Abstract—This paper proposes a new proactive weighted threshold signature scheme based on Iftene's general secret sharing, the generalized Chinese remainder theorem, and the RSA threshold signature, which is itself based on the Chinese reminder theorem. In our scheme, group members are divided into different subgroups, and a positive weight is associated to each subgroup, where all members of the same subgroup have the same weight. The group signature can be generated if and only if the sum of the weights of members involved is greater than or equal to a fixed threshold value. Meanwhile, the private key of the group members and the public key of the group can be updated periodically by performing a simple operation aimed at refreshing the group signature message. This periodical refreshed individual signature message can enhance the security of the proposed weighted threshold signature scheme.

Index Terms—Generalized Chinese remainder theorem, proactive weighted threshold signature, RSA cryptosystem, secret sharing.

1. Introduction

Since digital signature techniques are useful in tasks like identifying senders, protecting data integrity, and preventing denial of message ownership, they play an increasingly important role in today's electronic society. The concept of group signatures, which was introduced by Chaum and Heyst[1] in 1991, allows registered members of a predefined group to produce anonymous signatures on behalf of the group. In 1991, Desmedt and Frankel[2] proposed a \((t, n)\) threshold signature scheme. Harn[3] used the cryptographic technique of Shamir’s perfect secret sharing scheme[4], which is based on the Lagrange interpolating polynomial and the modified ElGamal signature[5], to construct a \((t, n)\) threshold signature scheme. In their schemes, at least \(t\) participants in the group can collaborate to generate a valid signature on behalf of the group, but \(t-1\) or fewer participants cannot.

In existing threshold signature schemes[2][3][6][7], each group member receives a copy of message to be signed, signs the message, and sends the message and its signature to a designated clerk. The clerk collects and authenticates each signature and produces a combined group signature. Therefore, in the group signature generating phase, all members play an equal role. There are many real-life examples of the threshold signature scheme. Typical examples include signing a document for a bank and the triggering mechanism for a nuclear weapon. However, we consider here a special kind of generalized threshold scenario that is a natural extension of threshold signature scheme. In the examples mentioned, it is likely that the members are not equal in terms of their privileges or authorities. Consider the example of a message to be signed that authorizes the launch of a nuclear missile. The president can sign the document alone, but some backup mechanisms should be in place in case something happens to him or her. Suppose the Department of Defense wants to implement a policy where the president can sign the document alone, but some backup mechanisms should be in place in case something happens to him or her. Suppose the Department of Defense wants to implement a policy where the president can sign the document alone, but other groups whose combined “weight” equals that of the president can also sign it: for example, two vice-presidents and one general, or one vice-president and three generals, or five generals. In this scenario, general access structures are useful.

In the traditional threshold signature schemes[2][3][6][7], if a shared distribution center (SDC) of a group wants to update the public/private key pair of the group, he needs to redistribute the individual secret keys for group members over a secure channel, and republish his group public key. In the proposed scheme, we developed a novel proactive scheme based on the generalized Chinese remainder theorem (GCRT).

In our proactive weighted threshold signature scheme, some positive weight is associated to each group member and the message can be signed if and only if the sum of the weights of the group members related is greater than or
equal to a fixed threshold. Meanwhile, the shared distribution center of a group can refresh the group’s signature message and the public key periodically by updating a parameter of GCRT.

2. Previous Works

Because of the difficulty of finding efficient threshold signature schemes for general access structures, we sought families of access structures that have other properties useful in the application of threshold cryptography. Multipartite secret sharing schemes [8], [9] are those that have a multipartite access structure in which the set of participants is divided into several parts, and all participants in the same part play an equal role. Several families of multipartite schemes have been proposed, including weighted threshold schemes [10], hierarchical schemes [11],[12], and compartmented schemes [8],[9]. This paper deals with weighted threshold schemes.

