Ring Signature Scheme Based on Lattice and Its Application on Anonymous Electronic Voting

Yihua Zhou[1], Songshou Dong[1*], and Yuguang Yang[1]
[1]Faculty of Information Technology, Beijing University of Technology
Beijing,100124 China
[e-mail: dongsongshou@emails.bjut.edu.cn]
*Corresponding author: Songshou Dong

Received May 2, 2021; revised July 13, 2021; revised September 26, 2021; accepted December 20, 2021; published January 31, 2022

Abstract

With the development of quantum computers, ring signature schemes based on large integer prime factorization, discrete logarithm problem, and bilinear pairing are under threat. For this reason, we design a ring signature scheme based on lattice with a fixed verification key. Compared with the previous ring signature scheme based on lattice, our design has a fixed verification key and does not disclose the signer's identity. Meanwhile, we propose an anonymous electronic voting scheme by using our ring signature scheme based on lattice and (t, n) threshold scheme, which makes up for the lack of current anonymous electronic voting that cannot resist attacks of the quantum computer. Finally, under standard model (SM), we prove that our ring signature scheme based on lattice is anonymous against the full-key exposure, and existentially non-forgeable against insider corruption. Furthermore, we also briefly analyze the security of our anonymous electronic voting scheme.

Keywords: Anti-quantum, anonymous electronic voting, lattice, ring signature

http://doi.org/10.3837/tiis.2022.01.016 **ISSN : 1976-7277**

1. Introduction

Electronic voting is a hot theme in the field of information security today. Compared with traditional election methods, electronic voting is fairer, safer, more efficient, and convenient. And it also can save a lot of material and human resources. The most basic requirement of electronic voting is to ensure the anonymity of the voter's identity, the fairness of casting a ballot cycle, the authentication of the voter's identity, and the correctness of the election results. Some researchers have made a lot of efforts on the theoretical research of electronic voting and the design of voting schemes, but there are still many shortcomings in ensuring the anonymity of the voters' identity under quantum computers [1]-[10].

In 2001, the notion of ring signature was first reported by Rivest et al. [11]. Then, the ring signatures are used in many fields, such as anonymous electronic voting, anonymous identity verification, and blockchain. So far, cryptographers have proposed many ring signature schemes [12]-[26]. Most of these schemes are constructed by large integer prime factorization [11],[14],[17], discrete logarithm problems [12],[13] and bilinear pairing [15],[16],[18],[19],[21]. However, the large integer prime factorization problem and the discrete logarithm problem can be effectively tackled by Shor's quantum algorithm in polynomial time [27]. Lattice ciphers are considered to be the most prospective cryptographic primitives in the post-quantum era and have attracted widespread attention. The design of cipher schemes based on the lattice has become a hot topic [28]-[47]. Random oracle model (ROM) and standard model (SM) are the two security levels of digital signatures. Some cryptographers believe that the signature schemes under SM is easier to be applied in engineering than these under ROM. Many ring signature schemes based on lattice have been designed by cryptographers recently [40]-[47]. However, these signatures [40]-[47] have some shortcomings: the length of the verification key is too large or the anonymity of the ring signature scheme cannot be guaranteed. Therefore, constructing a lattice-based ring signature with a short verification key under SM is an issue that needs to be solved urgently.

Related Works In 2010, the first ring signature was constructed under SM by Brakerski et al. [22]. The hash-and-sign mode [19] was used in this scheme. And the security of the scheme is analyzed under the small integer solution (SIS) problem. But the signature length of the scheme is big. In the same year, the ring signature based on lattice under SM with a verification key length of $(2k+N)mn\log q$ was reported by Wang et al. [23]. The bonsai trees model [36] was used in this scheme which reduces the length of the verification key. In 2011, Wang et al. [24] reported two ring signatures and under the hash-and-sign mode [19] by lattice basis delegation technique [36]-[37]. One is a ring signature with a verification key length of $Nmn\log q$ under ROM, and the other is a ring signature with a verification key length of $(N+d)mn\log q$ under SM. Although the second ring signature had a shorter signature size than Brakerski et al.'s scheme [22], the verification key length is still big. In 2016, the extended split-SIS problem was reported by Gao et al.. They reported a ring signature scheme based on the extended split-SIS problem with a shorter public key size [40]. But their scheme was constructed under ROM and cannot be well applied in practice. In 2018, an identity-based ring signature based on lattice was reported by Zhao et al., which solved the problem that traditional ring signatures need to rely on digital certificates, but this scheme is constructed under ROM and cannot be well applied in practice [41]. In the same year, Wang and Zhao used the Fiat-Shamir framework to design a ring signature without trapdoors under ROM [25]. Although their scheme is very efficient, the public key is still large, and the storage cost is high. In 2019, by using the extended split-SIS problem [40], a

ring signature scheme under SM was reported by Gao et al. [42], but the verification key of their scheme is still too big, and there will be a much storage cost. In the same year, a non-interactive deniable ring signature based on lattice was reported by Gao et al. [43]. When there is a malicious signer, this scheme can reveal the actual signer and protect the legal rights of other signers. However, the signature size of this scheme is too large which requires a lot of storage costs. At the same time, it is constructed under ROM which reduces the security of the scheme. A ring signature based on lattice that supports stealth addresses was designed by Liu et al. [44]. The security and privacy requirements in cryptocurrencies can be captured by this scheme. But it is constructed under ROM and cannot be used in practice well. A linkable ring signature was reported by Lu et al., which could solve the unlinkable problem of signatures created by the same signer but did not provide good proof of security [45]. In 2020, Zhao et al. used some algebraic structures on the ideal lattice and MP12 trapdoor derivation technology to design a ring signature scheme that the verification key size is constant, but this scheme will expose the identity of the signer [46]. In 2021, an efficient linkable ring signature scheme based on lattice with scalability to multiple layers was reported by Ren et al.. However, the verification key size is still too big [47]. For above ring signature schemes, they are either constructed under ROM [25],[40],[41],[43],[44], have a relatively large verification key size or signature size [22]-[25],[42],[47], or have some security risks [45],[46].

In 2019, Kurbatov et al. proposed to apply ring signatures to the construction of anonymous electronic voting schemes, but they did not give a specific implementation [8]. In 2020, an anonymous and coercion-resistant distributed electronic voting scheme was reported by Zaghloul et al., which uses the conditions of the parties' unwillingness to collude to reduce the possibility of voter information exposure [9]. However, in the post-quantum era, even if parties do not collude, the anonymity of the scheme cannot be guaranteed. In 2021, a distributed blockchain-based anonymous mobile electronic voting scheme was reported by Zaghloul et al., which increases the voter turnout rate during large-scale elections by using IoT devices. But in the post-quantum era, this scheme has security risks [10]. The above voting schemes have security risks in the post-quantum era.

Contributions

- A ring signature scheme based on lattice under SM is designed by us, which can realize the constant verified public key size. The ring signature scheme we proposed is based on identity, and therefore, it does not need to rely on digital certificates. We prove the anonymity against the full-key exposure and existential non-forgeability against insider corruption of our scheme under SM.
- Besides, we also extend our ring signature scheme to anonymous electronic voting by combining Shamir's (t, n) threshold scheme [48]. Our voting scheme uses a lattice-based ring signature structure to ensure the anonymity of voters, uses landmarks to prevent multiple votes by one voter, and uses (t, n) threshold scheme [48] to ensure the anonymity of votes before the ballots are made public. Finally, voters can use known information to determine whether their votes are counted to prevent the counting agency from losing votes privately.

2. Preliminaries

Notations. $[d]$ represents all positive integers from 1 to d. Vectors are expressed in lowercase italic bold letters. Matrix is represented by uppercase bold italic letters. $\|\cdot\|$ represents the l_2 norm. For matrix $\boldsymbol{A} = [\boldsymbol{a_1}, \cdots, \boldsymbol{a_m}] \in \mathrm{R}^{n \times m}$, the i-th column vector is

represented by $\boldsymbol{a_i}$. The Gram-Schmidt orthogonalization of vectors $\boldsymbol{a_1}, \cdots, \boldsymbol{a_m}$ is represented by vectors $\widetilde{\boldsymbol{a}}_1, \cdots, \widetilde{\boldsymbol{a}}_m$. The logarithm based on 2 is represented by the function log. The notations O and ω represent the growth of functions.

