IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 1, 2021, accepted June 29, 2021, date of publication July 5, 2021, date of current version July 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3094902

Secure Threshold Ring Signature Based on SM9

SHUANGGEN LIU, KANG CHEN, ZIKANG LIU, AND TENG WANG
School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Corresponding author: Teng Wang (wangteng@xupt.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61872058, and in part by the Key Research and Development Program of Shaanxi under Grant 2021NY-211.

ABSTRACT Nowadays, it becomes a major issue that has become increasingly prominent to ensure the privacy and security of information. With the wide application of SM9 algorithm in various fields, it is particularly important to improve the security of SM9 algorithm. Therefore, many researchers use the SM9 algorithm for supporting the underlying cryptography. And group signature, ring signature and two-party signature are introduced in succession to design the related scheme with significant effecting. In order to further improve the signature security and promote the promotion of SM9 algorithm. First, the SM9 identification and cipher algorithm is improved by using multi-KGC(Key Generation Center) to generate system parameters to achieve the purpose of improving the security of the key in this paper. Second, a threshold ring signature scheme based on SM9 is proposed by combining SM9 with threshold ring signature. The analysis shows that, compared with the existing schemes, the proposed scheme has more advantages in security, such as higher anonymity, unforgeability and non-repudiation, while resisting malicious user attacks and malicious KGC attacks. This scheme extends SM9 from single user signature to multi-users signature, and increases the application scenarios of SM9, which plays a positive role in the promotion of SM9.

INDEX TERMS Digital signatures, provably safe, random oracle model, SM9 identity-based cryptography, threshold ring signature.

I. INTRODUCTION

In 2002, Bresson *et al.* [1] have proposed the concept of threshold ring signature. Threshold ring signature is a group-oriented signature. If there are t members in a group who want to leak a message, they not only need to convince the recipient of the signature that at least t members of the group participated, but also make the recipient unable to determine which members participated in the leak of the message, at the same time achieve the purpose of hiding the identity of the members participating in the signature. In this case, threshold ring signatures will play important roles. The members participating in the signature all own a part of the key individually. If the attacker wants to obtain the complete key, he needs to hack all participating signers. This approach is difficult, so the security of the key is effectively guaranteed. Threshold ring signature has the characteristics of decentralized power and risk sharing, so the threshold ring signature scheme has been widely researched and discussed [2]–[4]. In order to satisfy different application requirements, researchers have proposed threshold ring signatures with different properties, such as solving the problem of attribute key escrow [5], implementing blockchain technology [6], and code-based threshold ring signature [7].

The Identity-Based Cryptography (IBC) theory [8] has been firstly proposed by Shamir (one of the inventors of the RSA algorithm) in 1984. The IBC algorithm is based on the theory of elliptic curve bilinear pairing and uses user identification (such as phone number, email address, ID card, unit name, etc.) as public keys. A cryptographic technology integrated with IBC can directly bind user identity with asymmetric key pair, which simplifies the process of certificate distribution and public key exchange in PKI/CA applications, and reduces the complexity of key and certificate management. Shamir has been used the existing RSA algorithm to propose an identity-based digital signature scheme. Ohgishi and Kasahara [9] published an identity-based key sharing scheme proposed using elliptic curve pairs in 2000. The following year, Boneh and Franklin [10] proposed an identity-based public key cryptographic algorithm based

The associate editor coordinating the review of this manuscript and approving it for publication was Gautam Srivastava.

on the bilinear Diffie-Hellman difficult problem. The IBC system has gradually been pushed to a new level of research. After that, the United States, the United Kingdom, and Japan began to design corresponding algorithms. The State Cryptography Administration of China formally has promulgated the commercial identification cryptographic algorithm model SM9 in 2008 [11], issued and implemented the SM9 identification cryptographic algorithm standard on March 28, 2016 [12]. It has been incorporated into the international standard in November 2018 [13]. The application of identification cryptographic algorithms is developing rapidly.

SM9 has been used and developed more and more widely in various fields by virtue of its simplicity and low consumption. On the one hand, the SM9 algorithm itself is an identification-based password algorithm, so it inherits all the characteristics of traditional identification passwords. It is widely used in secure email systems [14]–[16], blockchain [17], [18], Internet of Vehicles [19], Internet of Things equipment [20] and other fields. On the other hand, many scholars are paying attention to the optimization of SM9. Through the Miller loop [21], large number multiplication in the multi-core processor [22], and R-ate [24] optimization, the cost of calculation process is reduced and the algorithm performance is improved.

