Hindawi
Security and Communication Networks
Volume 2017, Article ID 1915239, 7 pages
https://doi.org/10.1155/2017/1915239

Research Article

An Efficient Code-Based Threshold Ring Signature Scheme with a Leader-Participant Model

Guomin Zhou,[1] Peng Zeng,[2] Xiaohui Yuan,[3,4] Siyuan Chen,[2] and Kim-Kwang Raymond Choo[5]

[1]*Department of Computer and Information Technology, Zhejiang Police College, Hangzhou, Zhejiang Province, China*
[2]*Shanghai Key Laboratory of Trustworthy Computing, East China Normal University, Shanghai, China*
[3]*Department of Computer Science and Engineering, University of North Texas, Denton, TX 76203, USA*
[4]*College of Information Engineering, China University of Geosciences, Wuhan, China*
[5]*Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX 78249, USA*

Correspondence should be addressed to Xiaohui Yuan; xiaohui.yuan@unt.edu

Received 23 March 2017; Accepted 2 July 2017; Published 1 August 2017

Academic Editor: Mamoun Alazab

Digital signature schemes with additional properties have broad applications, such as in protecting the identity of signers allowing a signer to anonymously sign a message in a group of signers (also known as a ring). While these number-theoretic problems are still secure at the time of this research, the situation could change with advances in quantum computing. There is a pressing need to design PKC schemes that are secure against quantum attacks. In this paper, we propose a novel code-based threshold ring signature scheme with a leader-participant model. A leader is appointed, who chooses some shared parameters for other signers to participate in the signing process. This leader-participant model enhances the performance because every participant including the leader could execute the decoding algorithm (as a part of signing process) upon receiving the shared parameters from the leader. The time complexity of our scheme is close to Courtois et al.'s (2001) scheme. The latter is often used as a basis to construct other types of code-based signature schemes. Moreover, as a threshold ring signature scheme, our scheme is as efficient as the normal code-based ring signature.

1. Introduction

Public-key cryptographic (PKC) method remains a topic of research interest partly due to its role in our increasingly digitalized society and the challenge of designing efficient and provably secure schemes with additional features required in contemporary applications. Existing PKC schemes are generally based on the hardness of number theory problems, such as factorization and discrete logarithm problems. While these number-theoretic problems are still secure at the time of this research, the situation could change with advances in quantum computing. For example, in the 1990s, Shor presented a quantum attack algorithm that could be used to solve both factorization and discrete logarithm problems in polynomial time with quantum computers [1, 2]. Thus, there is a pressing need to design PKC schemes that are secure against quantum attacks. Code-based PKC schemes, established by McEliece in 1978 [3], are one kind of such postquantum PKC schemes. Code-based PKC schemes are based on hard problems in coding theory and are considered as an appropriate solution to keep the message secure in the quantum era.

In 2001, Rivest et al. presented the ring signature as a digital signature scheme with additional property [4]. In a ring signature scheme, each member of the ring has a unique public-private key pair. For a message m, any signer in the ring is able to generate a signature on m with the private key and the ring public key which consists of the public keys of all signers in the ring. The user could only verify the validation of the signature without knowing who the true signer of the message m is; thus, it preserves the anonymity of the signer. Due to this property, ring signature has many potential applications in real-world scenarios. One practical application is a company soliciting opinions from its

employees. In order to improve the reliability of employee feedback, it is often necessary for multiple employees (which can be thousands in a large multinational corporation or company) to submit their opinions. At the same time, in order to prevent the retaliation of senior management or line supervisor, the true identity of the participating employees should not be revealed. Threshold ring signature is one appropriate solution for such an application, which enables the employees to reach a certain quantity to jointly generate a valid signature. Ring signature can also be used for data sharing in the cloud [5] and for privacy-preserving public auditing of shared data [6].

Since the notion of ring signatures was introduced, there have been a number of ring signature schemes proposed in the literature. Shacham and Waters [7] presented the first efficient ring signature scheme based on bilinear groups. The scheme is anonymous against full key exposure and unforgeable with respect to insider corruption. Kar [8] proposed an online/offline ring signature scheme whose security is based on both computational Diffie-Hellman and k-CAA problems. The scheme satisfies signer ambiguity and enables the misbehavior of the signer to be detected. Wang et al. [9] presented a new concept of identity-based quotable ring signature which could be used to derive new ring signatures on substrings of an original message from an original ring signature on the original message. The scheme is based on bilinear pairing of composite order and proven to be secure under the assumption that the subgroup decision problem and computational Diffie-Hellman problem are hard. Zeng et al. [10]. proposed an efficient noninteractive deniable ring signature scheme and proved its security in the standard model. Nevertheless, all the aforementioned schemes [7–10] are based on the hard problems in number theory and thus will became insecure as soon as large quantum computers are built. There are also some alternative ring signature schemes that are based on the hard problems not affected by quantum computer attacks, such as the schemes based on NTRU lattices [11] and based on multivariate quadratic polynomials [12].