2.1 Lattice

$\boldsymbol{b_1}, \boldsymbol{b_2}, \cdots, \boldsymbol{b_n}$ are n linearly independent vectors in R^n, let $\boldsymbol{B} = [\boldsymbol{b_1}, \boldsymbol{b_2}, \cdots, \boldsymbol{b_n}]$, $\Lambda(\boldsymbol{B}) = \{\boldsymbol{Bc} = \sum_{i=1}^{n} \boldsymbol{b_i c_i} | \boldsymbol{c} \in \mathrm{Z}^n\}$ represent the n-dimensional lattice Λ generated by the basis $\boldsymbol{B}$, where $\boldsymbol{B}$ is a basis of the lattice $\Lambda^{\perp}(\boldsymbol{B})$. The orthogonal lattice $\Lambda^{\perp}(\boldsymbol{B}) = \{\boldsymbol{e} \in \mathrm{R}^m | \boldsymbol{Be} = \boldsymbol{0} \bmod q, \boldsymbol{B} \in \mathrm{R}_q^{n \times m}\}$ [49].

2.2 Discrete Gaussians

For any $\eta > 0$ and $\boldsymbol{x} \in \mathrm{R}^{\mathrm{m}}$, the discrete Gaussian function with η as the parameter and $\boldsymbol{v} \in \mathrm{R}^{\mathrm{m}}$ as the center is defined as $\rho_{\boldsymbol{v},\eta}(\boldsymbol{x}) = \exp(-\pi \|\boldsymbol{x} - \boldsymbol{v}\|^2 / \eta^2)$.

The discrete Gaussian function on lattice $\Lambda \subseteq \mathrm{Z}^{\mathrm{m}}$ is defined as $\forall \boldsymbol{x} \in \Lambda$, $\mathrm{D}_{\Lambda,\boldsymbol{v},\eta}(\boldsymbol{x}) = \rho_{\boldsymbol{v},\eta}(\boldsymbol{x}) / \rho_{\boldsymbol{v},\eta}(\Lambda)$, where $\rho_{\boldsymbol{v},\eta}(\Lambda) = \sum_{\boldsymbol{z} \in \Lambda} \rho_{\boldsymbol{v},\eta}(\boldsymbol{z})$.

In particular, when representing a Gaussian function centered at 0, we often omit 0 [49].

2.3 Hard Problems on Lattice

The security of our ring signature scheme relies on the difficulty assumptions of the small integer solution (SIS) problem and the inhomogeneous small integer solution (ISIS) problem [32].

Definition 1 The small integer solution problem (SIS). A matrix $\boldsymbol{A} \in \mathrm{R}_q^{n \times m}$, parameters are given, the target of $SIS_{q,m,\beta}$ is to find a nonzero integer vector $\boldsymbol{v} \in \mathrm{Z}_q^m$, which satisfies $\boldsymbol{Av} = \boldsymbol{0} \bmod q$ and $\|\boldsymbol{v}\| \leq \beta$.

Definition 2 The inhomogeneous small integer solution problem (ISIS). A matrix $\boldsymbol{A} \in \mathrm{R}_q^{n \times m}$, parameters n, m, q, β, a vector $\boldsymbol{y} \in \mathrm{Z}_q^n$ are given, the target of $ISIS_{q,m,\beta}$ to find a nonzero integer vector $\boldsymbol{v} \in \mathrm{Z}_q^m$, which satisfies $\boldsymbol{Av} = \boldsymbol{y} \bmod q$ and $\|\boldsymbol{v}\| \leq \beta$.

2.4 Trapdoor and Basis Delegation Functions for Lattices

Ref. [32] gives three polynomial algorithms ($TrapGen$, $SampleD$, and $SamplePre$). The details are as follows:

The Gaussian smoothing parameter $\eta \geq \|\widetilde{\boldsymbol{B}}\| \cdot \omega(\log n)$ is used in the following algorithm [50].

$TrapGen(1^n)$. n, $q = poly(n)$, and $m \geq 5n\log q$ as inputs, $TrapGen(1^n)$ outputs $(\boldsymbol{A}, \boldsymbol{T})$, where $\boldsymbol{A}$ is statistically close to uniform on $\mathrm{Z}_q^{n \times m}$ and $\boldsymbol{T}$ is a trapdoor basis of $\Lambda^{\perp}(\boldsymbol{A})$, which satisfies $\|\widetilde{\boldsymbol{T}}\| \leq O(\sqrt{n\log q})$.

$SampleD(\boldsymbol{A}, \eta)$. Sample an $\boldsymbol{e}$ from distribution $\mathrm{D}_{\mathrm{Z}^m,\eta}$, where the distribution of $\boldsymbol{Ae}$ is uniform on Z_q^n.

$SamplePre(\boldsymbol{A}, \boldsymbol{T}, \boldsymbol{y}, \eta)$. $\boldsymbol{A} \in \mathrm{Z}_q^{n \times m}$, a trapdoor basis $\boldsymbol{T}$ for $\Lambda^{\perp}(\boldsymbol{A})$, a vector $\boldsymbol{y} \in \mathrm{Z}_q^n$, and η as inputs, $SamplePre(\boldsymbol{A}, \boldsymbol{T}, \boldsymbol{y}, \eta)$ outputs a vector $\boldsymbol{e}$, which satisfies $\boldsymbol{Ae} = \boldsymbol{y} \bmod q$, $\boldsymbol{e} \leq \eta\sqrt{m}$ and $\boldsymbol{e}$ is within negligible statistical distance of $\mathrm{D}_{\Lambda_{\boldsymbol{y}}^{\perp},\eta}$.

$BasisDel(\boldsymbol{A},\boldsymbol{R},\boldsymbol{T},\eta)$.[51] Let $q>2$, $\boldsymbol{A}\in \mathrm{R}_q^{n\times m}$, $\boldsymbol{R}$ be a matrix sampled from $\mathrm{D}_{m\times m}$, and $\boldsymbol{T}$ be a trapdoor basis of $\Lambda^{\perp}(\boldsymbol{A})$, $BasisDel(\boldsymbol{A},\boldsymbol{R},\boldsymbol{T},\eta)$ outputs a random trapdoor basis $\boldsymbol{T}^*$ for $\Lambda^{\perp}(\boldsymbol{AR^{-1}})$, which satisfies $\|\widetilde{\boldsymbol{T}^*}\|\leq\eta\sqrt{m}$.

2.5 (t,n) Threshold Scheme

The following are the details for (t,n) threshold scheme [48].

1. Setup. The trusted agency T distributes the initial secret number $S\geq 0$ among n users.
   - T chooses a prime number $p>\max(S,n)$, and defines $a_0=S$.
   - $t-1$ random independent coefficients $a_1,a_2\ldots,a_{t-1}$ are selected by T. A random polynomial defined on the group Z_p as follows:

$$f(x)=\sum_{i=0}^{t-1}a_i x^i$$

   - T calculates $S_i=f(i)\bmod p$ $(i\in[n])$, and safely transmits S_i together with its corresponding public index i to user P_i.

2. Recovery.

Any t users or more than t users can restore the initial secret number S by combining their secret shares. t secret shares are equivalent to providing t different points, so they can solve the t unknowns a_i in the equation $f(x)$ $(0\leq i\leq t-1)$(Lagrange interpolation polynomial method or Vandermonde matrix method). It is easy to know the secret number $S=a_0=f(0)$.

2.6 Basic Definition and Security Requirements of Ring Signature

2.6.1 Basic Definition of Ring Signature

The following three algorithms $RS=(KeyGen,Ring-Sign,Ring-Verify)$ are basic algorithm for a ring signature.

$KeyGen(n,N)$: The security parameter n as input, Key-Generator-Center (KGC) outputs the ring public parameters rpk and the ring members' private keys sk_i for $i\in[N]$.

$Ring-Sign(rpk,ID_i,M,r)$: A signer's identity ID_i, ring set r $(r\subseteq[N])$ and a message M are input, signer ID_j outputs a ring signature $\boldsymbol{\sigma}$ on message M.

$Ring-Verify(r,M,\boldsymbol{\sigma})$: Ring set r and a signature $\boldsymbol{\sigma}$ on message M are input. If $Ring-Verify(M,Ring-Sign(rpk,ID_i,M,r))=1$ holds true, verifier outputs 1; Otherwise verifier outputs 0.

The security of our scheme includes anonymity and existential non-forgeability. The specific security definition is presented in Ref. [17]. The following are details.

2.6.2 Anonymity against the Full-Key Exposure

A ring signature (*Gen*, *Sign*, *Verify*), a probabilistic polynomial time (PPT) challenger C, and a PPT adversary A are given, perform the following game:

1. Setup. The security parameter n is given, and the public parameter rpk, the master secret key (MSK), and signer's private key are generated through running the algorithm Setup by challenger C. Then adversary A receives rpk from challenger C.

2. Signature queries. Adversary A queries the signature with the ring set r, the message M, and signer ID. A ring signature $\boldsymbol{\sigma_{ID}} \leftarrow Sign(PP, M, ID, r, sk_{ID})$ is returned to adversary A by challenger C.