Furthermore, directly using the SM9 algorithm as the underlying cryptographic support of its own application to construct research schemes has also become a current research hotspot. In 2018, Zhang and Peng [25] proposed a blind signature scheme based on SM9 algorithm to realize the concealment protection of signed message data. In 2019, Shi *et al.* [26] used SM9 as the underlying encryption and decryption technology to propose an attribute-based encryption scheme, and realize more flexible and fine-grained access control to sensitive data. In the same year, in order to solve the privacy leakage problem in the blockchain transaction process, Yang *et al.* [27] proposed a group signature scheme based on the SM9 algorithm. Then, in 2020, He *et al.* [28] proposed a ring signature scheme based on SM9 to improve the privacy protection of signed users. But the above schemes are only applicable to single-user signature scenarios. Still in 2020, Mu *et al.* [29] combined SM9 with two-party signatures and proposed a secure two-party SM9 signature scheme. This scheme improves the security of signatures, and is suitable for dual-user signature scenarios with $t = 2$, $n = 2$. However, it is not applicable to scenarios that require multi-user signatures, such as electronic voting.

Nowadays, when faced with massive amounts of information, the seriousness of network security problems is self-evident. Once a network security problem occurs, it will cause serious economic losses and cause great harm to the development and progress of various businesses under the network background. Thus, in the current information age, ensuring the privacy and security of information has become an increasingly prominent issue. With the wide application of SM9 in various fields, its security issues have received close attention. The security of SM9 is based on the premise of the security of the private key. Once the private key is leaked, the system will face greater security risks. At the same time, anonymity is also an important attribute in cryptography applications. In practical applications, such as electronic cash and electronic elections, it is necessary to ensure that the signer's information will not be leaked. Therefore, while realizing the promotion of SM9, improving safety becomes particularly important.

This paper involves the construction of a multi-KGC(Key Generation Center) threshold ring signature scheme based on identity authentication. Our main contributes are as follows:

1) In this paper, a multi-KGC system is adopted to improve the SM9 identification cipher algorithm. The function of the single KGC is allocated to multi-KGC, and multi-KGC participates in parameter maintenance and key generation together. While rationally configuring resources, it avoids the over-concentration of functions of a single KGC, thereby improving the security of the key.
2) The SM9 standard algorithm is only suitable for single-user signature scenarios, and the SM9 scheme proposed at this stage is suitable for dual-user signature scenarios, and there is a problem that it cannot be satisfied with multi-user signature scenarios. In this paper, SM9 is combined with (t, n) threshold ring signature. The proposed multi-KGC threshold ring signature scheme can be applied to multi-user signature scenarios, thereby increasing the application scenarios of SM9 and promoting the popularization of SM9.
3) Through the security proof and the performance analysis, the proposed scheme not only improves the efficiency of signatures while guaranteeing general signature security, but also resists malicious KGC and user attacks. Thus, the proposed scheme has significant security advantages.

The rest of this paper is organized as follows. We present the preliminaries in Section II. Section III describes the algorithm model. We propose a threshold ring signature scheme based on the SM9 algorithm in Section IV. In Section V, the correctness and safety analysis for our scheme is carried out. Section VI discusses the performance comparison results. Finally, Section VII concludes this paper.

II. PRELIMINARIES

In this section, we briefly review bilinear pairs and their corresponding properties. We also define some symbols and review the algorithms that constitute threshold ring signature schemes. Then a security experiment of the existence of unforgeability of a threshold ring signature scheme is given.

A. NOTATIONS

Table 1 lists the commonly used notations in this paper.

TABLE 1. Notations and their meaning.

Notations	Meaning
p	prime order in the group
P_1	generator for G_1 group
P_2	generator for G_2 group
m	a message
M	simulator
A	adversary
H_i	hash function
ID_i	user's identity
D_{ID_i}	user's signature private key
K_i	user's signature public key
I	the actual signers in the threshold ring
$\bar{I}$	non-participating signers in the threshold ring
H_i	hash function
s_i	a random integer
c_i	a random integer
k	the number of KGCs in the multi-KGC system
ks	a master private key in SM9
ke_j	a master private key in our scheme
P_{pub-s}	a master public key in SM9
P_{pub-e}	a master public key in our scheme
f	a polynomial equation with degree $n-t$
q_H	number of Hash inquiry
q_E	number of Extract inquiry
$GF(p)$	finite field
$x\|\|y$	the splicing of x and y
$\lceil x \rceil$	top function, the smallest integer not less than x
$\lfloor x \rfloor$	base function, the largest integer not greater than x

B. BILINEAR PAIRINGS

We denote G_1 and G_2 as two cyclic additive groups with prime order p. G_T is a cyclic multiplicative group, whose order is also p. Correspondingly, a bilinear pairing is denoted as a map $e : G_1 \times G_2 \rightarrow G_T$ which satisfies the following properties [30].

