in ensuring digital communication security and protecting privacy. As technology continues to advance, and research delves deeper into this field, we firmly believe that it will play an increasingly pivotal role in the future of information security.

Future work

With the continuous development of the field of cryptography, there are still many directions in the area of lattice-based digital signatures that need to be explored and improved. In the direction of homomorphic signatures, future research can focus on improving the performance and security of homomorphic signatures. In the direction of secure multi-party computation and privacy protection, combining homomorphic signatures (Zheng et al. 2023) with secure multi-party computation to achieve collaborative computation while protecting data privacy is of great significance.

Additionally, there is also a significantly important new idea, which is the integration of quantum cryptography (Zeng 2006) with classical cryptography. Researchers can explore how to combine quantum cryptography and post-quantum cryptography to create more robust security solutions. This may include integrating quantum key distribution with classical encryption algorithms to enhance overall security (Wang et al. 2021). With the rapid development of quantum computing technology, post-quantum cryptography, as an extension of traditional cryptography, plays a crucial role in safeguarding communication security in the era of quantum computing. However, as the potential threat of quantum computing becomes more evident, traditional cryptographic algorithms may become vulnerable. In this scenario, quantum cryptography has emerged as a new research focus.

In comparison, post-quantum cryptography is an extension based on traditional classical cryptography, thus its security is established on the difficulty of classical mathematical problems. Quantum cryptography, on the other hand, is based on the principles of quantum physics, achieving unprecedented levels of security through techniques like quantum key distribution. For instance, measurements on quantum states lead to their alteration, immediately detecting any unauthorized interception. This enables quantum cryptography to provide unparalleled security. Similarly, within the field of quantum cryptography, there is also the area of quantum signatures. A significant feature of quantum signatures is that, before the signer sends the signature state, they cannot determine the specific content of the signature. As a result, they cannot repudiate their own signature. Additionally, any unauthorized interception leads to an alteration of the signature state, immediately detected.

In summary, quantum cryptography represents a novel means of security assurance, providing robust protection for communications in the era of quantum computing. It particularly demonstrates immense potential in safeguarding privacy and ensuring communication security. With the continuous advancement of quantum technology, we can expect significant progress in the research and implementation of quantum cryptography in the future.

Acknowledgements

This work was supported by National Key R and D Program of China (Grant No. 2022ZD0116800).

Author contributions

All the authors read and approved the final manuscript.

Declarations

Competing interests

The authors declare that they have no competing interests.

Received: 30 October 2023 Accepted: 4 December 2023
Published online: 01 April 2024

References

Abdalla M, Fouque PA, Lyubashevsky V et al (2015) Tightly secure signatures from lossy identification schemes. J Cryptol 2012:597–631

Abdalla M, An JH, Bellare M et al (2002) From identification to signatures via the Fiat-Shamir transform: minimizing assumptions for security and forward-security. Adv Cryptol EUROCRYPT. LNCS, pp 418–433

Abe M, Fujisaki E (1996) How to date blind signatures. In: International conference on the theory and application of cryptology and information security. Springer, Berlin Heidelberg, pp 244–251

Abhilash MH, Amberker B (2021) Efficient dynamic group signature scheme with verifier local revocation and time-bound keys using lattices. Comput Inform Technol 10(2):33–45

Aboud SJ, Al-Fayoumi MA (2007) Anonymous and non-repudiation E-payment protocol. Am J Appl Sci 4(8):538–542

Ajtai M (1996) Generating hard instances of lattice problems. In: Proceedings of the twenty-eighth annual ACM symposium on theory of computing, pp 99–108

Ajtai M, Kumar R, Sivakumar D (2001) A sieve algorithm for the shortest lattice vector problem. In: Proceedings of the thirty-third annual ACM symposium on Theory of computing, pp 601–610