In a seminal paper [4], Shamir made the first attempt to propose a construction of weighted threshold secret sharing scheme. In such a scheme, every participant has a weight, and the sets of participants whose weighted sum is greater than or equal to a given threshold are qualified. The proposed construction is very simple: taking a threshold scheme and giving every participant as many shadows as his or her weight. In the case of sharing the document for launching nuclear missiles among the president, vice presidents, and generals, Shamir’s solution is based on a threshold scheme with the threshold value of 5: the president holds five shadows, each vice president holds two shadows, and each general holds one shadow. Asmuth and Bloom [13] proposed a secret sharing scheme based on the Chinese remainder theorem (CRT) and used a special sequence of integers. In 2007, Iftene [14] extended the Asmuth-Bloom threshold scheme to a more general access structure in which the set of participants is partitioned into compartments, some positive weight is associated with each compartment, and the secret can be reconstructed when the sum of the weights of the participants involved is greater than or equal to a fixed threshold.

Kaya and Selčuk [15] proposed several threshold function sharing schemes (FSS) based on the Asmuth-Bloom secret sharing scheme for the RSA, ElGamal and Pailler cryptosystems. In 2007, Iftene and Grindei [16] proposed a weighted threshold signature based on RSA. However, in their scheme, individual signatures cannot be verified, and the group members cannot protect themselves against the cheating of other group members. The authors did not provide a complete description and security analysis of their scheme.

Therefore, we propose an improvement based on Iftene and Grindei’s scheme. A correctness and security analysis has been given to demonstrate the improved scheme. Furthermore, we extended the original scheme [16] to a novel proactive scheme based on GCRT. Portions of the work presented in this paper have previously been presented in Guo and Chang [17]. Compared with [17], we extend the paper a lot and add more technical details.

This paper proposes a \((\alpha, t, n)\) proactive weighted threshold signature scheme based on the work of Iftene [14], Kaya and Selcuk [15], and generalized Chinese remainder theorem. In our scheme, the group members are divided into different subgroups, and all members in the same subgroup play an equal role; a positive weight is associated to each subgroup, and all members in the same subgroup have the same weight. Our scheme allows group members to sign a message simultaneously, and the group signature can be produced if and only if the sum of the weights of members involved is greater than or equal to a fixed threshold. According to the security requirements, our scheme can refresh the signature message by updating the private keys of the group members periodically.

The reminder of this paper is organized as follows. In next section, we briefly review GCRT, Asmuth-Bloom secret sharing, and weighted threshold secret sharing based on the Chinese remainder theorem (CRT). In Section 4, we propose a new proactive weighted threshold signature scheme. Section 5 analyzes the correctness and the security of our scheme. Finally, conclusions are given in Section 6.

3. Preliminary

In this section, we will briefly introduce GCRT, Asmuth-Bloom secret sharing, and weighted threshold secret sharing based on CRT, which are the major building blocks of the proposed scheme.

3.1 Generalized Chinese Remainder Theorem

Before presenting our scheme, we firstly introduce GCRT [18],[19]. In GCRT, an additional integer \(k\) is required during the computations. Similar to CRT, \(n\) positive co-prime integers \(m_1, m_2, \ldots, m_n\) are needed to construct a system with simultaneous congruencies. A number \(Y\) can be represented in \(\{y_1, y_2, \ldots, y_n\}\) that satisfies \(\max\{y_i\}_{1 \leq i \leq n} < k < \min\{m_i\}_{1 \leq i \leq n}\), where \(y_i = [Y/m_j]\mod k\), for \(i = 1, 2, \ldots, n\). According to the GCRT, the number \(Y\) can be computed as follows:

\[
Y = \sum_{i=1}^{n} M_{S(i)} M'_{S(i)} N_i \left( \mod (k \prod_{i=1}^{n} m_i) \right)
\]

where

\[
M_{S(i)} = k \prod_{j=1, i \neq j}^{n} m_j
\]

\[
M'_{S(i)} = (k \mod (km_i))
\]

\[
N_i = \left[ y_i / m_i \right] / k .
\]

3.2 Asmuth-Bloom Secret Sharing

In this subsection, we introduce the Asmuth-Bloom secret sharing scheme [13] which shares a secret among the participants using modular arithmetic and reconstructs it by the Chinese remainder theorem. The detail of the scheme is
as follows:

1. A set of integers \( \{m_0, m_1, \ldots, m_n | m_0 < m_1 < \ldots < m_n\} \) is chosen that is subject to the following:
   a. \( \gcd(m_i, m_j) = 1 \) for \( i \neq j \), where \( \gcd(\cdot) \) is the greatest common divisor.
   b. \( \prod_{i=1}^{n} m_i > \prod_{i=1}^{n} m_{i-1} \).