- *Bilinear*: $\forall P \in G_1, \forall Q \in G_2$ and $x, y \in Z_P^*$, $e(xP, yQ) = e(P, Q)^{xy}$.
- *Non-degenerate*: $\exists P_1 \in G_1$, $Q_1 \in G_2$, such that $e(P_1, Q_1) \neq 1$.
- *Computable*: $\forall P_1 \in G_1$, $Q_1 \in G_2$, $e(P_1, Q_1)$ can be efficiently computed.

From the above properties, we can conclude that $\forall P \in G_1$, $Q_1, Q_2 \in G_2$, $e(P, Q_1Q_2) = e(P, Q_1) \cdot e(P, Q_2)$ and $\forall P \in G_1$, $Q \in G_2$, $e(P, Q) = e(Q, P)$.

We note that the Weil and Tate pairings associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear maps. Suppose that G is an additive group. Now we describe four mathematical problems.

Definition 1 (Discrete Logarithm Problem (DLP)): Given two group elements P and Q, find an integer n, such that $Q = nP$ whenever such an integer exists.

Definition 2 (Discrete Logarithm Problem on a finite field (DLP)): Given a finite field F_q and an element $g, h \in F_q$, find an integer d such that $g^d = h$ in F_q.

Definition 3 (Elliptic Curve Discrete Logarithm Problem (ECDLP)): Given the elliptic curve E defined on the finite field F_q, and two points $P, Q \in E(F_q)$ on E, find an integer d such that $dP = Q$ in E.

Definition 4 (Bilinear Pair Inversion Problem(BPIP)): Given $P \in G_1$, and $e(P, Q) \in G_1$, find $Q \in G_1$.

C. FRAMEWORK OF ID-BASED THRESHOLD RING SIGNATURE

An ID-based threshold ring signature scheme consists of four procedures: Setup, KeyGen, Sign, and Verify [31].

– *Setup*: KGC runs a probabilistic polynomial time algorithm (PPT), it produces the master secret key *ke* and the common public parameters params, which include a description of a finite signature space and a description of afinite message space.

– *KeyGen*: Given an input of signer's identity $ID \in \{0, 1\}^*$ and the master secret *ke*, it outputs the signer's secret signing key D_{ID}.

– *Sign*: Given input of a message *m*, a group of *n* users' identities ID_i, where $1 \leq i \leq n$, and the secret keys of *t* members D_{ID_i}, where $1 \leq i \leq n$. it outputs a (t, n) ID-based threshold ring signature on the message *m*.

– *Verify*: Given a threshold ring signature σ, a message *m*, the threshold value *t* and the group of signers' identities ID_i where $1 \leq i \leq n$ as the input, it outputs *True* or *False*, depending on whether σ is a valid signature signed by at least *t* members in the group ID_i on a message *m*.

These algorithms must satisfy the standard consistency constraint of ID-based threshold ring signature schemes, i.e. if we have $\sigma = Sign(m, ID_i, D_{ID_i})$ and $|D_{ID_i}| = t$ (where $|D_{ID_i}|$ denotes the number of elements in the set D_{ID_i}), we must have Verify$(\sigma, ID_i, m, t) = True$.

D. FORMAL DEFINITION AND SECURITY MODEL

In order to ensure the security of the threshold ring signature, a threshold ring signature scheme must meet the following conditions:

Definition 5 (Correctness): Let message *m*, if *t* signers generate signature σ according to the correct signature step, and the data is not modified during the transmission process, then σ can be verified by the verification step.

Definition 6 (Unforgeability): If adversary *A* does not know the private keys of at least *t* members, he cannot forge a valid (t, n) threshold ring signature. This can be formally defined by the following game:

The identity-based threshold ring signature scheme is unforgeable. If there is no attacker *A*, he can win the following games with a non-negligible advantage in polynomial time [32].