Akleylek S, Bindel N, Buchmann J et al (2016) An efficient lattice-based signature scheme with provably secure instantiation. In: Progress in cryptology-AFRICACRYPT 2016: 8th international conference on cryptology in Africa, Fes, Morocco, April 13–15, 2016, proceedings 8. Springer International Publishing, pp 44–60

Alkim E, Bindel N, Buchmann J et al (2015) TESLA: tightly-secure efficient signatures from standard lattices. IACR Cryptol. ePrint Arch 755

Ateniese G, Camenisch J, Joye M et al (2000) A practical and provably secure coalition-resistant group signature scheme. In: Annual international cryptology conference. Springer, Berlin, Heidelberg, pp 255–270

Awasthi AK, Lal S (2005) ID-based ring signature and proxy ring signature schemes from bilinear pairings. arxiv preprint cs/0504097

Bai S, Galbraith SD (2014) An improved compression technique for signatures based on learning with errors. In: Topics in cryptology - CT-RSA, pp 28–47

Baum C, Lin H, Oechsner S (2018) Towards practical lattice-based one-time linkable ring signatures. In: International conference on information and communications security. Cham: Springer International Publishing, pp 303–322

Bellare M, Micciancio D, Warinschi B (2003) Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assumptions. Springer, Berlin, pp 614–629

Bellare M, Rogaway P (1993) Random oracles are practical: a paradigm for designing efficient protocols. In: Proceedings of the 1st ACM conference on computer and communications security, pp 62–73

Bernstein D, Hopwood D, Hülsing A et al (2015) SPHINCS: practical stateless hash-based signatures. IACR Cryptol ePrint Arch 2014:795. https://doi.org/10.1007/978-3-662-46800-5_15

Bootle J, Cerulli A, Chaidos P et al (2016) Foundations of fully dynamic group signatures. In: International conference on applied cryptography and network security. Cham: Springer International Publishing, pp 117–136

Bos J W, Costello C, Naehrig M et al (2015) Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In: 2015 IEEE symposium on security and privacy. IEEE, pp 553–570

Bresson E, Stern J, Szydlo M (2002) Threshold ring signatures and applications to ad-hoc groups. In: Annual international cryptology conference. Springer, Berlin Heidelberg, pp 465–480

Breuil C, Diamond T (2001) On the modularity of elliptic curves over Q. JAMS

Camenisch JL, Piveteau JM, Stadler MA (1995) Blind signatures based on the discrete logarithm problem. In: Advances in cryptology-EUROCRYPT'94: workshop on the theory and application of cryptographic techniques Perugia, Italy, May 9–12, 1994 proceedings 13. Springer, Berlin Heidelberg, pp 428–432

Camenisch J, Stadler M (1997) Efficient group signature schemes for large groups. In: Annual international cryptology conference. Springer, Berlin Heidelberg, pp 410–424

Cash D, Hofheinz D, Kiltz E et al (2012) Bonsai trees, or how to delegate a lattice basis. J Cryptol 25:601–639

Chase M, Derler D, Goldfeder S et al (2017) Post-quantum zero-knowledge and signatures from symmetric-key primitives. ACM. https://doi.org/10.1145/3133956.3133997

Chase M, Lysyanskaya A (2006) On signatures of knowledge. Advances in cryptology-CRYPTO 2006: 26th Annual international cryptology conference, Santa Barbara, California, USA, August 20–24 2006, proceedings 26. Springer, Berlin Heidelberg, pp 78–96

Chaum D (1983) Blind signatures for untraceable payments. In: Advances in cryptology: proceedings of Crypto 82. Boston, MA: Springer US, pp 199–203

Chaum D, Van Heyst E (1991) Group signatures. In: Advances in cryptology-EUROCRYPT'91: workshop on the theory and application of cryptographic techniques Brighton, UK, April 8–11 1991, proceedings 10. Springer, Berlin Heidelberg, pp 257–265

Chen L, Pedersen TP (1994) New group signature schemes. In: Workshop on the theory and application of of cryptographic techniques. Springer, Berlin Heidelberg, pp 171–181