2. Let \( M \) denote \( \prod_{i=1}^{n} m_i \). We assume that \( x \) is the shared secret, and \( 0 \leq x < m_0 \). The dealer computes \( y = x + am_0 \), where \( a \) is an arbitrary positive integer generated randomly subject to the condition \( 0 \leq y < M \). Then let \( y = y \mod m_j \) be the shadows.

3. Assume \( S \) is a coalition of \( t \) participants gathered to construct the secret. Let \( M_S \) denote \( \prod_{i \in S} m_i \).
   a. Given \( y = y_j \mod m_j \) for \( i \in S \), by CRT, \( y \) is known in \( \mathbb{Z}_{M_S} \).
   b. Compute the secret as \( x = y \mod m_0 \). According to CRT, \( y \) can be determined uniquely in \( \mathbb{Z}_{M_S} \).

### 3.3 Weighted Threshold Secret Sharing Based on CRT

In 2007, Iftene\cite{14} proposed a weighted secret sharing scheme based on CRT. In his scheme, Asmuth-Bloom sequences can be extended. Now we are going to describe how to construct extended Asmuth-Bloom sequences in case of the weighted threshold access structure. Let \( m \geq 2 \), \( \omega = (\omega_1, \omega_2, \ldots, \omega_m) \) be a sequence of weights associated to \( n \) participants, and \( t \) be a global threshold. Let \( S \) denote qualified sets of participants which can recover the secret from their shadows. A \((\omega, t, n)\)-Asmuth-Bloom sequence is a sequence of positive integers \( m_0, m_1, m_2, \ldots, m_n \), such that

\[
\begin{align*}
\max_{S} \sum_{i=1}^{S} \omega_i \cdot \text{lcm}(\{m_j | j \in S\}) < \min_{S} \sum_{i=1}^{S} (\text{lcm}(\{m_j | j \in S\}))
\end{align*}
\]

where \( \text{lcm}(\cdot) \) is least common multiple.

A \((\omega, t, n)\)-Asmuth-Bloom sequence can be constructed as follows. Let \( m_{\omega}, m_{\omega}' \) be a generalized threshold \((t, K)\)-Asmuth-Bloom sequence, where \( K = \sum_{i=1}^{S} \omega_i \) and define \( m_0 = m_{\omega} \) and \( m_i = \text{lcm}(\{m_j | j \in P_i\}) \), for all \( 1 \leq i \leq n \), where \( \{P_1, P_2, \ldots, P_n\} \) is an arbitrary partition of the set \( \{1, 2, \ldots, K\} \), such that \( |P_i| = \omega_i \), for all \( 1 \leq i \leq n \). It is easy to prove that the sequence \( m_0, m_1, m_2, \ldots, m_n \) is indeed a \((\omega, t, n)\)-Asmuth-Bloom sequence. We will prove it in Section 5.

### 4. Proactive \((\omega, t, n)\) Weighted Threshold Signature

The notion of a \((k, n)\) threshold signature scheme has been extensively studied. This section extends the concept of threshold signatures, which we call the weighted threshold signature. Traditional threshold structures may be viewed as a special case of more general access structures.

Group signatures allow a certain number of members of a group to sign messages on behalf of the group, and all members of the group play an equal role. We divide the group into \( m \) subgroups, in such a way that all members in the same subgroup play an equal role, and different subgroups have different weights. The parameters \( \omega_1, \omega_2, \ldots, \omega_m \) refer to the weights related to \( m \) different subgroups, and \( t \) is the global threshold of the scheme. The weights often depend entirely on the significance of the members. A \((k, n)\) threshold signature scheme is simply a \((\omega, t, n)\) weighted threshold signature scheme with \( \omega_1 = \omega_2 = \cdots = \omega_m = 1 \) and \( k = t \).

#### 4.1 Parameter Generation Phase

This scheme utilizes the cryptographic techniques of extended Asmuth-Bloom sequences\cite{15} based on GCRT and the RSA threshold signature scheme\cite{15}. An SDC is responsible for initializing the system and generating the parameters for it.