Bresson et al. extended the notion of ring signatures into threshold ring signatures, which are increasingly popular due to their practical utilities in comparison to the conventional ring signatures [13]. Similar to ring signature schemes, a (t, N) threshold ring signature scheme allows at least t signers in the ring of N signers to cooperate with each other to sign a message without leaking any identity information of the t signers. Existing threshold ring signature schemes are mostly based on the number theory [14–17]; hence, as mentioned above, such schemes could be insecure in the quantum world. To the best of our knowledge, Dallot and Vergnaud's scheme [18] and Aguilar Melchor et al.'s scheme [19] are the only two code-based threshold ring signature schemes published in the literature. Dallot and Vergnaud's scheme [18] combined Bresson et al.'s construction [13] and Courtois et al.'s signature [20], which results in the signature size twice the number of system users. Aguilar Melchor et al.'s scheme [19] is a generalization of Stern's identification and signature scheme [21] and has low efficiency in the signature size.

In this paper, we propose a novel code-based (t, N) threshold ring signature scheme. The security of our proposed scheme is based on the hardness of the syndrome decoding (SD) problem (known to be an NP-complete problem) and the indistinguishability of Goppa codes from random linear codes. In the proposed scheme, a leader is appointed from the t signers, who chooses some shared parameters for other $t-1$ signers to participate in the signing process. This leader-participant model enhances the performance because every participant including the leader could execute the decoding algorithm (as a part of signing process) concurrently and immediately upon receiving the shared parameters from the leader.

The rest of this paper is organized as follows: Section 2 presents background information and preliminaries. Section 3 describes our proposed method, whose security analysis is presented in Section 4 and efficiency is evaluated in Section 5. Conclusion is presented in Section 6.

2. Preliminaries

2.1. Definitions and Problems in Coding Theory. For the rest of this paper, we consider linear codes over binary field $\mathbb{F}_2$.

Definition 1 (weight). The (Hamming) weight of a vector (or word) $c \in \mathbb{F}_2^n$, denoted by $wt(c)$, is the number of nonzero bits in c.

Definition 2 (code). An $[n, k, d]$ (linear) code $\mathscr{C}$ is a linear k-dimensional subspace of $\mathbb{F}_2^n$ with minimum distance d, which is defined as

$$d = \min_{c_1 \neq c_2 \in \mathscr{C}} wt\left(c_1 - c_2\right). \tag{1}$$

An $[n, k, d]$ code has the $\lfloor (d-1)/2 \rfloor$-error-correcting capability.

Definition 3 (generator matrix and parity-check matrix). A generator matrix G of an $[n, k, d]$ code $\mathscr{C}$ is a $k \times n$ matrix whose rows form a basis of $\mathscr{C}$. A parity-check matrix H of $\mathscr{C}$ is a generator matrix of the dual of $\mathscr{C}$, which has the order $(n-k) \times n$.

The security of our threshold ring signature scheme is based on the following two hard problems in coding theory. Let $\varepsilon_{n,w}$ denote the set of all vectors of length n and weight w.

Problem 4 (Syndrome Decoding (SD)).

Input. It includes an integer w, a vector $s \in \mathbb{F}_2^r$, and a $r \times n$ random binary matrix H.

Property. Find a vector $e \in \varepsilon_{n,w}$ such that

$$He^T = s^T, \tag{2}$$

where v^T denotes the transpose of vector (or matrix) v. The advantage of adversary $\mathscr{A}$ solves the SD problem denoted by $\mathrm{Adv}_{\mathrm{SD}}(\mathscr{A})$, which is negligible since the SD problem was proven to be NP-complete in [22].

To describe the following Goppa Code Distinguishing (GCD) problem, we denote by $\mathcal{G}_0 = \text{Goppa}(n-k, n)$ the set of parity-check matrices of all binary irreducible $[n, k]$ Goppa codes and $\mathcal{G}_1 = \text{Rand}(n-k, n)$ the set of the parity-check matrices of all random binary $[n, k]$ linear codes. Set $\mathcal{G} = \mathcal{G}_0 \cup \mathcal{G}_1$.

Problem 5 (Goppa Code Distinguishing (GCD)).

Input. A matrix H is randomly chosen from set $\mathcal{G}$.

Property. Return b s.t. $H \in \mathcal{G}_b$.

Let $\mathcal{D}$ be a probabilistic polynomial time (PPT) distinguisher for the GCD problem. The advantage, denoted by $\text{Adv}_{n,k}(\mathcal{D})$, of $\mathcal{D}$ is defined as follows:

$$\text{Adv}_{n,k}(\mathcal{D}) = \left|\Pr\left[\mathcal{D}(H) = b \mid b \longleftarrow_R \{0,1\}, H \longleftarrow \mathcal{G}_b\right] - \frac{1}{2}\right|. \tag{3}$$

The indistinguishability assumption of the GCD problem holds if $\text{Adv}_{n,k}(\mathcal{D})$ is negligible.