1) *System establishment*: Selects the identities of *n* users, denoted as $U = \{ID_1, ID_2, \cdots, ID_n\}$. Assume that attacker *A* has breached the $t-1$ members set Ψ, and the remaining unattended users form a set T. Simulator *M* runs the initialization algorithm to generate system public parameters and secret parameters. Then public parameters and secret parameters of members in set Ψ are sent to *A*.
2) *Prediction simulation stage*: *A* can adaptively perform polynomial Hash inquiry, Extract inquiry, and

TABLE 2. SM9 digital signature system parameters.

Notations	Meaning
cid	curve identifier
F_q	elliptic curve base field
a	elliptic curve equation parameters
b	elliptic curve equation parameters
β	twisted line parameter
N	prime factor of curve order
cf	the cofactor cf relative to N
β	twisted line parameter
N	prime factor of curve order
G_1	N-th order cyclic subgroup
G_2	N-th order cyclic subgroup
G_T	N-th factorial cyclic group
eid	the identifier of the bilinear pair e
φ	the homomorphic map from G_2 to G_1

Signature inquiry. M sends the corresponding simulation results to A.

- Hash inquiry: A requests any input hash value for-m M.
- Extract inquiry: A selects an identity ID_i, M calculates Extract D_{ID_i}, and sends D_{ID_i} to A.
- Signature inquiry: A selects a group of n members ID_i, $1 < i < n$, threshold $t < n$, message m. M calculates the identity-based (t, n) threshold ring signature σ'.

3) *Forgery stage*: At the end of the game, A outputs the signature σ' of the message m. If the following conditions are met, A wins the game:
   - Verify $(S_1', S_2', S_3', \cdots, f') = True$.
   - m does not appear in the ring signature query.
   - As a forgery signer $ID^* \in U$.

Definition 7 (Anonymity): In a threshold ring signature scheme, t signers generate a signature σ through the signature algorithm. For any adversary, it is impossible to know which t signers generated the signature through the signature σ.

III. ALGORITHM DESCRIPTION

A. SM9 SYSTEM PARAMETERS KEY PAIR GENERATION

Table 2 lists the system parameter groups of SM9 digital signature [11], [12].

1) The KGC chooses a random $ks \in [1, N-1]$ as the master private key and computes an element $P_{pub-s} = ks \cdot P_2$ of group G_2 as the master public key.
2) The KGC chooses and publicizes the identifier hid for the signing private key generation function denoted by one byte.
3) The KGC computes $t_1 = H_1(ID_A||hid, N) + ks$ in the finite field F_N. If $t_1 = 0$, then it reselects the master private key, computes and publicizes the master public key, and updates all registered users' signing private keys. Else, it computes $t_2 = ks \cdot t_1^{-1}$ mod N, then, computes $d_{sA} = [t_2]P_1$.

B. SM9 DIGITAL SIGNATURE GENERATION ALGORITHM

Assume that the message to be signed is a bit string m, in order to obtain the digital signature (h, S) of message m, user A as the signer should implement the following steps:

Algorithm 1 SM9 Digital Signature Generation Algorithm

```
Input: SM9 system parameters, message $m$
Output: signature $(h, S)$
 1: Compute $g = e(P_1, P_{pub-s})$ in $G_T$
 2: Generate a random number $r \in [1, N-1]$
 3: Compute $w = g^r$ int $G_T$ and convert the data type of $w$ to bit stream
 4: Compute $h = H_2(m||w, N)$
 5: $l = (r - h)$ $mod$ $N$
 6: if $l = 0$ then
 7:     goto (2)
 8: else
 9:     Compute $S = [l]d_{sA}$ in $G_1$
10:     Convert the data type of $h$ and $S$ to byte stream
11: end if
12: return Signature $(h, S)$ of message $m$
13: end
```

C. SM9 DIGITAL SIGNATURE VERIFICATION ALGORITHM

In order to verify received message m' and signature (h', S'), user B should implement the following steps as the verifier:

Algorithm 2 SM9 Digital Signature Verification Algorithm

```
Input: signature $(h', S')$, message $m'$
Output: "$True$" or "$False$"
 1: Check whether $h' \in [1, N-1]$ is established, if not, the verification fails
 2: Convert the data type of $S'$ to a point on the elliptic curve, and check whether $S' \in G_1$ is established, if not, the verification fails
 3: Compute $g = e(P_1, P_{pub-s})$ in $G_T$
 4: Compute $t = g^{h'}$ in $G_T$
 5: Compute $h_1 = H_1(ID_A||hid, N)$
 6: Compute $P = [h_1]P_2 + P_{pub-s}$ in $G_2$
 7: Compute $u = e(S', P)$ in $G_T$
 8: Compute $w' = u \cdot t$ in $G_T$, convert the data type of $w'$ to a bit string
 9: Compute $h_2 = H_2(m'||w', N)$, check whether $h_2 = h'$ is established, if yes, the verification is passed. Otherwise, the verification fails
10: end
```

D. BILINEAR THRESHOLD RING SIGNATURE SYSTEM PARAMETERS

Let P_1 and P_2 be the generators of G_1 and G_2, for each user i, $1 \leq i \leq n$, a random element $x_i \in_R Z_P$ is picked as the user's private key and the user's public key is computed as $K_i = P_2^{x_i}$. To generate a (t, n) threshold ring signature, let $L = \{K_1, \cdots, K_n\}$ be the set of n public keys. Let $I \subseteq \{1, \cdots, n\}$, $|I| = t$, be the set of indices of t actual signers. Let $\bar{I} = \{1, \cdots, n\} \backslash I$. Let $H : \{0, 1\}^* \rightarrow Z_P$ be a hash function. For security analysis, H is viewed as a random oracle [31].

E. BILINEAR THRESHOLD RING SIGNATURE GENERATION ALGORITHM

The signature generation is proceeded as follows.

Algorithm 3 Bilinear Threshold Ring Generation Algorithm

```
Input: system parameters, message $m$, threshold $t$
Output: signature $\sigma = (S_1, \cdots, S_n, f)$
For each $i \in \bar{I}$, randomly generate $s_i, c_i \in_R Z_P$, compute $z_i = e(P_1^{s_i}, P_2) \cdot e(P_1^{c_i}, K_i)$
For each $i \in I$, compute $z_i = e(P_1^{r_i}, P_2)$, where $r_i \in_R Z_P$
$c_0 \leftarrow H(L, t, m, z_1, \cdots, z_n)$
For $i \in \bar{I}$, find a polynomial $f$ of degree $n - t$ such that $f(i) = c_i$ and $f(0) = c_0$
For each $i \in I$, set $c_i = f(i)$ and compute $S_i = r_i - c_i x_i \ mod\ p$
return Signature $\sigma = (S_1, \cdots, S_n, f)$
end
```

F. BILINEAR THRESHOLD RING SIGNATURE VERIFICATION ALGORITHM

The signature $\sigma = (S_1, \cdots, S_n, f)$ is valid if

$$f(0) = H(L, t, m, e(P_1^{S_1}, P_2) \cdot e(P_1^{f(1)}, K_1), \cdots, e(P_1^{S_n}, P_2) \cdot e(P_1^{f(n)}, K_n)) \tag{1}$$

IV. THRESHOLD RING SIGNATURE SCHEME BASED ON SM9

A. MULTIPLE KGC SYSTEM

We use the same set of notations as in *Sec.II* and *Sec.III*.

Compared with the signature verification algorithm of the SM9 standard, considering that there are t users participating in the signature and the functional requirements of KGC in the threshold ring signature. We propose to use the multi-KGC mode to improve the parameter generation steps of the standard SM9 signature algorithm. The function of single KGC is allocated to multi-KGC, and multi-KGC participate in parameter maintenance and key generation together. While rationally configuring resources, it avoids the over-concentration of functions of a single KGC, thus protecting the user's private key.

Suppose there are k KGCs, all KGCs jointly agree that the random number $ks \in [1, n-1]$, each holding another random number $ke_j \in [1, n-1]$, where j represents the j-th KGC. Each KGC calculates the elements $P_{pub-s} = [ks]P_2$ and $P_{pub-j} = [ke_j]P_2$ in G_2, and calculates sequentially $P_{pub-e} = \Sigma_{j=1}^{k} P_{pub-j}$, until $j = k$, site $P_{pub-e} = [\Sigma_{j=1}^{k} ke_j]P_2$. Then the signature master key pair is$(ke, P_{pub-s}, P_{pub-e})$, each KGC secretly keeps ks and its own ke, and discloses P_{pub-s} and P_{pub-e}.