1) We use \( p_1, p_2, \ldots, p_n \) to denote \( n \) group members and divide the group into \( m \) subgroups, where all members in the same subgroup have the same weight. Let \( P = \{P_1, P_2, \ldots, P_n\} \) be a partition of \( p = \{p_1, p_2, \ldots, p_n\} \), \( 1 \leq m < n \), and consider a sequence \( \mu = (\mu_1, \mu_2, \ldots, \mu_m) \), where \( \mu_1 = |P_1| \) for all \( 1 \leq i \leq m \) and \( |P_i| \) means the number of members of \( P_i \). The weighted threshold access structures are described as

\[
\Gamma = \{S \in P(|1, 2, \ldots, n|) \sum_{i=1}^{m} \omega_i \geq t \}, \text{ where } e_i \text{ is the number of members involved in each subgroup.}
\]

2) Kay and Selçuk\cite{15}, in order to use the sequence securely in their proposed scheme, modified the Asmuth-Bloom sequence as

\[
\prod_{i=1}^{m} m_i > \prod_{i=1}^{n} m_{\nu-i} \cdot \cdot \cdot (1)
\]

According to Iftene’s general secret sharing scheme, a \((\omega, t, n)\)-Asmuth-Bloom sequence \( m_{\omega}^2 \), \( m_1, m_2, \ldots, m_n \) can be constructed from Kay and Selçuk’s modified threshold \((t, Q)\)-Asmuth-Bloom sequence. Let \( m_{\omega}^2, m_1, m_2, \ldots, m_n \) be a \((t, Q)\)-Asmuth-Bloom sequence, and define \( m_0 = m_{\omega}^2 \) and \( m_i = \text{lcm}(\{m_j \mod P_i \}) \), for all \( 1 \leq i \leq n \), where \( Q = \sum_{i=1}^{m} \mu_i \cdot \omega_i \).

3) In the RSA setup, choose two random safe primes \( p \) and \( q \), where \( p = 2p' + 1 \), \( q = 2q' + 1 \), with \( p' \) and \( q' \) themselves large random primes. \( N = pq \) is computed and the public key \( e \) and private key \( d \) are chosen from \( \mathbb{Z}_{\phi(N)} \), where \( ed \equiv 1 (\text{mod} \phi(N)) \). Use \((\omega, t, n)\)-Asmuth-Bloom
secret sharing to share $d$ with

\[ m_0 = \phi(N) = 4p'q'. \]

### 4.2 Individual Signature Generation and Verification

In this subsection, individual signature generation and verification phases are detailed.

1) In the individual signature generation phase, let $M$ be the message to be signed, and assume that a permissible subset $S, S \in \Gamma$, wants to obtain the signature $s = M^d \mod N$. The SDC randomly selects an integer $k$ that satisfies $\max\{y_i, 1 \leq i \leq k\} < k < \min\{y_j, 1 \leq j \leq k\}$. Let $M'_S$ denote $k \prod_{j \in S} m_j$. The SDC computes $y = d + am_b$, where $a$ is a positive integer generated randomly, subject to the condition that $0 \leq y < M'_S$. Given the system $y_i = \lceil y/m_j \rceil \mod k$ for $i \in S$, solve $y \mod \mathbb{Z}_{M'_S}$ using GCRT. Then compute the secret as $d = y \mod m_b$.

We utilize Kaya and Selçuk’s scheme, which is suitable for a threshold signature scheme. Let $M_{S[0]}$ denote $k \prod_{j \in S, \not\in S} m_j$, and $M'_{S,j}$ be the multiplicative inverse of $M_{S[0]}$ in $\mathbb{Z}_{m_j^*}$, that is, $M_{S[0]}M'_{S,j} = k \mod m_j$.

In the individual signature generation phase, each group member $p_i$ generates its individual signature. Each $p_i$ computes $u_i$ as

\[ u_i = M_{S[0]}M'_{S,j}N_i \mod M'_S \]  

(2)

where $N_i = \lceil y/m_j/k \rceil$.