2.2. (t, N) *Threshold Ring Signature.* We use the formal definition of threshold ring signature scheme following the work of Bresson et al. [13]. Let us assume that there are N signers $\mathcal{S}_i$, $1 \le i \le N$, forming a ring $\mathcal{R}$ and the threshold of generating a valid signature is t with $t < N$. For simplicity, we assume the first t signers $\mathcal{S}_1, \ldots, \mathcal{S}_t$ are the true signers in $\mathcal{R}$. A (t, N) threshold ring signature scheme consists of four algorithms (*Setup, KeyGen, Sign, Verify*).

Setup(λ). The algorithm takes as input a security parameter λ and outputs the system public parameter $\mathcal{P}$.

KeyGen($\mathcal{P}$). The algorithm takes as input the parameter $\mathcal{P}$ and generates N pairs of public-private key (pk_i, sk_i) for the signers $\mathcal{S}_i \in \mathcal{R}$, $1 \le i \le N$. The N public keys pk_i, $1 \le i \le N$, form the ring public key $PK = \{pk_1, pk_2, \ldots, pk_N\}$ and each private key sk_i is sent to the signer $\mathcal{S}_i$ via a secure channel, $1 \le i \le N$.

Sign($m, \mathcal{P}, PK, TSK$). The algorithm takes as input a message m, the parameter $\mathcal{P}$, the ring public key PK, and a private key set $TSK = \{sk_1, \ldots, sk_t\}$ of t singers and outputs a threshold ring signature σ on m.

Verify(m, PK, σ). The algorithm takes as input the message m, the ring public key PK, and the threshold ring signature σ and outputs 1 if (m, σ) is a valid message-signature pair. Otherwise, the algorithm outputs 0.

2.3. Security Model. A threshold ring signature scheme needs to satisfy the correctness, anonymity, and unforgeability properties.

Correctness. We say that a (t, N) ring signature scheme satisfies the correctness property if, for any valid t private key set TSK and message m, the following equation holds:

$$Verify(m, PK, Sign(m, \mathcal{P}, PK, TSK)) = 1. \tag{4}$$

Anonymity. We say that a (t, N) ring signature scheme satisfies the anonymity property if, for a given message-signature pair (m, σ), any attacker $\mathcal{A}$ has only the probability $1/\binom{N}{t}$ to determine the real signers participating in the signing process. More formally, the anonymity says that, for two message-signature pairs (m, σ_0) and (m, σ_1) signed by two signer sets $\{\mathcal{S}_{01}, \ldots, \mathcal{S}_{0t}\}$ and $\{\mathcal{S}_{11}, \ldots, \mathcal{S}_{1t}\}$, respectively, the following absolute value is negligible:

$$\left|\Pr\left[\mathcal{A}(\sigma_b) = b \mid b \longleftarrow_R \{0,1\}, \sigma_b \longleftarrow \{\mathcal{S}_{b1}, \ldots, \mathcal{S}_{bt}\}\right] - \frac{1}{2}\right|. \tag{5}$$

Unforgeability. To define unforgeability, we introduce an attack model of (t, N) threshold ring signatures. A PPT forger $\mathcal{F}$ is allowed to access a corruption oracle, a signature oracle, and a hash oracle and make adaptively queries on them. After the corruption queries, $\mathcal{F}$ can obtain at most $t-1$ private keys of ring members. $\mathcal{F}$ can also use the signature queries to obtain threshold ring signatures for messages and signers chosen by $\mathcal{F}$. Then, $\mathcal{F}$ attempts to forge a signature σ' on a chosen message m' (note that σ' is not allowed to be an output of some signature oracle). We say that a (t, N) threshold ring signature scheme satisfies the unforgeability property if, for any PPT attacker $\mathcal{F}$, the probability, denoted by $\text{Succ}_{\mathcal{F}}$, that $\mathcal{F}$ succeeds in this attack is negligible.

We remark that there is a special signer, referred to as leader, in our (t, N) threshold ring signature scheme. The leader is randomly chosen during each sign process without any additional privileges. The leader in our scheme must act honestly. Otherwise, anonymity of t participating signers cannot be achieved.

3. Our Threshold Ring Signature Scheme

For simplicity, we denote $v_{1 \le i \le N}$ to be the sequence $v_1, v_2, \ldots, v_N$. Our code-based (t, N) threshold ring signature scheme can be described as follows.

Setup(λ). Given a security parameter λ, the algorithm chooses integers n, k, d, and w to, respectively, represent length, dimension, minimum distance, and error-correcting ability of the code underpinning our scheme. The algorithm outputs the system public parameter, $\mathcal{P} = (n, k, d, w)$.