3. Private key queries. Adversary A queries the private key with signer ID. The private key $sk_{ID} = \boldsymbol{T_{ID}}$ is sent to adversary A by challenger C.

4. Challenge. A signature query to challenger C on message M, a ring r, and two identities $ID_b \in r$ $(b \in \{0,1\})$ is submitted by adversary A. A random number $b \in \{0,1\}$ is picked by challenger C. Finally, a ring signature $\boldsymbol{\sigma_{ID_b}} \leftarrow Sign(PP, M, ID_b, r, sk_{ID_b})$ is returned to adversary A by challenger C.

5. Guess. A guess b' is output by adversary A.

$|\Pr[b' = b] - 1/2|$ is the superiority of adversary A in this game. If the superiority of adversary A is negligible, then this ring signature is considered to satisfy anonymity against full-key exposure.

2.6.3 Existential Non-forgeability against Insider Corruption

If for any PPT adversary A and any polynominal $n(\cdot)$, the probability that A succeeds in the following game is negligible, then a ring signature scheme (*Gen*, *Sign*, *Verify*) is existentially unforgeable against insider corruption.

1. Algorithm $Gen(1^k)$ generates key pairs $\{(pk_i, sk_i)\}_{i=1}^{n(k)}$. the set of public keys $\{(pk_i)\}_{i=1}^{n(k)}$ is given to A.

2. Adversary A has the right to obtain signatures $\boldsymbol{\sigma} \leftarrow Sign_{sk_{ID}}(M, r)$ where M is the message to be signed, r is ring set and $sk_{ID} \in r$.

3. A has the right to obtain private key sk_{ID} of signer with identity *ID*.

4. $(r^*, M^*, \boldsymbol{\sigma}^*)$ is output by adversary A. If $Vrfy_{r^*}(M^*, \boldsymbol{\sigma}^*) = 1$, then adversary A succeeds. $(*, M^*, \boldsymbol{\sigma}^*)$ is never queried by A, and $r^* \subseteq S \backslash C$, where C represents the set of corrupt users.

2.7 The Basic Steps of Electronic Voting

For different electronic voting schemes, the implementation process is different. Generally speaking, implementation process of an electronic voting system includes the following 6 steps [52]-[56].

Step 1 Registration: A voter obtains a mark that can be verified by the registration agency. Some personal information and voting information of voters may be implicit in this mark.

Step 2 Signature: The management agency first verifies whether the voter has voted for the first time, and if not, rejects the signature; If it is the first vote, the management agency signs the message and transmits this signature to the voter.

Step 3 Voting: After obtaining the signature, the voter can construct a ballot that he considers safe and send it to the counting agency.

Step 4 Statistics: After receiving all the votes, the counting agency will make their numbers public.

Step 5 Verification: According to the information published by the ballot counting agency, voters can know whether their ballots have been counted correctly. If they find that their votes have been tampered with or not made public, they can protest.

Step 6 Disclosure: If voters have no objections, according to the ballot opening agreement, the counting agency can restore the information of votes and make them public.

3. Lattice-based Ring Signature and Its Application on Anonymous Electronic Voting

3.1 Ring Signature Scheme Based on Lattice

The following are the parameters required by our scheme.

Let N, $n, \beta, q \geq N\beta \cdot \omega(\sqrt{n\log n})$, $m \geq 5n\log q$, $s \geq O(\sqrt{n\log q})$(the upper bound of the Gram-Schmidt size of the signer's private key) and Gaussian parameter $\eta \geq s \cdot \omega(\sqrt{\log q})$.

A bit string distributed on $\{0,1\}^*$ represents the massage, define the anti-collision hash function $H_1: \{0,1\}^* \to \{0,1\}^d$, where d is a positive integer, and another anti-collision hash function $H_2: \{0,1\}^* \to Z_q^{m\times m}$, $H_2(ID) \sim D_{m\times m}$. The following describes our algorithm.

Algorithm 1 KeyGen.

The security parameter n, number of people in the ring N, $m \in Z$, prime $q \in Z$, and $\eta \in R$ are inputs.

1. KGC (We assume that KGC is credible) computes $(\boldsymbol{A}, \boldsymbol{T}) \leftarrow TrapGen(n, m, q)$ where $\boldsymbol{T} \in Z_q^{m\times m}$, and selects vectors $\boldsymbol{b_0}, \cdots, \boldsymbol{b_d} \leftarrow Z_q^{\boldsymbol{n}}$;

2. For $i \in [N]$, define $\boldsymbol{A_i} = \boldsymbol{AH_2}(ID_i)^{-1}$($ID_i$ is the identity of i-th ring member), KGC extracts the basis $\boldsymbol{T_i} \leftarrow BasisDel(\boldsymbol{A}, \boldsymbol{H_2}(ID_i), \boldsymbol{T}, \eta)$, where $\boldsymbol{T_i} \in Z_q^{m\times m}$ ($\|\widetilde{\boldsymbol{T_i}}\| \leq \eta\sqrt{m}$) is a trapdoor basis of lattice $\Lambda_q^{\perp}(\boldsymbol{A_i})$;

3. Set the ring public parameter $rpk = \{N, \boldsymbol{A}, \boldsymbol{b_0}, \cdots, \boldsymbol{b_d}\}$, and $sk_i = \boldsymbol{T_i}$, $i \in [N]$ as the private key of i-th ring member.

Algorithm 2 Ring-Sign

The public key $rpk = \{N, \boldsymbol{A}, \boldsymbol{b_0}, \cdots, \boldsymbol{b_d}\}$, the identity ID_i and $sk_i = \boldsymbol{T_i}$ of i-th signer, a message $M \in \{0,1\}^*$ and $r = \{ID_1, \cdots, ID_N\}$ are input. The signer ID_i computes as follows:

1. Let $\boldsymbol{A}^* = \sum_{i=1}^{N} \boldsymbol{A_i} = [\boldsymbol{a_1^*}, \cdots, \boldsymbol{a_m^*}]$, $\boldsymbol{k} = (\boldsymbol{a_1^*}^T, \boldsymbol{a_2^*}^T, \cdots, \boldsymbol{a_m^*}^T)$, compute $\boldsymbol{\mu} = \boldsymbol{H_1}(\boldsymbol{k}, M)$ where $\boldsymbol{\mu} = (\mu[1], \mu[2], \cdots, \mu[d])$;

2. Compute $\boldsymbol{b_\mu} = \boldsymbol{b_0} + \sum_{i\in[d]} \mu[i]\boldsymbol{b_i}$ and $\boldsymbol{A_i} = \boldsymbol{AH_2}(ID_i)^{-1}$;

3. Randomly select $\boldsymbol{R} \in Z_q^{m\times m}$, define $\boldsymbol{B_i} = \boldsymbol{A_i R^{-1}}$, and extract the basis $\boldsymbol{T_{i*}} \leftarrow BasisDel(\boldsymbol{A_i}, \boldsymbol{R}, \boldsymbol{T_i}, \eta)$, where $\boldsymbol{T_{i*}} \in Z_q^{m\times m}$ is a trapdoor basis of lattice $\boldsymbol{\Lambda_q^{\perp}(B_i)}$ and satisfies $\|\widetilde{\boldsymbol{T_{i*}}}\| \leq \eta\sqrt{m}$;

4. Compute $\boldsymbol{e} \leftarrow SamplePre(\boldsymbol{B_i}, \boldsymbol{T_{i*}}, \boldsymbol{b_\mu}, \eta)$;

5. Output ring signature $\boldsymbol{\sigma} = \{\boldsymbol{e}, \boldsymbol{R}^* = \boldsymbol{H_2}(ID_i)^{-1}\boldsymbol{R^{-1}}\}$.

Algorithm 3 Ring-Verify

rpk, M, η, r={ $ID_1, \cdots, ID_N$ } as inputs. Let $\boldsymbol{A}^* = \sum_{i=1}^{N} \boldsymbol{A_i} = [\boldsymbol{a_1^*}, \cdots, \boldsymbol{a_m^*}]$, $\boldsymbol{k} = (\boldsymbol{a_1^*}^T, \boldsymbol{a_2^*}^T, \cdots, \boldsymbol{a_m^*}^T)$. Verifier computes $\boldsymbol{H_1}(\boldsymbol{k}, M) = \boldsymbol{\mu} = (\mu[1], \mu[2], \cdots, \mu[d])$ and $\boldsymbol{b_\mu} = \boldsymbol{b_0} + \sum_{i\in[d]} \mu[i]\boldsymbol{b_i}$; Accept if the following conditions are fulfilled: $\boldsymbol{AR^*e} = \boldsymbol{b_\mu} \bmod q$ and $\|\boldsymbol{e}\| \neq 0$ and $\|\boldsymbol{e}\| \leq \eta\sqrt{m}$.