Cruz JP, Kaji Y (2017) E-voting system based on the bitcoin protocol and blind signatures. IPSJ Tran Math Model Appl 10(1):14–22

Dagdelen Ö, El Bansarkhani R, Göpfert F et al (2014) High-speed signatures from standard lattices. In: International conference on cryptology and information security in Latin America. Cham: Springer International Publishing, pp 84–103

Diffie W, Hellman ME (2022) New directions in cryptography. The Work of Whitfield Diffie and Martin Hellman, Democratizing Cryptography, pp 365–390

Dinur I, Kindler G, Safra S (1998) Approximating-CVP to within almost-polynomial factors is NP-hard. In: Proceedings 39th annual symposium on foundations of computer science (Cat. No. 98CB36280). IEEE, pp 99–109

Ducas L, Durmus A, Lepoint T et al (2013) Lattice signatures and bimodal Gaussians. In: Annual cryptology conference. Springer, Berlin Heidelberg, pp 40–56

Ducas L, Kiltz E, Lepoint T et al (2018) Crystals-dilithium: a lattice-based digital signature scheme. IACR Trans Cryptogr Hardw Embedd Syst 238–268

Ducas L, Lyubashevsky V, Prest T (2014) Efficient identity-based encryption over NTRU lattices

Ducas L, Prest T (2016) Fast fourier orthogonalization. In: Proceedings of the ACM on international symposium on symbolic and algebraic computation, pp 191–198

Dworkin MJ (2015) SHA-3 standard: permutation-based hash and extendable-output functions

El Gamal T (1985) A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans Inf Theory 31:469–472

Fiat A, Shamir A (1986) How to prove yourself: practical solutions to identification and signature problems. In: Conference on the theory and application of cryptographic techniques. Springer, Berlin Heidelberg, pp 186–19

Fouque PA, Hoffstein J, Kirchner P et al (2018) Falcon: Fast-Fourier lattice-based compact signatures over NTRU. Submission to the NIST's post-quantum cryptography standardization process 36(5):1–75

Gao W, Hu Y, Wang B et al (2017) Identity-based blind signature from lattices in standard model. In: Information security and cryptology: 12th international conference, inscrypt 2016, Beijing, China, November 4–6, 2016, revised selected papers. Springer International Publishing, pp 205–218

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, pp 197–206

Goldreich O, Levin L (1989) A hard predicate for all one-way functions. In: 21st STOC, pp 25–32

Goldwasser S, Micali S, Rackoff C (1989) The knowledge complexity of interactive proof-systems. SIAM J Comput 18(1):186–208

Gordon SD, Katz J, Vaikuntanathan V (2010) A group signature scheme from lattice assumptions. Springer, Berlin, pp 395–412

Gu C, Chen L, Zheng Y (2012) ID-based signatures from lattices in the random oracle model. In: Web information systems and mining: international conference, WISM 2012, Chengdu, China, October 26–28, 2012, proceedings. Springer, Berlin Heidelberg, pp 222–230

Guillou LC, Quisquater J-J (1990) A paradoxical" indentity-based signature scheme resulting from zero-knowledge. In: Advances in cryptology - Crypto '88, volume 403 of LNCS, pp 216-231. Springer

Güneysu T, Lyubashevsky V, Pöppelmann T (2012) Practical lattice-based cryptography: a signature scheme for embedded systems. In: Cryptographic hardware and embedded systems-CHES 2012: 14th international workshop, Leuven, Belgium, September 9–12 2012, proceedings 14. Springer, Berlin Heidelberg, pp 530–547

Harn L (1995) Cryptanalysis of the blind signature based on the discrete logarithm problem. Electron Lett 31(14):1136–1137

Hwang SJ, Chen CC (2003) Cryptanalysis of nonrepudiable threshold proxy signature schemes with known signers. Informatica 14(2):205–212

Jeong IR, Kwon JO, Lee DH (2008) Ring signature with weak linkability and its applications. IEEE Trans Knowl Data Eng 20(8):1145–1148