KeyGen($\mathcal{P}$). Given $\mathcal{P} = (n, k, d, w)$, the algorithm performs the following:

(i) For each signer $\mathcal{S}_i$ in the ring $\mathcal{R} = \{\mathcal{S}_i | 1 \le i \le N\}$, choose a parity-check matrix H_i of a w-error-correcting irreducible $[n, k, d]$ Goppa code, which has a corresponding fast decoding algorithm $\mathcal{DEC}_{H_i}$, $1 \le i \le N$.

(ii) For each signer $\mathcal{S}_i \in \mathcal{R}$, choose a random binary $(n-k) \times (n-k)$ invertible matrix Q_i and a random permutation $n \times n$ matrix P_i, $1 \le i \le N$.

(iii) Compute

$$\widetilde{H}_i = Q_i H_i P_i, \quad 1 \le i \le N. \tag{6}$$

(iv) For each signer $\mathcal{S}_i \in \mathcal{R}$, set the private key $sk_i = (Q_i, H_i, P_i, \mathcal{DEC}_{H_i})$ and public key $pk_i = \widetilde{H}_i$, $1 \le i \le N$. The ring public key is

$$PK = \left(\widetilde{H}_{1\le i\le N}\right) = \left(\widetilde{H}_1, \widetilde{H}_2 \ldots, \widetilde{H}_N\right) \tag{7}$$

and each private key $sk_i = (Q_i, H_i, P_i, \mathcal{DEC}_{H_i})$ is sent to the signer $\mathcal{S}_i$ via a secure channel, $1 \le i \le N$.

Sign$(m, \mathcal{P}, PK, TSK)$. Given message m, system parameter $\mathcal{P}$, ring public key $PK = (\widetilde{H}_{1\le i\le N})$, and private key set $TSK = (sk_{1\le i\le t})$ of t signers, where $sk_i = (Q_i, H_i, P_i, \mathcal{DEC}_{H_i})$ for each $1 \le i \le t$, the algorithm first elects a leader $\mathcal{S}_l$ randomly from the involved signer set $\{\mathcal{S}_i | 1 \le i \le t\}$. Note that $\mathcal{S}_l$ is just a signer participating in the signing process without any additional privileges. The signing processes are executed as follows:

(i) For each $\mathcal{S}_i$, $1 \le i \ne l \le t$, randomly choose $e_{ij} \in \mathbb{F}_2^n$, $j = t+1, t+2, \ldots, N$, and compute

$$s_i^T = h(m)^T + \sum_{j=t+1}^{N} \widetilde{H}_j e_{ij}^T, \quad 1 \le i \ne l \le t, \tag{8}$$

where $h : \{0,1\}^* \to \{0,1\}^{n-k}$ is a one-way collision-resistant hash function.

(ii) For each $\mathcal{S}_i$, $1 \le i \ne l \le t$, compute $Q_i^{-1} s_i^T$. If $Q_i^{-1} s_i^T$ is a decodable syndrome, compute $\mathcal{DEC}_{H_i}(Q_i^{-1} s_i^T)$ to obtain a vector e_i' such that

$$H_i e_i'^T = Q_i^{-1} s_i^T, \quad 1 \le i \ne l \le t. \tag{9}$$

Otherwise, return to the previous step to recompute s_i.

(iii) Compute

$$e_i^T = P_i^T e_i'^T, \quad 1 \le i \ne l \le t. \tag{10}$$

For all signers $\mathcal{S}_i$, $1 \le i \ne l \le t$, the above signing processes can be concurrent.

(iv) Each $\mathcal{S}_i$ sends $N - t + 1$ generated vectors $(e_i, e_{i(t+1)}, e_{i(t+2)}, \ldots, e_{iN})$, $1 \le i \ne l \le t$, to the leader $\mathcal{S}_l$.

(v) Upon receiving all vectors $(e_i, e_{i(t+1)}, e_{i(t+2)}, \ldots, e_{iN})$, $1 \le i \ne l \le t$, $\mathcal{S}_l$ executes the following steps:

(a) For each $t+1 \le j \le N$, choose a random e_{lj} under the condition $wt(e_{lj} + \sum_{i=1, i\ne l}^{t} e_{ij}) = w$. Set

$$e_j = \sum_{i=1}^{t} e_{ij}, \quad t+1 \le j \le N. \tag{11}$$

(b) If t is an odd number, then compute

$$s_l^T = h(m)^T + \sum_{j=t+1}^{N} \widetilde{H}_j e_{lj}^T. \tag{12}$$

Otherwise (i.e., t is an even number), compute

$$s_l^T = \sum_{j=t+1}^{N} \widetilde{H}_j e_{lj}^T. \tag{13}$$

(c) Compute $Q_l^{-1} s_l^T$. If $Q_l^{-1} s_l^T$ is a decodable syndrome, compute $\mathcal{DEC}_{H_l}(Q_l^{-1} s_l^T)$ to obtain an vector e_l' such that

$$H_l e_l'^T = Q_l^{-1} s_l^T. \tag{14}$$

Otherwise, return to the first step executed by $\mathcal{S}_l$ to choose another e_{lj}.