3.2 Anonymous Electronic Voting Scheme Based on Our Ring Signature Scheme

Fig. 1 describes the process of anonymous electronic voting.

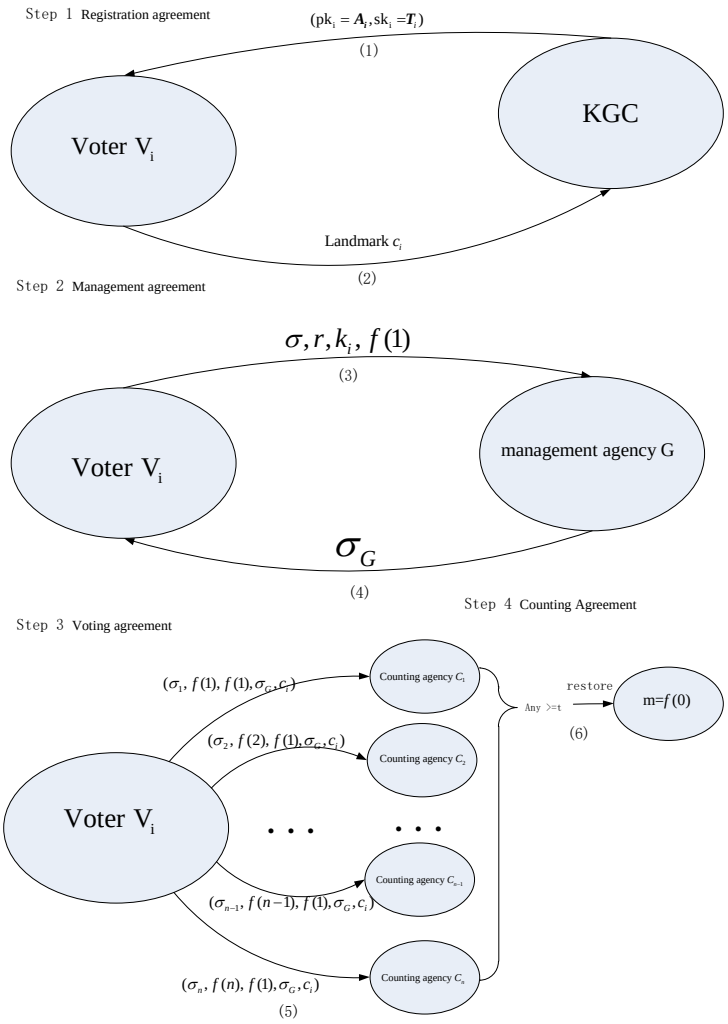

Fig. 1. The process of anonymous electronic voting

3.2.1 Parameters

- Voter: A voter has a legal public key and a legal private key;
- Registration agency: Registration agency KGC computes the private key and public key of voters;
- Management agency: sk_G and pk_G are the private key and public key of management agency G respectively;
- Counting agency: Counting agency is C_i $(i \in [n])$.

3.2.2 Scheme

1. Registration agreement

KGC computes $(\boldsymbol{A},\boldsymbol{T}) \leftarrow TrapGen(n,m,q)$, selects vectors $\boldsymbol{b_0},\cdots,\boldsymbol{b_d} \leftarrow \mathrm{Z}_q^n$, and makes $\boldsymbol{b_0},\cdots,\boldsymbol{b_d}$ public. The voter V_i is eligible to vote registers at KGC (if he doesn't register, he will be considered to be abstention), and submits his identity ID_i to KGC. KGC will allow voter V_i to register after verifying that he is eligible for election. After that, KGC generates public key, private key, and verification information for voter V_i as the following steps:

- KGC computes $\boldsymbol{A_i} = \boldsymbol{AH_2}(ID_i)^{-\mathbf{1}}$, and extracts $\boldsymbol{T_i} \leftarrow BasisDel(\boldsymbol{A},\boldsymbol{H_2}(ID_i),\boldsymbol{T},\eta)$, where $\boldsymbol{T_i} \in \mathrm{Z}_q^{m\times m}$ is a trapdoor basis of lattice $\Lambda_{\boldsymbol{q}}^{\perp}(\boldsymbol{A_i})$ which satisfies $\left\|\widetilde{\boldsymbol{T_i}}\right\| \le \eta\sqrt{m}$. Define the ID_i's private key as $sk = \boldsymbol{T_i}$ and ID_i's public key as $pk = \boldsymbol{A_i}$.
- V_i selects a random bit string $\boldsymbol{w_i} \in \{0,1\}^*$, calculates $\boldsymbol{c_i} = h(\boldsymbol{w_i})$ (h is a strong anti-collision hash function where $h:\{0,1\}^* \to \mathrm{Z}_q^n$), calculates $\boldsymbol{sig} \leftarrow SamplePre(\boldsymbol{A_i},\boldsymbol{T_i},\boldsymbol{c_i},\eta)$, and sends the $(\boldsymbol{sig},\boldsymbol{c_i})$ to KGC. After KGC verifies that the signature is legal, KGC makes $\boldsymbol{c_i}$ public. (It is assumed that KGC is a black box)

2. Management agreement

Voter V_i uses the vote M as the secret number of (t,n) threshold scheme and calculates $f(1),\ldots,f(n)$ respectively (f is a random polynomial). Voter V_i randomly selects several legitimate voters to form a ring (including the current voter himself). It is assumed that n voters are selected to form a ring $r = \{ID_1,\cdots,ID_n\}$. The process of signature is performed as the following way:

- Let $\boldsymbol{A}^* = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{A_i} = [\boldsymbol{a_1^*},\cdots,\boldsymbol{a_m^*}], \boldsymbol{k} = (\boldsymbol{a_1^*}^T,\boldsymbol{a_2^*}^T,\cdots,\boldsymbol{a_m^*}^T)$, compute $\boldsymbol{\mu} = \boldsymbol{H_1}(\boldsymbol{k},f(1))$ where $\boldsymbol{\mu} = (\mu[1],\mu[2],\cdots,\mu[d])$;
- Compute $\boldsymbol{b_\mu} = \boldsymbol{b_0} + \sum_{i\in[d]}\mu[i]\boldsymbol{b_i}$ and $\boldsymbol{A_i} = \boldsymbol{AH_2}(ID_i)^{-\mathbf{1}}$;
- Randomly select $\boldsymbol{R} \in \mathrm{Z}_q^{m\times m}$, define $\boldsymbol{B_i} = \boldsymbol{A_iR^{-1}}$, and extract a basis $\boldsymbol{T_{i*}} \leftarrow BasisDel(\boldsymbol{A_i},\boldsymbol{R},\boldsymbol{T_i},\eta)$ where $\boldsymbol{T_{i*}} \in \mathrm{Z}_q^{m\times m}$ ($\left\|\widetilde{\boldsymbol{T_{i*}}}\right\| \le \eta\sqrt{m}$) is a trapdoor basis of lattice $\boldsymbol{\Lambda_q^{\perp}(B_i)}$;
- Compute $\boldsymbol{e} \leftarrow SamplePre(\boldsymbol{B_i},\boldsymbol{T_{i*}},\boldsymbol{b_\mu},\eta)$, and output ring signature $\boldsymbol{\sigma} = \{\boldsymbol{e},\boldsymbol{R}^* = \boldsymbol{H_2}(ID_i)^{-\mathbf{1}}\boldsymbol{R^{-1}}\}$.

Finally, voter V_i sends $\boldsymbol{\sigma} = \{\boldsymbol{e},\boldsymbol{R}^* = \boldsymbol{H_2}(\mathrm{ID_i})^{-\mathbf{1}}\boldsymbol{R^{-1}}\}, r = \{ID_1,\cdots,ID_n\}, \boldsymbol{w_i}, f(1)\}$ to management agency G through an anonymous channel. G first verifies whether the signature is correct according to the following steps:

- Computes $\boldsymbol{H_1}(\boldsymbol{k},f(1)) = \boldsymbol{\mu} = (\mu[1],\mu[2],\cdots,\mu[d])$ and $\boldsymbol{b_\mu} = \boldsymbol{b_0} + \sum_{i\in[d]}\mu[i]\boldsymbol{b_i}$;
- Accept if the following conditions are fulfilled: $\boldsymbol{AR}^*\boldsymbol{e} = \boldsymbol{b_\mu}$ and $\boldsymbol{e} \neq 0$ and $\|\boldsymbol{e}\| \le \eta\sqrt{m}$.