Jiang MM, Hu YP, Wang BC et al (2014) Efficient proxy signature on lattice. J Beijing Univ Posts Telecommun 37(3):89

Jiang Y, Kong F, Ju X (2010) Lattice-based proxy signature. In: 2010 International conference on computational intelligence and security. IEEE, pp 382–385

Kansal M, Dutta R, Mukhopadhyay S (2020) Group signature from lattices preserving forward security in dynamic setting. Adv Math Commun 14(4)

Katz J, Wang N (2003) Efficiency improvements for signature schemes with tight security reductions. In: Proceedings of the 10th ACM conference on computer and communications security, pp 155–164

Kim H , Baek J , Lee B et al (2001) Secret computation with secrets for mobile agent using one-time proxy signature

Kim HJ, In Lim J, Lee DH (2001) Efficient and secure member deletion in group signature schemes. In: Information security and cryptology-ICISC–2000 third international conference Seoul, Korea, December 8–9, 2000, proceedings 3. Springer, Berlin Heidelberg, pp 150–161

Kim KS, Hong D, Jeong IR (2013) Identity-based proxy signature from lattices. J Commun Netw 15(1):1–7

Kim S, Park S, Won D (1997) Proxy signatures, revisited. In: International conference on information and communications security. Springer, Berlin Heidelberg, pp 223–232

Koblitz N (1987) Elliptic curve cryptosystems. Math Comput 48(177):203–209

Laguillaumie F, Langlois A, Libert B et al (2013) Lattice-based group signatures with logarithmic signature size. Springer, Berlin, pp 41–61

Lamport L (1979) Constructing digital signatures from a one-way function. Technical Report SRI-CSL-98, SRI International Computer Science Laboratory

Li LH, Tzeng SF, Hwang MS (2003) Generalization of proxy signature-based on discrete logarithms. Comput Secur 22(3):245–255

Li MX, Zheng YJ, Xu M (2014) A lattice-based proxy signature scheme under the standard model. J Sichuan Univ Eng Sci Edn 46(1):102–106

Li Z, Zhang JX, Feng C et al (2017) Electronic cash protocol research review. Comput Sci Explor 11(11):1701

Li C, Tian Y, Chen X et al (2021) An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems. Inf Sci 546:253–264

Libert B, Ling S, Mouhartem F et al (2016) Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In: International conference on the theory and application of cryptology and information security. Springer, Berlin Heidelberg, pp 373–403

Lin WD, Jan JK (2000) A security personal learning tools using a proxy blind signature scheme. In: Proceedings of international conference on Chinese language computing, Illinois, USA, pp 273–277

Ling S, Nguyen K, Wang H et al (2017) Lattice-based group signatures: achieving full dynamicity with ease. In: Applied cryptography and network security: 15th international conference, ACNS 2017, Kanazawa, Japan, July 10–12, 2017, proceedings 15. Springer International Publishing, pp 293–312

Ling S, Nguyen K, Wang H et al (2018) Constant-size group signatures from lattices. In: Public-key cryptography-PKC 2018: 21st IACR international conference on practice and theory of public-key cryptography, Rio de Janeiro, Brazil, March 25–29, 2018, Proceedings, Part II 21. Springer International Publishing, pp 58–88

Ling S, Nguyen K, Wang H et al (2019) Forward-secure group signatures from lattices. In: Post-quantum cryptography: 10th international conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 revised selected papers 10. Springer International Publishing, pp 44–64

Lu XH, Wen QY, Wang LC (2016) Efficient, revocable lattice proxy signature. J Sichuan Univ Eng Sci Edn 48(1):139–145

Luo Q, Jiang CY (2020) A new constant-size group signature scheme from lattices. IEEE Access 8:10198-10207

Lysyanskaya A, Ramzan Z (1998) Group blind digital signatures: a scalable solution to electronic cash. In: International conference on financial cryptography. Springer, Berlin Heidelberg, pp 184–197