Next, each $p_i$ uses its $u_i$ to generate its individual signature as follows:

\[ s_i = M^u \mod N. \]  

(3)

2) In the individual signature verification phase, we first add the constraint that $q_i = 2m_jk + 1$ is a prime for each $1 \leq i \leq n$. These values are the moduli used to verify the correctness of individual signatures. Let $g_i$ be an element of order $m_i$ in $\mathbb{Z}_{m_i^*}^*$. Each member $p_i$ computes $v_i = g_i^{y_i} \mod q_i$, $1 \leq i \leq n$, as $p_i$’s public key, and broadcasts $g_i$ and $v_i$ to each member. Let $h : \{0,1\} \rightarrow \{0,1,\ldots, 2^l - 1\}$ be a hash function, where $L_i$ is another security parameter ($L_i = 128$). Let

\[ M' = M'_{S[0]} \mod N \]  

(4a)

\[ v'_i = v_{i,j}^{y_i} \mod q_i \]  

(4b)

\[ z_i = y_iM'_{S,j} \mod m_i \]  

(4c)

Each member $p_i$ first computes

\[ W = M^w \mod N \]  

(5a)

\[ U = g_i^z \mod q_i \]  

(5b)

where $r \in \{0,1,\ldots, 2^{(\log_{m_j}2) \cdot l_i}\}$ and $L(m)$ is the bit-length of $m_i$. Then the member computes the proof as

\[ \sigma_i = h(M', g_i, z_i, v'_i, W, U) \]  

and $D_i = r + \sigma_i z_i \in \mathbb{Z}$, and sends the proof $(\sigma_i, D_i)$ along with the partial signature $s_i$ to the designated clerk. After receiving individual signatures, the clerk uses the proof $(\sigma_i, D_i)$ to check the following equation:

\[ \sigma_i = h(M', g_i, z_i, v'_i, M'^{th} s_i^{\omega_i} \mod N, g_i^{\omega_i} v'_i^{\omega_i} \mod q_i) \].  

(6)

If (6) holds, the individual signatures on the message $M$ are valid.

### 4.3 $(\omega, t, n)$ Weighted Threshold Signature Generation and Verification

After individual signatures are verified, the designated clerk computes the weighted threshold signature as follows:

1) Combining the individual signatures. The incomplete signature $\overline{\sigma}$ can be obtained by combining the $s_i$ values:

\[ \overline{\sigma} = \prod_{i \in S} s_i \mod N. \]  

(7)

2) Correction. Let $\lambda = M'^{t} \mod N$ be the corrector. The incomplete signature can be corrected by trying

\[ (\overline{\sigma} \lambda^t)' = \overline{\sigma}(\lambda^t)' = M \mod N. \]  

(8)

Then the signature $s$ is computed by $s = \overline{\sigma} \lambda^t \mod N$, where $\delta$ denotes the value of $t$ that satisfies (8).

3) Verification phase. The verification phase is the same as the standard RSA verification. The verifier checks the following equation:

\[ s^t = M \mod N. \]  

(9)

If (9) holds, the weighted threshold signature $\{M, s\}$ is valid.

### 4.4 Update the Threshold Signature

If the SDC wants to update the private key of the group members and the corresponding generated individual signature message, he can broadcast an additional value $k'$ to all participating group members. And then, the group members can compute their new private keys as follows:

\[ u_i = M_{S[0]}M'_{S,j}N_i \mod M'_S \]  

where $M_{S[0]}M'_{S,j} = k' \mod m_j$ and $N_i = \lceil y/m_j/k' \rceil$.

Their individual signatures can be computed as $s_i = M^u \mod N$.

### 5. Correctness and Security Analysis

Similar to Kaya et al.’s scheme\(^{(15)}\), a general threshold signature scheme based on the RSA cryptosystem is proposed, which utilizes a general secret sharing scheme\(^{(14)}\) based on the Chinese remainder theorem and extended Asmuth-Bloom sequence to achieve the weighted threshold scheme.