If the signature is not correct, then refuses to receive the data; Otherwise, calculates $\boldsymbol{c_i'} = h(\boldsymbol{w_i})$, checks if there is already public $\boldsymbol{c_i}$ that satisfies $\boldsymbol{c_i} = \boldsymbol{c_i'}$, if not, refuses to receive the data; If it is equal, then checks whether c_i is already stored in the database, if it has been stored, which means that V_i has voted once and refuses to receive data, if not, stores $f(1)$ and $\boldsymbol{c_i}$ in the database, and then uses its private key SK_G to compute $\boldsymbol{\sigma_G} \leftarrow SamplePre(\boldsymbol{PK_G},\boldsymbol{SK_G},h(\boldsymbol{\sigma},\boldsymbol{c_i}),\eta)$. Finally sends $\boldsymbol{\sigma_G}$ to the signer V_i.

3. Voting agreement

If V_i verifies that the signature $\boldsymbol{\sigma_G}$ is correct, then calculates the signature $\boldsymbol{\sigma_j}$ of $f(j)$ (the signature method is the same as the signature method of $f(1)$). Finally, V_i sends $(\boldsymbol{\sigma_j},f(j),f(1),\boldsymbol{\sigma_G},\boldsymbol{c_i})$ through an anonymous channel to the counting agency $C_j (j \in [N])$. C_j verifies whether the signature is correct, and publishes $(j,\boldsymbol{c_i},f(1))$ if it is correct .

4. Collection agreement

If a voter V_i finds that his $(j, \boldsymbol{c_i}, f(1))$ has not been published, he raises $(f(1), \boldsymbol{\sigma_G})$ to protest. KGC asks C_j to join $(j, \boldsymbol{c_i}, f(1))$.

5. Counting Agreement

After the voting is over, t counting agencies calculate the vote M of the voter V_i according to the (t, n) threshold scheme.

4. Security Analysis

4.1 Security Analysis of Ring Signature Scheme Based on Lattice

4.1.1 Correctness

When the verifier receives the ring signature $\boldsymbol{\sigma} = \{\boldsymbol{e}, \boldsymbol{R}^* = \boldsymbol{H_2}(ID_j)^{-\mathbf{1}}\boldsymbol{R}^{-\mathbf{1}}\}$, it runs the Algorithm 3 Ring-Verify to check whether the ring signature is legal or not. If $\boldsymbol{AR}^*\boldsymbol{e} \neq \boldsymbol{b_\mu}$ or $\|\boldsymbol{e}\| = 0$ or $\|\boldsymbol{e}\| > \eta\sqrt{m}$, the signature is illegal. Otherwise, combining the public key A, public parameter $\{\boldsymbol{b_0}, \cdots, \boldsymbol{b_d}\}$, message M and r=$\{ID_1, \cdots, ID_n\}$, the correctness of our signature scheme mainly rely on the equation $\boldsymbol{AR}^*\boldsymbol{e}$=$\boldsymbol{b_\mu} \bmod q$. The detailed steps are described as follows:

Let $\boldsymbol{A}^* = \sum_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{A_i} = [\boldsymbol{a_1^*}, \cdots, \boldsymbol{a_m^*}]$, $\boldsymbol{k} = (\boldsymbol{a_1^*}^T, \boldsymbol{a_2^*}^T, \cdots, \boldsymbol{a_m^*}^T)$

$\boldsymbol{H_1}(\boldsymbol{k}, M) = \boldsymbol{\mu} = (\mu[1], \mu[2], \cdots, \mu[d])$

$$\boldsymbol{b_\mu} = \boldsymbol{b_0} + \sum_{i \in [d]} \mu[i]\boldsymbol{b_i}$$

According to the $SamplePre$ function, $\boldsymbol{AR}^*\boldsymbol{e}$=$[\boldsymbol{AH_2}(ID_j)^{-\mathbf{1}}\boldsymbol{R}^{-\mathbf{1}}]\boldsymbol{e} = \boldsymbol{b_\mu}$.

4.1.2 Anonymity against the Full-Key Exposure

Theorem 1 Complete anonymity against the full-key exposure is satisfied by the ring signature scheme based on lattice proposed in this paper.

Proof

1. **Setup**. There are a PPT adversary A and a PPT challenger C. The security parameter n is given. Challenger C computes $(\boldsymbol{A}, \boldsymbol{T}) \leftarrow TrapGen(n, m, q)$, and outputs $rpk = \{N, \boldsymbol{A}, \boldsymbol{b_0}, \cdots, \boldsymbol{b_d}\}$ and the signer's private key $sk_j = \boldsymbol{T_j}$ $(\boldsymbol{j \in [N]})$. Then challenger C sends rpk to adversary A.

2. **Signature queries**. Input the ring set r, the message M, and signer ID_i. Adversary A queries challenger C for the signature. Challenger C computes $\boldsymbol{\sigma_i} \leftarrow Ring - Sign(rpk, ID_i, M, r)$, and sends $\boldsymbol{\sigma_i}$ to adversary A.

3. **Private key queries**. Adversary A randomly queries the private key $\boldsymbol{T_j}$ corresponding to identiry $ID_j (j \in [N])$. Challenger C sends $\boldsymbol{T_j}$ to adversary A.

4. **Challenge**. Challenger C provides parameters to adversary A: message M, ring set r, and the public keys of two users ID_0, ID_1. Challenger C arbitrarily selects $b \in \{0,1\}$, inputs the corresponding private key $\boldsymbol{T_b}$ of ID_b, and computes $\boldsymbol{\sigma_b} \leftarrow Ring - Sign(rpk, ID_b, M, r)$. Finally $\boldsymbol{\sigma_b}$ is send to adversary A by challenger C.

5. b' is given by the adversary A.

In the above process, the signatures of the two users ID_0 and ID_1 are $\boldsymbol{\sigma_0}$ and $\boldsymbol{\sigma_1}$ respectively. Because $\boldsymbol{\sigma_0}$ and $\boldsymbol{\sigma_1}$ are obtained from $\mathrm{D}_{\Lambda^{\perp}(\boldsymbol{B_b}),\boldsymbol{\eta}}$ using $SamplePre$ function, $\boldsymbol{\sigma_0}$ and $\boldsymbol{\sigma_1}$ have the same distribution structure. The statistical distance between $\boldsymbol{\sigma_0}$ and $\boldsymbol{\sigma_1}$ is negligible, so $\boldsymbol{\sigma_0}$ and $\boldsymbol{\sigma_1}$ are indistinguishable. Therefore, it is negligible that the superiority of adversary A to win the game. This scheme satisfies complete anonymity against full-key exposure.

4.1.3 Non-forgeability against the Insider Corruption

Theorem 2 Let q, m, N, η, β, r be set as parameters for the ring signature scheme and assume the $SIS_{q,m,2\eta\sqrt{m}}$ problem is hard, existential non-forgeability against the insider corruption is satisfied by our ring signature scheme under SM.

Proof If there is an adversary A that can break our scheme with the probability of ϵ, then we can design a polynomial algorithm B to work out the problem of $SIS_{q,m,2\eta\sqrt{m}}$ with a possibility of at least $\epsilon(q_E C_{q_E}^{q_E/2})^{-1}$. The total of queries of adversary A is represented by q_E. The following is the detailed process.

Setup. Public parameters are generated by the algorithm B as the following way.

1. Choose $l \in [q_E]$ as the size of the ring, $r = \{ID_1, \cdots, ID_l\}$;
2. Run $TrapGen(n, m, q)$ to generate $\boldsymbol{A} \in \mathrm{Z}_q^{n\times m}$ and $\boldsymbol{T} \in \mathrm{Z}_q^{m\times m}$, where $\boldsymbol{T} \in \mathrm{Z}_q^{m\times m}$ is a trapdoor basis of $\Lambda^{\perp}(\boldsymbol{A})$.
3. For each signer ID_i in the ring.

- If $i \in [q_E]$ and $ID_i \notin r$, select $\boldsymbol{R} \in \mathrm{Z}_q^{m\times m}$, calculate $\boldsymbol{A_i} = \boldsymbol{AH_2}(ID_i)^{-1}\boldsymbol{R^{-1}}$and $\boldsymbol{T_i} \leftarrow BasisDel(\boldsymbol{A}, \boldsymbol{RH_2}(ID_i), \boldsymbol{T}, \eta)$, and finally store $< ID_i, \boldsymbol{A_i}, \boldsymbol{T_i} >$ in the database.
- If $i \in [q_E]$ and $ID_i \in r$, calculate $\boldsymbol{A_i} = \boldsymbol{AH_2}(\mathrm{ID_i})^{-1}$ and $\boldsymbol{T_i} \leftarrow BasisDel(\boldsymbol{A}, \boldsymbol{H_2}(ID_i), \boldsymbol{T}, \eta)$.