In this system, KGC compute $t_1 = H_1(ID_i||hid, N) + ks$, if $t_1 \neq 0$, then, compute $t_j = ke_j \cdot t_1^{-1}\ mod\ N$, and set $D_{ID_i} = [\Sigma_{j=1}^{k} t_j]P_1$ as the private key. The user's public key is updated to $K_i = P_2^{D_{ID_i}}$.

B. SIGNATURE GENERATION ALGORITHM

The signature generation is proceeded as follows.

Algorithm 4 Algorithm Generation of Threshold Ring Signature Scheme Based on SM9

```
Input: system parameters, message $m$, threshold $t$
Output: signature $\sigma = (S_1, \cdots, S_n, f)$
For each $i \in \bar{I}$, randomly generate $s_i, c_i \in_R Z_P$, compute $g_1 = e(P_1, P_{pub-e})$, $w_1 = g_1^{s_i}$, $w_2 = g_1^{c_i D_{ID_i}}$, computer $z_i = w_1 \cdot w_2$
For each $i \in I$, randomly generate $r_i \in_R Z_p$, compute $g_1 = e(P_1, P_{pub-e})$, $z_i = g_1^{r_i}$
Convert the data type of $z_i$ to a bit string according to the details given by *Algorithm 6* and *Algorithm 7*
Compute $c_0 \leftarrow H(L||t||m||z_1|| \cdots ||z_n, N)$
For $i \in \bar{I}$, find a polynomial $f$ of degree $n - t$ such that $f(i) = c_i$ and $f(0) = c_0$. The $f$ has the form $f_i(x) = c_0 + c_1 x + \cdots + c_i x^{n-t}$
For each $i \in I$, set $c_i = f(i)$ and compute $S_i = (r_i - c_i)D_{ID_i}$
return Signature $\sigma = (S_1, \cdots, S_n, f)$
end
```

C. SIGNATURE VERIFICATION ALGORITHM

The signature verification process is shown as follows.

Algorithm 5 Algorithm Verification of Threshold Ring Signature Scheme Based on SM9

```
Input: signature $\sigma = (S'_1, \cdots, S'_n, f')$, message $m'$, threshold $t$
Output: "*True*" or "*False*"
Check whether the polynomial $f$ degree is $n - t$ degree, if not, the verification fails
Check whether $f(0)$ is a constant term, if not, the verification fails
Compute $g = e(P_1, P_{pub-e})$
Compute $t_i = g^{f'(i)}$
Compute $h_i = H_1(ID_i||hid, N)$
Compute $P_i = [h_i]P_2 + P_{pub-s}$
Compute $u_i = e(S'_i, P_i)$
Compute $w'_i = u_i \cdot t_i$, then, convert the data type of $w'_i$ to a bit string according to the details given by *Algorithm 6* and *Algorithm 7*
Compute $h = H(L||t||m'||w'_0|| \cdots ||w'_i, N)$
If $h = f'(0)$, then, the verification is passed
end
```

D. DATA TYPE CONVERSION

The signature generation is proceeded as follows.

Algorithm 6 Conversion of Field Elements to Byte Strings

```
Input: Element $a = (a_{m-1}, a_{m-2}, \ldots, a_1, a_o)$ in $F_{q^m}(m \geq 1)$, $q = p$
Output: The byte string $S$ of length $l$, where
```

$$l = \lceil \log_2^{q/8} \rceil * m \tag{2}$$

```
If $m = 1$, then $a = a_0 (q = p)$, $a$ must be an integer in the interval $[0, q-1]$, according to the details of $Algorithm\ 8$, convert a into a byte string $S$ of length $l$
If $m > 1$, then $a = (a_{m-1}, a_{m-2}, \cdots, a_1, a_o)$ $(q = p)$, where $a_i \in F_q$, $i = 0, 1, \cdots, m-1$
    1) Set $r = \lceil \log_2^{q/8} \rceil$
    2) Perform $i$ from $m-1$ to 0: According to the details of $Algorithm\ 8$, convert $a_i (q = p)$ into a byte string $s_i$ of length $r$
    3) $S = s_{m-1}||s_{m-2}||\cdots||s_0$
end
```