(d) Compute

$$e_l^T = P_l^T e_l'^T. \tag{15}$$

(e) Output $\sigma = (e_1, e_2, \ldots, e_N)$ as the threshold ring signature on the message m.

Verify(m, PK, σ). Given the ring public key $PK = (\widetilde{H}_{1\le i\le N})$ and a message-signature pair $(m, \sigma = (e_1, e_2, \ldots, e_N))$, the verifier can check the validity of σ by executing the following steps:

(i) Check if $e_i \in \varepsilon_{n,w}$ holds for each $1 \le i \le N$. If it does not, output 0 and terminate the verification process.

(ii) Check if

$$h(m)^T = \sum_{i=1}^{N} \widetilde{H}_i e_i^T \tag{16}$$

holds. If it holds, output 1, and 0, otherwise.

4. Security Analysis

In the section, we analyze the security of our scheme, based on the security model defined in Section 2.3.

4.1. Correctness. Let $(m, \sigma = (e_1, e_2, \ldots, e_N))$ be a valid message-signature pair generated by t signers $\mathcal{S}_i$, $i = 1, 2, \ldots, t$, as in Section 3. First, it is clear that each e_i has length n and weight w, based on our construction (see (10), (11), and (15)). Thus, $e_i \in \varepsilon_{n,w}$ holds for each $1 \le i \le N$. Now it remains to show (16): $h(m)^T = \sum_{i=1}^{N} \widetilde{H}_i e_i^T$. Starting from the right side of the equation, we have

$$\sum_{i=1}^{N} \widetilde{H}_i e_i^T = \sum_{i=1}^{t} \widetilde{H}_i e_i^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T$$

$$\overset{(6)}{=} \sum_{i=1}^{t} Q_i H_i P_i e_i^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T$$

$$\begin{aligned}
&\overset{(10),(15)}{=} \sum_{i=1}^{t} Q_i H_i e_i'^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&\overset{(9),(14)}{=} \sum_{i=1}^{t} s_i^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&= s_l^T + \sum_{i=1,i\neq l}^{t} s_i^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&\overset{(8)}{=} s_l^T + (t-1)\, h(m)^T + \sum_{i=1,i\neq l}^{t} \sum_{j=t+1}^{N} \widetilde{H}_j e_{ij}^T \\
&\quad + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T.
\end{aligned} \tag{17}$$

Next, we consider two cases with respect to the value of t. Recall that all the operations in this paper are executed over the binary field $\mathbb{F}_2$. If t is an odd number, then we have

$$\begin{aligned}
\sum_{i=1}^{N} \widetilde{H}_i e_i^T &= s_l^T + \sum_{i=1,i\neq l}^{t} \sum_{j=t+1}^{N} \widetilde{H}_j e_{ij}^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&\overset{(12)}{=} h(m)^T + \sum_{j=t+1}^{N} \widetilde{H}_j e_{lj}^T + \sum_{i=1,i\neq l}^{t} \sum_{j=t+1}^{N} \widetilde{H}_j e_{ij}^T \\
&\quad + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&= h(m)^T + \sum_{j=t+1}^{N} \left(\widetilde{H}_j e_{lj}^T + \sum_{i=1,i\neq l}^{t} \widetilde{H}_j e_{ij}^T \right) \\
&\quad + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&\overset{(11)}{=} h(m)^T + \sum_{j=t+1}^{N} \widetilde{H}_j e_j^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T = h(m)^T.
\end{aligned} \tag{18}$$

Otherwise (i.e., t is an even number), we have

$$\begin{aligned}
\sum_{i=1}^{N} \widetilde{H}_i e_i^T &= s_l^T + h(m)^T + \sum_{i=1,i\neq l}^{t} \sum_{j=t+1}^{N} \widetilde{H}_j e_{ij}^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&\overset{(13)}{=} \sum_{j=t+1}^{N} \widetilde{H}_j e_{lj}^T + h(m) + \sum_{i=1,i\neq l}^{t} \sum_{j=t+1}^{N} \widetilde{H}_j e_{ij}^T \\
&\quad + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T \\
&\overset{(11)}{=} h(m)^T + \sum_{j=t+1}^{N} \widetilde{H}_j e_j^T + \sum_{i=t+1}^{N} \widetilde{H}_i e_i^T = h(m)^T.
\end{aligned} \tag{19}$$

To sum up, we have $h(m)^T = \sum_{i=1}^{N} \widetilde{H}_i e_i^T$ for both cases of t. Together with the relation $e_i \in \varepsilon_{n,w}$, $1 \le i \le N$, we have

$$Verify\,(m, PK, \sigma) = 1. \tag{20}$$

This demonstrates that our threshold ring signature scheme satisfies the correctness property.