Lyubashevsky V (2009) Fiat-Shamir with aborts: applications to lattice and factoring-based signatures. In: International conference on the theory and application of cryptology and information security. Springer, Berlin Heidelberg, pp 598–616

Lyubashevsky V (2012) Lattice signatures without trapdoors. In: Annual international conference on the theory and applications of cryptographic techniques. Springer, Berlin Heidelberg, pp 738–755

Lyubashevsky V, Micciancio D (2006) Generalized compact knapsacks are collision resistant. In: International colloquium on automata, languages, and programming. Springer, Berlin Heidelberg, pp 144–155

Lyubashevsky V, Nguyen NK, Plancon M (2022) Efficient lattice-based blind signatures via gaussian one-time signatures. In: IACR international conference on public-key cryptography. Cham: Springer International Publishing, pp 498–527

Lyubashevsky V, Peikert C, Regev O (2010) On ideal lattices and learning with errors over rings. In: Advances in Cryptology-EUROCRYPT 2010: 29th annual international conference on the theory and applications of cryptographic techniques, French Riviera, May 30–June 3, 2010, proceedings 29. Springer Berlin Heidelberg, pp 1–23

Mambo M, Usuda K, Okamoto E (1996) Proxy signatures: delegation of the power to sign messages. IEICE Trans Fundam Electron Commun Comput Sci 79(9):1338–1354

Merkle RC (1980) Protocols for public key cryptosystems. In: IEEE symposium on security & privacy, pp 122–134. IEEE

Micciancio D (2007) Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Comput Complex 16:365–411

Miller VS (1985) Use of elliptic curves in cryptography. Conference on the theory and application of cryptographic techniques. Springer, Berlin Heidelberg, pp 417–426

National Institute of Standards and Technology (2009) Digital signature standard (DSS). Federal Information Processing Standards (FIPS) Publication 186-3, Available at http://www.itl.nist.gov/fipspubs/by-num.htm

Nayak SK, Mohanty S, Majhi B (2017) CLB-ECC: certificateless blind signature using ECC. J Inf Process Syst 13(4)

Nelsen M, Chuang I (2010) Quantum computation and quantum information

Ong H, Schnorr C-P (1990) Fast signature generation with a Fiat-Shamir-like scheme. In: Advances in cryptology - Eurocrypt '90, volume 473 of LNCS, pp 432-440. Springer

Peikert C, Rosen A (2006) Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In: Theory of cryptography: third theory of cryptography conference, TCC 2006, New York, NY, USA, March 4–7, 2006. proceedings 3. Springer, Berlin Heidelberg, pp 145–166

Petzoldt A, Bulygin S, Buchmann J (2013) A multivariate based threshold ring signature scheme. Appl Algebra Eng Commun Comput 24:255–275

Pointcheval D, Stern J (2000) Security arguments for digital signatures and blind signatures. J Cryptol 13:361–396

Pointcheval D, Stern J (1996) Provably secure blind signature schemes. In: International conference on the theory and application of cryptology and information security. Springer, Berlin Heidelberg, pp 252–265

Regev O (2023) An efficient quantum factoring algorithm. arXiv:2308.06572 [quant-ph]

Rivest R L, Shamir A, Tauman Y (2001) How to leak a secret. In: Advances in cryptology-ASIACRYPT 2001: 7th International conference on the theory and application of cryptology and information security Gold Coast, Australia, December 9–13, 2001 proceedings 7. Springer, Berlin Heidelberg, pp 552–565

Rivest RL, Shamir A, Adleman LM (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126

Rückert M (2010) Lattice-based blind signatures. In: International conference on the theory and application of cryptology and information security. Springer, Berlin Heidelberg, pp 413–430

Schnorr CP (1990) Efficient identification and signatures for smart cards. Advances in cryptology-CRYPTO'89 proceedings 9. Springer, New York, pp 239–252