4. Select $d+1$ uniformly distributed short random vectors $\boldsymbol{c_0}, \cdots, \boldsymbol{c_d} \in \mathrm{D}_{\mathrm{Z}^m,\tau}$ $(\tau = \frac{\beta}{d+1})$ and a specific signer $ID_t \in r$, and calculate $\boldsymbol{b_j} = \widetilde{\boldsymbol{A_t}}\boldsymbol{c_j}(j = 0, \cdots, d)$.
5. Send system parameters $< \boldsymbol{A}, \boldsymbol{b_0}, \cdots, \boldsymbol{b_d} >$ to adversary A.

Query phase. B responds the queries from A.

1. Corruption query (ID_i). If $ID_i \notin r$, B finds $< ID_i, \boldsymbol{A_i}, \boldsymbol{T_i} >$ in the database and returns $\boldsymbol{T_i}$ to adversary A. Otherwise, algorithm B aborts.
2. Signing query (ID_i, M_i).

Let $\boldsymbol{A}^* = \sum_{i=1}^{n} \boldsymbol{A_i} = [\boldsymbol{a_1^*}, \cdots, \boldsymbol{a_m^*}]$, $\boldsymbol{k} = (\boldsymbol{a_1^*}^T, \boldsymbol{a_2^*}^T, \cdots, \boldsymbol{a_m^*}^T)$.

- If $ID_i = ID_t$, B first calculates $\boldsymbol{H_1}(\boldsymbol{k}, M_i) = \boldsymbol{\mu} = (\mu[1], \mu[2], \cdots, \mu[d])$. After that, algorithm B calculates $\boldsymbol{e_{M_i}} = \boldsymbol{c_0} + \sum_{j\in[d]} \mu[j]\boldsymbol{c_j} \in \mathrm{Z}_q^n$, and returns $\boldsymbol{e_{M_i}}$ to adversary A.
- If $< \mathrm{ID}_i, \boldsymbol{A_i}, \boldsymbol{T_i} >$ is in the database,the algorithm B first calculates $\boldsymbol{H_1}(\boldsymbol{k}, M_i) = \boldsymbol{\mu} = (\mu[1], \mu[2], \cdots, \mu[d])$ and $\boldsymbol{b_\mu} = \boldsymbol{b_0} + \sum_{i\in[d]} \mu[i]\boldsymbol{b_i}$. After that, the algorithm B calculates $\boldsymbol{e_{M_i}} \leftarrow SamplePre(\boldsymbol{A_i}, \boldsymbol{T_i}, \boldsymbol{b_\mu}, \eta)$, and returns $\boldsymbol{e_{M_i}}$ to adversary A.
- Otherwise, B looks for $ID_v \in r$ and $< ID_v, \boldsymbol{A_v}, \boldsymbol{T_v} >$ is in the database. Algorithm B calculates $\boldsymbol{H_1}(\boldsymbol{k}, M_i) = \boldsymbol{\mu} = (\mu[1], \mu[2], \cdots, \mu[d])$, $\boldsymbol{b_\mu} = \boldsymbol{b_0} + \sum_{i\in[d]} \mu[i]\boldsymbol{b_i}$, $\boldsymbol{e_{M_i}} \leftarrow SamplePre(\boldsymbol{A_v}, \boldsymbol{T_v}, \boldsymbol{b_\mu}, \eta)$, and returns $\boldsymbol{e_{M_i}}$ to adversary A.

Forge phase. Finally, a forged signature $< ID_i^*, M_i^*, \boldsymbol{e}^* >$ is output by the adversary A. Let $\boldsymbol{A}^* = \sum_{i=1}^{n} \boldsymbol{A_i} = [\boldsymbol{a_1^*}, \cdots, \boldsymbol{a_m^*}]$, $\boldsymbol{k} = (\boldsymbol{a_1^*}^T, \boldsymbol{a_2^*}^T, \cdots, \boldsymbol{a_m^*}^T)$. If $ID_i^* \neq ID_t$, abort. Otherwise algorithm B calculates $\boldsymbol{H_1}(\boldsymbol{k_i}, M_i^*) = \boldsymbol{\mu}^* = (\mu^*[1], \mu^*[2], \cdots, \mu^*[d])$, $\boldsymbol{e_{M_i^*}} = \boldsymbol{c_0} + \sum_{i\in[d]} \mu^*[i]\boldsymbol{c_j} \in \mathrm{Z}_q^n$, and outputs $\boldsymbol{e} = \boldsymbol{e}^* - \boldsymbol{e_{M_i^*}}$ as a solution. If $\boldsymbol{e}^*$ is a legal signature, then we have $\boldsymbol{A_t e}^* = \boldsymbol{b_{\mu^*}}$ where $\|\boldsymbol{e}^*\| \leq \eta\sqrt{m}$. On the other hand, $\boldsymbol{b_{\mu^*}} = \boldsymbol{b_0} + \sum_{j\in[d]} \mu^*[j]\boldsymbol{b_j}$ where $\boldsymbol{b_j} = \widetilde{\boldsymbol{A_t}}\boldsymbol{c_j} \in \mathrm{Z}_q^n$, so we have $\boldsymbol{A_t e_{M_i^*}} = \boldsymbol{b_{\mu^*}}$ with $\left\|\boldsymbol{e_{M_i^*}}\right\| \leq \eta\sqrt{m}$. Therefore, $\boldsymbol{e} = \boldsymbol{e}^* - \boldsymbol{e_{M_i^*}}$ can be used as a solution to the $SIS_{q,m,2\eta\sqrt{m}}$ problem.

Remark The probability of exiting from the above process is at most $1 - (q_E C_{q_E}^{q_E/2})^{-1}$, adversary A outputs a forged signature $< ID_i^*, M_i^*, \boldsymbol{e}^* >$ with the probability of ϵ. Let $\boldsymbol{e_0} = \boldsymbol{e}^* - \boldsymbol{e_{M_i^*}}$, then $\|\boldsymbol{e_0}\| = \left\|\boldsymbol{e}^* - \boldsymbol{e_{M_i^*}}\right\| \leq \|\boldsymbol{e}^*\| + \left\|\boldsymbol{e_{M_i^*}}\right\| = 2\eta\sqrt{m}$. The probability of $\|\boldsymbol{e_0}\| = 0$ is at most $n^{\omega(1)}$, so the probability that algorithm B solves the problem of $SIS_{q,m,2\eta\sqrt{m}}$ is at least $\epsilon(q_E C_{q_E}^{q_E/2})^{-1}$.

4.2 Security Analysis of Anonymous Electronic Voting

Here we briefly analyze the security of our anonymous electronic voting.

Anonymity: The use of ring signature technology can make voters unconditionally anonymous. At the same time, our scheme satisfies anonymity under the condition of the quantum computer.

Uniqueness: Since the system will refuse voters to submit the bit string $\boldsymbol{w}$ repeatedly, voters repeatedly. In addition, because the difficulty of stealing other people's bit string $\boldsymbol{w}$ is equivalent to solving the one-way hash problem, it is difficult for voters to submit votes by stealing other people's bit string $\boldsymbol{w}$. Therefore, in this design, each voter can only submit one legal ballot.

Confidentiality and fairness: (t, n) threshold scheme is used to hide the content of the ballot so that the content of the ballot is confidential before the ballot is counted. And the ballots are counted after the vote is finished, so the result of the vote is fair.

Verifiability: Whether their votes are counted correctly can be verified by voters.

Legality: Suppose that a management agency G colludes with an unqualified person and submits an illegal ballot. Meanwhile, the total of votes exceeds the number of registered people, and it will be discovered. The power of counting agency C is decentralized, which skirts management organization G and counting agency C from colluding with cheating. When this situation happens, management agency G takes the primary liability.

Traceability: If a malicious voter is found, the identity of the voter can be revealed through KGC.

Authentication: The identity of a voter can be verified with his private key.

Authorization: A voter can be authorized to vote by KGC.

Accounting: If a voter finds out that his ballot has not been counted correctly, he can initiate a protest and ask to add his ballot.

5. Results and Discussion

The previous ring signature schemes based on lattice have two main problems:
1. The size of the verification key is too large;
2. The anonymity of ring signatures cannot be guaranteed.