4.2. Anonymity. Assume that there is an adversary $\mathscr{A}$ who receives two valid message-signature pairs $(m, \sigma_0 = (e_{01}, e_{02}, \ldots, e_{0N}))$ and $(m, \sigma_1 = (e_{11}, e_{12}, \ldots, e_{1N}))$ generated by two sets $\{\mathcal{S}_{01}, \ldots, \mathcal{S}_{0t}\}$ and $\{\mathcal{S}_{11}, \ldots, \mathcal{S}_{1t}\}$ of signers, respectively. From the view of $\mathscr{A}$, each vector e_{bi}, $b = 0, 1$, $i = 1, 2, \ldots, N$, in the signatures σ_0 or σ_1 is completely random. This results in a negligible absolute value $|\Pr[\mathscr{A}(\sigma_b) = b | b \leftarrow_R \{0,1\}, \sigma_b \leftarrow \{\mathcal{S}_{b1}, \ldots, \mathcal{S}_{bt}\}] - 1/2|$ and, hence, our threshold ring signature scheme satisfies the anonymity property.

4.3. Unforgeability. We prove the unforgeability using the attack model in Section 2.3. Let $\mathscr{F}$ be a PPT algorithm that has a nonnegligible probability $\mathrm{Succ}_{\mathscr{F}}$ in attacking our proposed (t, N) threshold ring signature scheme. Using $\mathscr{F}$, we construct another PPT algorithm $\mathscr{C}$ to solve the SD problem with nonnegligible advantage. That is, given a random $(n - k) \times n$ matrix H' and a random decodable syndrome s', $\mathscr{C}$ can find a vector $e' \in \varepsilon_{n,w}$, s.t. $H' e'^T = s'^T$. Thus, $\mathscr{C}$ plays the following games with $\mathscr{F}$.

Game 0. $\mathscr{C}$ randomly chooses an index l from $\{1, 2, \ldots, N\}$ and sets the public key PK_l of the signer $\mathcal{S}_l$ as H'. For all other signers, $\mathscr{C}$ chooses $N - 1$ parity-check matrices, denoted by H_i $(1 \le i \le N, i \neq l)$, of random permuted Goppa codes as their public keys and the corresponding private keys will not be used. After that, $\mathscr{C}$ sends all N matrices to $\mathscr{F}$. $\mathscr{F}$ queries the hash oracle and the sign oracle several times and seeks to obtain a valid signature for some message. We denote the probability that $\mathscr{F}$ wins Game 0 by $\Pr(G_0)$.

Game 1. $\mathscr{C}$ replaces the original hash function with the hash simulator $\mathscr{H}$. $\mathscr{C}$ can respond to $\mathscr{F}$ as follows.

When $\mathscr{F}$ makes a query to the hash simulator $\mathscr{H}$, $\mathscr{H}$ stores an index r in a list $\Lambda(m)$ associated with message m. If $\Lambda(m)$ is empty, then $\mathscr{H}$ just chooses a random vector $e_l \in \mathbb{F}_2^n$ and computes $s_l^T = H' e_l^T + \Sigma_{i=1,i\neq l}^{N} H_i e_i^T$ as the output of the simulator. Otherwise (i.e., $r = \Lambda(M)$), $\mathscr{H}$ picks a random e_l from $\varepsilon_{n,w}$ and computes $s_l^T = H' e_l^T + \Sigma_{i=1,i\neq l}^{N} H_i e_i^T$ as the output of the simulator. In both cases, $\mathscr{H}$ outputs a random s_l^T. So we have the probability that $\mathscr{F}$ wins Game 1 equal to $\Pr(G_1) = \Pr(G_0)$.

Game 2. $\mathscr{C}$ replaces the signature oracle with the signing simulator *Sim*. $\mathscr{C}$ can respond to $\mathscr{F}$ as follows.

When $\mathscr{F}$ makes a query to *Sim* on message m, *Sim* chooses a random index $r \in \mathbb{F}_2$ and sets $\Lambda(m) = r$. Then, $\mathscr{C}$ runs $\mathscr{H}$ with input m. If there is no $e_l \in \varepsilon_{n,w}$, then *Sim* aborts; otherwise, *Sim* outputs e_l and sets $\Lambda(m)$ empty.