Shamir A (1985) Identity-based cryptosystems and signature schemes. Advances in cryptology: proceedings of CRYPTO 84 4. Springer, Berlin Heidelberg, pp 47–53

Shao Z (2003) Proxy signature schemes based on factoring. Inf Process Lett 85(3):137–143

Shao Q, Hong HJ, Li B (2021) Research on blockchain electronic voting scheme based on Elgamal strong blind signature. Small Microcomput Sys 42(11):2400–2406

Shor PW (1999) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev 41(2):303–332

Shum K, Wei VK (2002) A strong proxy signature scheme with proxy signer privacy protection. In: Proceedings. Eleventh IEEE international workshops on enabling technologies: infrastructure for collaborative enterprises. IEEE, pp 55–56

Singh S, Padhye S (2020) Identity based blind signature scheme over NTRU lattices. Inf Process Lett 155:105898

Stehlé D, Steinfeld R (2011) Making NTRU as secure as worst-case problems over ideal lattices

Sun Y, Liu Y, Wu B (2019) An efficient full dynamic group signature scheme over ring. Cybersecurity 2:1–15

Sun Y, Liu Y (2020) A lattice-based fully dynamic group signature scheme without nizk. In: International conference on information security and cryptology. Cham: Springer International Publishing, pp 359–367

Tang YL, Zhou J, Liu K et al (2017) Blind identity-based signature scheme on lattice under standard model. Comput Sci Explor 11(12):1965–1971

Tang Y, Xia F, Ye Q et al (2021) Identity-based linkable ring signature on NTRU lattice. Secur Commu Netw 2021:1–17

Wang LJ, Zhang KY, Wang JY et al (2021) Experimental authentication of quantum key distribution with post-quantum cryptography. npj Quantum Inf 7:67

Wang XW, Hou SH (2019) An improved and efficient proxy blind signature scheme. Comput Sci 46(B06):358–361

Wang FH, HU YP, Wang CX (2010) Lattice based blind signature scheme. J Wuhan Univ (Inf Sci) 35(05):550–553

Washington L (2008) Elliptic curves: number theory and cryptography. CRC Press

Winternitz RS (1984) A secure one-way hash function built from DES[C]//IEEE symposium on security & privacy. IEEE. https://doi.org/10.1109/SP.1984.10027

Xia F, Yang B, Ma S et al (2011) Lattice-based proxy signature scheme. J Hunan Univ Natl Sci Edn 38(6):84–88

Xie R, He C, Xu C et al (2019) Lattice-based dynamic group signature for anonymous authentication in IoT. Ann Telecommun 74:531–542

Xie J, Hu YP, Jiang MM (2021) Forward secure GGIE proxy signature. Comput Res Dev 58(3):583–597

Yang C, Qiu P, Zheng S et al (2015) An efficient lattice-based proxy signature scheme without trapdoor. In: 2015 International conference on intelligent information hiding and multimedia signal processing (IIH-MSP). IEEE, pp 189–194

Yu L (2013) A lattice-based proxy signature scheme. Comput Eng 39(10):123–126

Yung M, Katz J (2010) Digital signatures

Zeng ZH (2006) Quantum cryptography [J]

Zhang L, Ma Y (2014) A lattice-based identity-based proxy blind signature scheme in the standard model. Math Probl Eng

Zheng ZY, Liu FX, Tian K (2023) Mathematical theory of post-quantum cryptography. Higher Education Press of China

Zheng ZY, Liu FX et al (2022) A generalization of NTRUEncrypt—cryptosystem based on ideal lattice. J Inf Secur 13:165–180. https://doi.org/10.4236/jis.2022.133010

Zheng Z, Liu F, Tian K (2023) An unbounded fully homomorphic encryption scheme based on ideal lattices and Chinese remainder theorem. J Inf Secur 14:366–395. https://doi.org/10.4236/jis.2023.144021

Zhu H, Tan Y, Zhu L et al (2018) An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks. Sensors 18(5):1663

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.