A ring signature scheme based on lattice that the length of verification key is constant is proposed by us. The master public key is used as the verification key, which ensures that the size of the verification key will not increase with the increase of the number of people in the ring. The identity of the signer is hidden through the random matrix, ensuring the anonymity of the ring signature. We prove the anonymity and the existential non-forgeability under SM. Finally, we extend our ring signature scheme to anonymous electronic voting by combining (t, n) threshold scheme [48]. We briefly explained the security of our anonymous electronic voting scheme. Our anonymous electronic voting can guarantee anonymity under the conditions of quantum computers. At the same time, our anonymous voting scheme can prevent multiple votes by one voter, prevent the counting agency from losing votes privately, and ensure the anonymity of votes before the ballots are made public. The comparison between our ring signature scheme and other ring signature schemes is shown in **Table 1**. The comparison shows that our scheme has a smaller public key size, verification key size, private key size, and signature size than the schemes in Ref. [40] and Ref. [42]. At the same time, our scheme is constructed under the SM, which has more advantages than the scheme in Ref. [40]. Our scheme is more efficient in computational costs. The notations $\mathrm{T_{BD}}$, $\mathrm{T_{TG}}$ and $\mathrm{T_{SP}}$ represent the cost of the algorithms $BasisDel$, $TrapGen$ and $SamplePre$ respectively. And $\mathrm{T_{GSP}}$ and $\mathrm{T_{ERB}}$ represent the cost of the algorithms $GenSamplePre$ and $ExtRandBasis$ used in Ref. [42] respectively. $\mathrm{T_{SD}}$ and $\mathrm{T_{E}}$ represent the cost of the algorithms $SampleD$ and $Exbasis$ used in Ref. [40] respectively. We elide the costs of hashing and addition operations. Algorithm $BasisDel$ is faster than algorithm $ExtRandBasis$. Therefore, it is more efficient in terms of both storage and computational cost for our scheme. The same methodology of Ref. [57] is used to select parameters in **Table 2**. N represents the number of people in a ring.

Table 1. Comparison with the other schemes

Schemes	Ref.[40]	Ref.[42]	This work
Public key size	$4mn\log q$	$(3mn + Nn + n)\log q$	$(mn + Nn + n)\log q$
Verification key size	$Nmn\log q$	$(N + 1)mn\log q$	$mn\log q$
Private key size	$(mm + 4Nmm)\log q$	$(mm + 4Nmm)\log q$	$(Nmm + mm)\log q$
Signature size	$Nm\log q$	$(N + 1)m\log q$	$m\log q$
Sign cost	$T_{ERB}+T_{SD}+T_{E}$	T_{GSP}	$T_{BD}+T_{SP}$
Extract cost	$T_{TG}+NT_{ERB}$	$T_{TG}+NT_{ERB}$	$T_{TG}+NT_{BD}$
SM?	No	Yes	Yes

Table 2. Parameters setting

Parameter	Definition	Sample
n		125
N		50
β		10
q	$q = N\beta \cdot \omega(\sqrt{n\log n})$	14759
m	$m \geq 5nlogq$	8655
s	$s \geq O(\sqrt{n\log q})$	41
η	$\eta \geq s \cdot \omega(\sqrt{\log q})$	152
d		40
Signature size	$m\log q$	14.6321KB
Private key size	$(Nmm + mm)\log q$	6458660KB
Public key size	$(mn + dn + n)\log q$	1837.6705KB

6. Conclusion

In conclusion, we report a ring signature scheme based on the lattice, and the verification key size can keep constant. Specifically, we use the master public key as the verification key, which ensures that the size of the verification key is constant. The identity of the signer is hidden through the random matrix, ensuring the anonymity of the ring signature. Furthermore, we prove the anonymity and the existential non-forgeability under SM. Finally, we extend our ring signature scheme to anonymous electronic voting by combining (t, n) threshold scheme. We briefly explained the security of our anonymity electronic voting scheme. Our anonymous electronic voting can guarantee anonymity under the conditions of quantum computers. Meanwhile, our anonymity voting scheme can prevent multiple votes by one voter, prevent the counting agency from losing votes privately, and ensure the anonymity of votes before the ballots are made public.

7. Future Work

In our ring signature scheme, we assume that the key distributor is a trusted organization. If KGC is not credible, our plan will not guarantee anonymity. But at present, it does not affect the expansion of the plan to anonymous electronic voting. In the future, we need to consider that how to solve the problem of untrusted KGC.

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 62071015, 62171264).

References

[1] J. C. Benaloh, M Yung, "Distributing the power of a government to enhance the privacy of voters," in *Proc. of the Fifth Annual ACM Symposium on Principles of Distributed Computing*, Calgary, Alberta, Canada, pp. 52-62, 1986. Article (CrossRef Link)

[2] D. Chaum, "Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA," in *Proc. of Workshop on the Theory and Application of Cryptographic Techniques*, Davos, Switzerland, pp. 177-182, 1988. Article (CrossRef Link)

[3] K. Ohta, "An electrical voting scheme using a single dministrator," *IEICE Spring National Convention Record*, vol. 296, 1988. Article (CrossRef Link)

[4] K. R. Iversen, "A cryptographic scheme for computerized general elections," in *Proc. of Annual International Cryptology Conference*, Santa Barbara, California, USA, pp. 405-419, 1991. Article (CrossRef Link)

[5] A. Fujioka, T. Okamoto and K. Ohta, "A practical secret voting scheme for large scale elections," in *Proc. of International Workshop on the Theory and Application of Cryptographic Techniques*, Gold Coast, Queensland, Australia, pp. 244-251, 1992. Article (CrossRef Link)

[6] K. Sako, "Electronic voting system with objection to the center," in *Proc. of 1992 Symposium on Cryptography and Information Security*, 1992.

[7] L. F. Cranor, "Electronic voting: computerized polls may save money, protect privacy," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 2, no. 4, pp. 12-16, 1996. Article (CrossRef Link)

[8] O. Kurbatov, P. Kravchenko, N. Poluyanenko, O. Shapoval, T. Kuznetsova, "Using ring signatures for an anonymous e-voting system," in *Proc. of 2019 IEEE International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, pp. 187-190, 2019. Article (CrossRef Link)

[9] E. Zaghloul, T. Li, J. Ren, "Anonymous and coercion-resistant distributed electronic voting," in *Proc. of 2020 International Conference on Computing, Networking and Communications (ICNC)*, Big Island, HI, USA, pp. 389-393, 2020. Article (CrossRef Link)

[10] E. Zaghloul, T. Li, J. Ren, "d-BAME: distributed blockchain-based anonymous mobile electronic voting," *IEEE Internet of Things Journal*, vol. 8, no. 22, pp.16585-16597, 2021. Article (CrossRef Link)

[11] R. L. Rivest, A. Shamir, Y. Tauman, "How to leak a secret," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security*, Gold Coast, Australia, pp. 552-565, 2001. Article (CrossRef Link)

[12] M. Abe, M. Ohkubo, K. Suzuki, "1-out-of-n signatures from a variety of keys," in *Proc. of International Conference on the Theory and Application of Cryptology and Information Security. Queenstown*, New Zealand, pp. 415-432, 2002. Article (CrossRef Link)

[13] J. Herranz, G. Sáez, "Forking lemmas for ring signature schemes," in *Proc. of International Conference on Cryptology in India*., New Delhi, India, pp. 266-279, 2003. Article (CrossRef Link)

[14] Y. Dodis, A. Kiayias, A. Nicolosi, V. Shoup, "Anonymous identification in ad hoc groups," in *Proc. of International Conference on the Theory and Applications of Cryptographic Techniques*, Interlaken, Switzerland, pp. 609-626, 2004. Article (CrossRef Link)

[15] F. Zhang, R. Safavi-Naini, W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Proc. of International Workshop on Public Key Cryptography*, Singapore, pp. 277-290, 2004. Article (CrossRef Link)

[16] A. K. Awasthi, S. Lal, "ID-based ring signature and proxy ring signature schemes from bilinear pairings," *International Journal of Network Security*, vol. 4, no. 2, pp. 187-192, 2007. Article (CrossRef Link)

[17] A. Bender, J. Katz and R. Morselli, "Ring signatures: Stronger definitions, and constructions without random oracles," *Journal of Cryptology*, vol. 22, no. 1, pp. 114-138, 2009. Article (CrossRef Link)