**Theorem 1.** The sequence $m_0^2, m_1, m_2, \ldots, m_n$ is a $(\omega, t, n)$ Asmuth-Bloom sequence.

**Proof.** To prove this theorem, we only need to prove the equivalent property:
Because \( m_m^n = \prod_{i=1}^{n} (m_i, m_i'; m_i'' \cdots m_i^q) \) is a \((t, Q)\)-Asmuth-Bloom sequence, the sequences used in the Asmuth-Bloom scheme can be generalized as follows:

\[
m_m^n \max_{\sum_{i=1}^{n} \omega_i = t} \left[ \left( \sum_{i=1}^{n} \omega_i \right) \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \text{lcm} \left( \{ m_i \mid i \in S \} \right) \right] \right] < \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \left( \sum_{i=1}^{n} \omega_i \right) \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \text{lcm} \left( \{ m_i \mid i \in S \} \right) \right] \right].
\]

Thus, we can derive

\[
\min_{\sum_{i=1}^{n} \omega_i = t} \left[ \left( \sum_{i=1}^{n} \omega_i \right) \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \text{lcm} \left( \{ m_i \mid i \in S \} \right) \right] \right] = \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \left( \sum_{i=1}^{n} \omega_i \right) \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \text{lcm} \left( \{ m_i \mid i \in S \} \right) \right] \right] = \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \left( \sum_{i=1}^{n} \omega_i \right) \min_{\sum_{i=1}^{n} \omega_i = t} \left[ \text{lcm} \left( \{ m_i \mid i \in S \} \right) \right] \right]
\]

and

\[
\text{lcm} \left( \{ m_i \mid i \in S \} \right) = \prod_{i \in S} m_i = \prod_{i \in S} m_i'.
\]

Further, \( m_m^n \) can be any integer from \( 0, \ldots, m_m^n \).

Theorem 2. If the sum of the associated weights of members involved is less than the global threshold, the members cannot generate a valid group signature.

Proof. To generate a \((\omega, t, n)\) weighted threshold signature, the sum of associated weights \( \omega_i \) involved has to satisfy

\[
\sum_{i=1}^{n} \omega_i \geq t.
\]

As in the previous section, \( y = d + am_0 \). Let \( y_i = [y / m_i] \bmod k \) be the shadows. To recover \( d \), it suffices to find \( y \). Assume that \( \{ y_1', y_2', \ldots, y_r' \} \) is a qualified set, and if \( y_1', y_2', \ldots, y_r' \) are known, then by the generalized Chinese remainder theorem, \( y \) is a known mod\( \bar{m} = \prod_{i=1}^{r} m_i' \). As \( M' = \bar{M} \) and \( m_m'^2, m_m'^2', \ldots, m_m'^q' \) is a \((t, Q)\)-Asmuth-Bloom sequence that uniquely determines \( y \) and \( d \).

On the other hand, if only \( t-1 \) weighted shadows are known, no information about \( d \) can be recovered. Assume a coalition \( S' \) of weight \( t-1 \) has been gathered, and let \( y' \) be the unique solution for \( y \) in \( \mathbb{Z}_{m_m^n} \) and \( M' = \prod_{i=1}^{t-1} m_i' \). According to (1), \( M / M' > m_m'^2 \), so \( y' \) is smaller than \( M \) for \( j < m_m'^2 \). Since \( \gcd(m_m^n, M') = 1 \) all \( (y' + jM') \bmod m_m^n \) are distinct for \( 0 \leq j < m_m^n \). Hence, \( d \) can be any integer from \( \mathbb{Z}_{m_m^n} \). Therefore, no useful information is available without \( t \) weighted shadows.

Theorem 3. The individual signatures can be verified by the designated clerk.

Proof. From (4), (5), and (6), the values \( M\omega M_s \) and \( g_i^{\omega M} \) can be computed separately as

\[
M\omega M_s = M^{r + \omega n M_j} M^{M_{\omega M_j}} M^{\omega M_{\omega M_j}} = M^{\omega M_{\omega M_j}} \bmod N
\]

and

\[
g_i^{\omega M} = g_i^{r + \omega n M_j} g_i^{M_{\omega M_j}} g_i^{\omega M_{\omega M_j}} = g_i^{r + \omega n M_j} g_i^{\omega M_{\omega M_j}} = g_i^{\omega M_{\omega M_j}} \bmod q_i.
\]

Therefore, the correctness of (6) can be verified, that is, \( s_i \) must be an individual signature on message \( M \).

Theorem 4. If \( s' = M \bmod N \), then the threshold signature \( \{ M, s \} \) of the message \( M \) is valid.