Game 2 differs from Game 1 only in the case that *Sim* aborts. The probability that *Sim* aborts is at most $q_{\mathrm{Sim}}/2^n$,

where q_{Sim} represents the maximum query times to the *Sim*. It follows that the probability, denoted by $\Pr(G_2)$, of $\mathcal{F}$ winning Game 2 satisfies

$$\left|\Pr\left(G_1\right) - \Pr\left(G_2\right)\right| \leq \frac{q_{\text{Sim}}}{2^n}. \tag{21}$$

Game 3. $\mathcal{C}$ replaces the public key (the permuted parity-check matrix of random Goppa codes) with the parity-check matrix of random linear code for each signer in this game. According to the indistinguishability assumption (see Section 2), $\mathcal{F}$ has only a negligible advantage $\text{Adv}_{n,k}(\mathcal{F})$ in solving the GCD problem. That is, we have the probability that $\mathcal{F}$ wins Game 3 as $|\Pr(G_3) - \Pr(G_2)| = \text{Adv}_{n,k}(\mathcal{F})$.

Game 4. The wining condition is changed in this game. $\mathcal{C}$ picks a random number k in $\{1, \ldots, q_{\mathcal{H}}\}$, where $q_{\mathcal{H}}$ is the maximum query times to $\mathcal{H}$. $\mathcal{F}$ should generate the k-th forgery message-signature pair which can pass the verification. Hence, the probability of $\mathcal{F}$ wining this game is $\Pr(G_4) = \Pr(G_3)/q_{\mathcal{H}}$.

We remark that if $\mathcal{F}$ wins Game 4, then $\mathcal{F}$ is able to inverse the SD problem (i.e., find a vector $e' \in \varepsilon_{n,w}$ s.t. $H'e'^T = s'^T$). Hence, we have $\Pr(G_4) = \text{Adv}_{\text{SD}}(\mathcal{C})$.

Combining all these together, we have $\text{Succ}_{\mathcal{F}} = \Pr(G_0)$ and

$$q_{\mathcal{H}}\text{Adv}_{\text{SD}}\left(\mathcal{C}\right) + \text{Adv}_{n,k}\left(\mathcal{F}\right) \geq \text{Succ}_{\mathcal{F}} + \frac{q_{\text{Sim}}}{2^n}. \tag{22}$$

In other words, if there is a PPT forger $\mathcal{F}$ which can forge a valid message-signature pair with a nonnegligible probability in attacking our scheme, then we can construct a PPT algorithm $\mathcal{C}$ to inverse the SD problem with a nonnegligible probability. Thus, we can conclude that our proposed threshold ring signature scheme is existentially unforgeable under the chosen message attack if both the GCD problem and SD problem are hard.

5. Efficiency Analysis

In this section, we evaluate the efficiency of our threshold ring signature scheme, in terms of the public key size, the signature size, and the time complexity of the signing process.

The Public-Key Size. As mentioned in Section 3, the ring public key in our threshold ring signature scheme is $PK = (\widetilde{H}_1, \widetilde{H}_2, \ldots, \widetilde{H}_N)$, in which each $\widetilde{H}_i$ is an $(n-k) \times n$ matrix over $\mathbb{F}_2, i = 1, 2, \ldots, N$. Hence, the ring public key PK has size $n(n-k)N$ bits.

The Signature Size. The signature in our scheme is $\sigma = (e_1, e_2, \ldots, e_N)$, where $e_i \in \varepsilon_{n,w}$, $i = 1, 2, \ldots, N$. This results in a signature of size nN bits.

Time Complexity of the Signing Process. We omit the consideration of computing a hash function because it is a fast operation compared to other operations involved in our (t, N) threshold ring signature scheme. As previously discussed in Section 3, each signer $\mathcal{S}_i$ in our scheme should compute a vector s_i (see (8), (12), and (13)), $1 \leq i \leq t$. The time complexity of computing s_i is $O((N-t)(n-k)n)$. According to Engelbert et al. [23], a fast decoding algorithm has time complexity $O(n^2)$; therefore, we should execute $t!$ decoding algorithms on average to generate a decodable syndrome [20]. So the total time complexity of the signing process in our threshold ring signature scheme is as follows:

$$2t!\left(O\left((N-t)\left(n-k\right)n\right) + O\left(n^2\right)\right). \tag{23}$$

Note that the time complexity of the signing process in our scheme is independent of the number of signers. The factor of the complexity of our method is two, rather than t, in comparison to the CFS scheme [20]. This is because $t-1$ signers (with the exception of the leader) can undertake concurrent operations in our scheme. This enables our scheme to be an efficient code-based threshold ring signature scheme.

6. Conclusion

In this paper, we proposed a novel threshold ring signature scheme based on the hard problems in coding theory. We prove that our method satisfies correctness, unforgeability, and anonymity. In comparison to other postquantum digital signature schemes, our scheme has a lower signature size. Our scheme also uses the leader-participant model to allow signers to sign messages concurrently. This significantly reduces the time complexity of the signing process.