[18] H. Shacham, B. Waters, "Efficient ring signatures without random oracles," in *Proc. of International Workshop on Public Key Cryptography*, Beijing, China, pp. 166-180, 2007. Article (CrossRef Link)
[19] X. Boyen, "Mesh signatures," in *Proc. of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Barcelona, Spain, pp. 210-227, 2007. Article (CrossRef Link)
[20] X. Boyen, "Lattice mixing and vanishing trapdoors: a framework for fully secure short signatures and more," in *Proc. of International workshop on public key cryptography*, Paris, France, pp. 499-517, 2010. Article (CrossRef Link)
[21] L. Nguyen, "Accumulators from bilinear pairings and applications to id-based ring signatures and group membership revocation," *IACR Cryptology ePrint Archive*, vol. 2005, p. 123, 2005. Article (CrossRef Link)
[22] Z. Brakerski, Y. T. Kalai, "A framework for efficient signatures, ring signatures and identity based encryption in the standard model," *IACR Cryptology ePrint Archive*, vol. 2010, pp. 1-44, 2010. Article (CrossRef Link)
[23] F. H. Wang, Y. P. Hu, C. X. Wang, "A lattice-based ring signature scheme from bonsai trees," *Journal of Electronics and Information Technology*, vol. 32, no. 10, pp. 2400-2403, 2010. Article (CrossRef Link)
[24] J. Wang, B. Sun, "Ring signature schemes from lattice basis delegation," in *Proc. of International Conference on Information and Communications Security*, Beijing, China, pp. 15-28, 2011. Article (CrossRef Link)
[25] S. Wang, R. Zhao and Y. Zhang, "Lattice-based ring signature scheme under the random oracle model," *International Journal of High Performance Computing and Networking*, vol. 11, no. 4, pp. 332-341, 2018. Article (CrossRef Link)
[26] C. A. Melchor, S. Bettaieb, X. Boyen, L. Fousse, "Adapting lyubashevsky's signature schemes to the ring signature setting," in *Proc. of AFRICACRYPT 2013*, Cairo, Egypt, pp. 1-25, 2013. Article (CrossRef Link)
[27] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM review*, vol. 41, no. 2, pp. 303-332, 1999. Article (CrossRef Link)
[28] D. Micciancio, C. Peikert, "Trapdoors for lattices: simpler, tighter, faster, smaller," in *Proc. of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cambridge, UK, pp. 700-718, 2012. Article (CrossRef Link)
[29] V. Lyubashevsky, *Towards practical lattice-based cryptography*, University of California, San Diego, USA, 2008. Article (CrossRef Link)
[30] M. Ajtai, "Generating hard instances of lattice problems," in *Proc. of the twenty-eighth annual ACM symposium on Theory of Computing*, pp. 99-108, 1996. Article (CrossRef Link)
[31] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *Journal of the ACM (JACM)*, vol. 56, no. 6, pp. 1-40, 2009. Article (CrossRef Link)
[32] C. Gentry, C. Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. of the 40th Annual ACM Symposium on Theory of Computing*, Victoria, British Columbia, Canada, pp. 197-206, 2008. Article (CrossRef Link)
[33] D. Micciancio, O. Regev, "Lattice-based cryptography," *Post-quantum cryptography*, Cincinnati, OH, USA, pp. 147-191, 2009. Article (CrossRef Link)
[34] V. Lyubashevsky, "Lattice signatures without trapdoors," in *Proc. of Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Cambridge, UK, pp. 738-755, 2012. Article (CrossRef Link)
[35] P. Q. Nguyen, J. Zhang and Z. Zhang, "Simpler efficient group signatures from lattices," in *Proc. of IACR International Workshop on Public Key Cryptography*, Gaithersburg, MD, USA, pp. 401-426, 2015. Article (CrossRef Link)
[36] D. Cash, D. Hofheinz, E. Kiltz, C. Peikert, "Bonsai trees, or how to delegate a lattice basis," *Annual international conference on the theory and applications of cryptographic techniques*, Monaco, French Riviera, pp. 523-552, 2010. Article (CrossRef Link)

[37] D. Cash, D. Hofheinz, E. Kiltz, "How to delegate a lattice basis," *IACR Cryptology ePrint Archive*, vol. 2009, 2009. Article (CrossRef Link)
[38] H. Chen, Y. Hu, Z. Lian, "Leveled homomorphic encryption in certificateless cryptosystem," *Chinese Journal of Electronics*, vol. 26, no. 6, pp. 1213-1220, 2017. Article (CrossRef Link)
[39] D. Xin, L. Yang, L. Yan, X. F. Song, "Identity-based fully homomorphic encryption from ring-lwe: arbitrary cyclotomics, tighter parameters, efficient implementations," in *Proc. of 2019 2nd International Conference on Mathematics, Modeling and Simulation Technologies and Applications* (*MMSTA 2019*), Atlantis Press, pp. 143-147, 2019. Article (CrossRef Link)
[40] W. Gao, Y. P. Hu, B. C. Wang, J. Xie, "Improved lattice-based ring signature schemes from basis delegation," *The Journal of China Universities of Posts and Telecommunications*, vol. 23, no. 3, pp. 11-28, 2016. Article (CrossRef Link)
[41] G. M. Zhao, M. M. Tian, "A simpler construction of identity-based ring signatures from lattices," in *Proc. of International Conference on Provable Security*, Jeju, South Korea, pp. 277-291, 2018. Article (CrossRef Link)
[42] W. Gao, Y. P. Hu, B. C. Wang, J. S. Chen, X. Wang, "Efficient ring signature scheme without random oracle from lattices," *Chinese Journal of Electronics*, vol. 28, no. 2, pp. 266-272, 2019. Article (CrossRef Link)
[43] W. Gao, L. Chen, Y. P. Hu, C. J. P. Newton, B. C. Wang, J. S. Chen, "Lattice-based deniable ring signatures," *International Journal of Information Security*, vol. 18, no. 3, pp. 355-370, 2019. Article (CrossRef Link)
[44] Z. Liu, K. Nguyen, G. M. Yang, H. X. Wang, D. S. wong, "A lattice-based linkable ring signature supporting stealth addresses," in *Proc. of European Symposium on Research in Computer Security*, Luxembourg, pp. 726-746, 2019. Article (CrossRef Link)
[45] X. Lu, M. H. Au, Z. Zhang, "Raptor: a practical lattice-based (linkable) ring signature," in *Proc. of International Conference on Applied Cryptography and Network Security*, Bogota, Colombia, pp. 110-130, 2019. Article (CrossRef Link)
[46] Z. Q. Zhao, B. H. Ge, N. N. Zhao, P. K. Qin, H. Meng, "Efficient ring signature scheme on lattice," *Application Research of Computers*, vol. 38, no. 06, pp. 1855-1858, 2021. Article (CrossRef Link)
[47] Y. Ren, H. Guan, Q. Zhao, "An efficient lattice-based linkable ring signature scheme with scalability to multiple layer," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-10, 2021. Article (CrossRef Link)
[48] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979. Article (CrossRef Link)
[49] M. Ajtai, "Generating hard instances of the short basis problem," *International Colloquium on Automata, Languages, and Programming*, Prague, Czech Republic, pp. 1-9, 1999. Article (CrossRef Link)
[50] D. Micciancio, O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM Journal on Computing*, vol. 37, no. 1, pp. 267-302, 2007. Article (CrossRef Link)
[51] S. Agrawal, D. Boneh, X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proc. of Annual Cryptology Conference*, Santa Barbara, CA, USA, pp. 98-115, 2010. Article (CrossRef Link)
[52] J. C. Benaloh, M. Yung, "Distributing the power of a government to enhance the privacy of voters," in *Proc. of the Fifth Annual ACM Symposium on Principles of Distributed Computing*, Calgary, Alberta, Canada, pp. 52-62, 1986. Article (CrossRef Link)
[53] L. F. Cranor, "Electronic voting: computerized polls may save money, protect privacy," *XRDS: Crossroads, The ACM Magazine for Students*, vol. 2, no. 4, pp. 12-16, 1996. Article (CrossRef Link)
[54] M. Volkamer, "Requirements for electronic voting machines," *Evaluation of Electronic Voting*, pp. 73-91, 2009. Article (CrossRef Link)
[55] G. O. Ofori-Dwumfuo, E. Paatey, "The design of an electronic voting system," *Research Journal of Information Technology*, vol. 3, no. 2, pp. 91-98, 2011. Article (CrossRef Link)
[56] T. Hall, "Electronic voting," *Electronic Democracy*, pp. 153-176, 2012. Article (CrossRef Link)

[57] C. Y. Li, Y. Tian, X. B. Chen, J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Information Sciences*, vol. 546, pp. 253-264, 2021.
Article (CrossRef Link)

Yihua Zhou received her PhD degree in Beijing Institute of Technology, China in 2006. He is currently deputy director of the Institute of Information Security, Faculty of Information, Beijing University of Technology, and supervisor of postgraduates of computer science and technology and software engineering. His main research interests include Classical and quantum cryptography, privacy protection, blockchain theory and technology, network information security, trusted computing technology.

Songshou Dong studied for a master's degree in Beijing University of Technology in 2019. Her main research interests include post-quantum cryptography.

Yuguang Yang received her PhD degree in Beijing University of Posts and Telecommunications, China in 2006. She is currently a professor and PhD tutor in Beijing University of Technology. Her main research interests include information security and the intersection of information security and other disciplines.