Proof. According to (5) and (6), we can compute the value \( \delta \) as follows:

\[
(\overline{y} \lambda')' = \overline{y} \lambda' = M^{\sum_{i=1}^{n} y_i \bmod q_i} M^{\omega M_{\omega M_j}} = M^{\omega M_{\omega M_j}} \bmod N
\]

From (13), we can derive

\[
\delta = j = \left( \sum_{i=1}^{n} y_i \bmod q_i \right) / M_s.
\]

Then the signature \( s \) can be computed as

\[
s = \overline{s} \lambda' \bmod N = N^{\sum_{i=1}^{n} y_i / M_s} \bmod N = N^{\sum_{i=1}^{n} y_i / M_s} \bmod N = N^{\sum_{i=1}^{n} y_i / M_s} \bmod N.
\]

According to (14), we can conclude \( s' = M \bmod N \).

The security of our proposed scheme is the same as that of Kaya et al.’s scheme [15], which is based on the difficulty of breaking the RSA scheme.

6. Conclusions

This paper proposed a novel proactive \((\omega, t, n)\) weighted threshold signature based on Iftene’s general secret sharing scheme, GCRT, and the RSA threshold signature, which is based on CRT. In our scheme, the group members are divided into different subgroups, and a
positive weight is associated to each subgroup where all members in the same subgroup have the same weight. And
SDC can refresh the private key of the group members, and
members in the same subgroup have the same weight. And
positive weight is associated to each subgroup where all
members in the same subgroup have the same weight. And

References

Advances in Cryptology-EUROCRYPT 1991, Brighton,
authenticators and signatures,” in Proc. of Advances in
scheme and digital multisignature,” IEE Proc.-Computer
digital signature scheme based on discrete exponentiation,”
Advances in Cryptology-EUROCRYPT 2000, Bruges, 2000,
pp. 207–220.
untraceable signature for group communications,” IEE
[8] S. L. Ng, “Ideal secret sharing schemes with multipartite
access structures,” IEE Proc.-Communications, vol. 153,
secret sharing schemes,” in Proc. of Advances in Cryptology
weighted threshold secret sharing,” in Proc. of Advances in Cryptology-
signatures,” in Proc. of the 32nd Int. Colloquium on
446–458.
remainder theorem with applications in e-voting,”
Electronic Notes in Theoretical Computer Science, vol. 186,
[15] K. Kaya and A. A. Selçuk, “Robust threshold schemes based
on the Chinese remainder theorem,” in Proc. of Advances in
Cryptography-AFRICACRYPT 2008, Casablanca, Morocco,
on the Chinese remainder theorem,” in Proc. of the 9th Int.
Symposium on Symbolic and Numeric Algorithms for
on the Chinese remainder theorem,” in Proc. of the 7th Int.
Conf. on Intelligent Information Hiding and Multimedia
[18] Y.-P. Lai and C.-C. Chang, “Parallel computational
algorithms for generalized Chinese remainder theorem,”
Computers and Electrical Engineering, vol. 29, no.8,
group-oriented cryptoscheme without trusted centers,” IEEE
Journal on Selected Areas in Communications, vol. 11, no. 5,

Cheng Guo was born in Liaoning Province, China in 1980. He received the B.S. degree in computer science from Xi’an University of Architecture and Technology in 2002. He received the M.S. and Ph.D. degrees in computer application and technology and from the Dalian University of Technology, Dalian in 2006 and 2009, respectively. Now he works as a postdoctor with the National Tsing Hua University, Hsinchu. His current research interests include information security and cryptography.

Chin-Chen Chang received his B.S. degree in applied mathematics in 1977 and the M.S. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu. He received his Ph.D. degree in computer engineering in 1982 from the National Chiao Tung University, Hsinchu. During the academic years of 1980 to 1983, he was with the Department of Computer Engineering at the National Chiao Tung University. From 1983 to 1989, he was with the Institute of Applied Mathematics, National Chung Hsing University Taichung. From August 1989 to July 1992, he was a professor and the Head of the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi. From August 1992 to July 1995, he was the Dean of the College of Engineering at the same university. From August 1995 to October 1997, he was the Provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From 2002 to 2005, he was a chair professor with National Chung Cheng University. Since February 2005, he has been a chair professor with Feng Chia University, Taichung. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, computer cryptography, image compression, and data structures.