Future research includes exploring practical applications of the proposed scheme and implementing a prototype of the scheme for evaluation in a real-world context (e.g., in an Internet of Battlefield Things application).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work was supported in part by the NSFC-Zhejiang Joint Fund for the Integration of Industrialization and Informatization under Grant no. U1509219, the Shanghai Natural Science Foundation under Grant no. 17ZR1408400, the National Natural Science Foundation of China under Grant no. 61632012, and the Shanghai Sailing Program under Grant no. 17YF1404300.

References

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (SFCS '94)*, pp. 124–134, IEEE, 1994.

[2] 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.

[3] R. J. McEliece, "A public-key cryptosystem based on algebraic coding theory," *DSN Progress Report 42–44*, pp. 114–116, 1978.

[4] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in Cryptology—ASIACRYPT*, vol. 2248 of *Lecture Notes in Comput. Sci.*, pp. 552–565, Springer, 2001.

[5] N. Shirsath Priyanka and K. BECOMP, "Data Sharing in Cloud Using Identity Based Ring Signature," in *Proceedings of the BECOMP K. Data Sharing in Cloud Using Identity Based Ring Signature. International Research Journal of Engineering and Technology*, p. 07, 2015.

[6] B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," *IEEE Transactions on Cloud Computing*, vol. 2, no. 1, pp. 43–56, 2014.

[7] H. Shacham and B. Waters, "Efficient ring signatures without random oracles," in *Public Key Cryptography*, vol. 4450 of *Lecture Notes in Comput. Sci.*, pp. 166–180, Springer, Berlin, Germany, 2007.

[8] J. Kar, "Online/off-line ring signature scheme with provable security," in *Proceedings of the 13th IEEE International Conference on Intelligence and Security Informatics, ISI 2015*, p. 197, May 2015.

[9] K. Wang, Y. Mu, and W. Susilo, "Identity-based quotable ring signature," *Information Sciences. An International Journal*, vol. 321, Article ID 11586, pp. 71–89, 2015.

[10] S. Zeng, Q. Li, Z. Qin, and Q. Lu, "Non-interactive deniable ring signature without random oracles," *Security and Communication Networks*, vol. 9, no. 12, pp. 1810–1819, 2016.

[11] Y. Zhang, Y. Hu, J. Xie, and M. Jiang, "Efficient ring signature schemes over NTRU Lattices," *Security and Communication Networks*, vol. 9, no. 18, pp. 5252–5261, 2016.

[12] M. Mohamed S E and A. Petzoldt, "Efficient Multivariate Ring Signature Schemes," in *IACR Cryptology ePrint Archive*, p. 247, 247, 2017.

[13] E. Bresson, J. Stern, and M. Szydlo, "Threshold ring signatures and applications to ad-hoc groups," in *Advances in Cryptology*, Lecture Notes in Comput. Sci., pp. 465–480, Springer, Berlin, Germany, 2002.

[14] A. Petzoldt, S. Bulygin, and J. Buchmann, "A multivariate based threshold ring signature scheme," *Applicable Algebra in Engineering, Communication and Computing*, vol. 24, no. 3-4, pp. 255–275, 2013.

[15] H. Wang and S. Han, "A provably secure threshold ring signature scheme in certificateless cryptography," in *Proceedings of the 2010 International Conference of Information Science and Management Engineering, ISME 2010*, pp. 105–108, August 2010.

[16] T. H. Yuen, J. K. Liu, M. H. Au, W. Susilo, and J. Zhou, "Threshold ring signature without random oracles," in *Proceedings of the 6th International Symposium on Information, Computer and Communications Security, ASIACCS 2011*, pp. 261–267, March 2011.

[17] H. Xiong, Z. Qin, F. Li, and J. Jin, "Identity-based threshold ring signature without pairings," in *Proceedings of the 2008 International Conference on Communications, Circuits and Systems, ICCCAS 2008*, pp. 478–482, May 2008.

[18] L. Dallot and D. Vergnaud, "Provably secure code-based threshold ring signatures," in *Cryptography and Coding*, vol. 5921, pp. 222–235, Springer, 2009.

[19] C. Aguilar Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *Institute of Electrical and Electronics Engineers. Transactions on Information Theory*, vol. 57, no. 7, pp. 4833–4842, 2011.

[20] N. T. Courtois, M. Finiasz, and N. Sendrier, "How to achieve a McEliece-based digital signature scheme," in *Advances in Cryptology—ASIACRYPT 2001*, vol. 2248 of *Lecture Notes in Comput. Sci.*, pp. 157–174, Springer, Berlin, Germany, 2001.

[21] D. R. Stinson, *Advances in Cryptology — CRYPTO' 93*, vol. 773, Springer, Berlin, Germany, 1994.

[22] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the Inherent Intractability of Certain Coding Problems," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 384–386, 1978.

[23] D. Engelbert, R. Overbeck, and A. Schmidt, "A summary of McEliece-type cryptosystems and their security," *Journal of Mathematical Cryptology*, vol. 1, no. 2, pp. 151–199, 2007.