Algorithm 7 Byte String to Bit String Conversion

```
Input: Byte string $M$ of length $l$
Output: Bit string $s$ of length $n$, where $n = 8l$
Let $M_{l-1}, M_{l-2}, \cdots, M_0$ be the byte from the leftmost to the rightmost of $M$
Let $s_{n-1}, s_{n-2}, \cdots, s_0$ be the bit from the leftmost to the rightmost bit of $s$, then $s_i$ is $M_j$, and the $i - 8j + 1$th bit from the right, where $j = \lfloor i/8 \rfloor$
end
```

Algorithm 8 Integer to Byte String Conversion

```
Input: Non-negative integer $x$, and the target length of the byte string $l$ (where $l$ satisfies $2^{8l} > x$)
Output: The byte string $M$ of length $l$
Let $M_{l-1}, M_{l-2}, \cdots, M_0$ be the leftmost to rightmost byte of $M$
The bytes of $M$ satisfy:
    $$x = \Sigma_{i=0}^{l-1} 2^{8i} M_i \qquad (3)$$
end
```

V. SCHEME CORRECTNESS AND SAFETY PROOF

A. CORRECTNESS

Theorem 1: The algorithm scheme is provably safe.

Proof: For the signature algorithm, in the signature verification stage, it is necessary to verify whether h and $f'(0)$ are equal, because $h = H(L||t||m'||w'_0||\cdots||w'_i, N)$, $f'(0) = H(L||t||m||z_1||\cdots||z_n, N)$, verifying that two are equal is equivalent to verifying that z and w' are equal.

Because $u_i = e(S'_i, P_i)$

$$\begin{aligned} u_i &= e([r_i - c_i]D_{ID_i}, [h_i]P_2 + P_{pub-s}) \\ &= e([r_i - c_i][\Sigma_{j=1}^{k} t_j]P_1, [h_i]P_2 + [ks]P_2) \\ &= e(P_1, P_2)^{(r_i - c_i)[\Sigma_{j=1}^{k} t_j](h_i + ks)} \\ &= e(P_1, P_2)^{(r_i - c_i)[\Sigma_{j=1}^{k} ke_j](h_i + ks)} \end{aligned} \tag{4}$$

Also because $t_i = g^{f'(i)}$

$$\begin{aligned} t_i &= e(P_1, P_{pub-e})^{c_i} \\ &= e(P_1, P_2)^{c_i[\Sigma_{j=1}^{k} ke_j]} \end{aligned} \tag{5}$$

Then $w' = u_i \cdot t_i$

$$\begin{aligned} w' &= e(P_1, P_2)^{(r_i - c_i)[\Sigma_{j=1}^{k} ke_j]} \cdot e(P_1, P_2)^{c_i[\Sigma_{j=1}^{k} ke_j]} \\ &= e(P_1, P_2)^{r_i[\Sigma_{j=1}^{k} ke_j]} \\ &= e(P_1, P_{pub-e})^{r_i} \\ &= z \end{aligned} \tag{6}$$

So the verification is passed and the correctness of the signature algorithm has been proven. ■

B. UNFORGEABILITY

Theorem 2: The algorithm scheme can resist key attacks.

Proof: The so-called key security refers to deriving the private key D_{ID_i} of the signer U_i through given public information, which is computationally infeasible. Since the private keys of all signers are calculated by multi-KGC, if you want to calculate the corresponding private key from public information, you must know the private key D_{ID_A} and the identity ID_A. Using $t_1 = H_1(ID_A||hid, N) + ks$, $t_j = ke_j \cdot t_1^{-1}$, $D_{ID_A} = [\Sigma_{j=1}^{k} t_j]P_1$ can calculate the private key. But since calculating $[\Sigma_{j=1}^{k} t_j]$ in D_{ID_A} is a DLP problem, so $[\Sigma_{j=1}^{k} t_j]$ is protected. In addition, if the attacker wants to obtain the signer's private key through the threshold ring signature result, he not only breaks through the singleness of the hash function but also faces the $BPIP$ problem. At the same time, suppose the adversary forges the key pair of the signer U_i and uses the key pair to sign. After receiving the signature, user U_A needs to verify whether h and $f'(0)$ are equal. Because the adversary cannot obtain the system master keys ks and ke_j, the probability of $h = f'(0)$ is extremely small, and the probability of passing verification is extremely small, so the adversary cannot forge the key pair of the signer U_i. Therefore, the key security of the scheme is satisfactory. ■

Theorem 3: This threshold ring signature scheme satisfies the requirement of unforgeability.

Proof: Under the random oracle model, if the attacker A can break the scheme in polynomial time with a non-negligible advantage δ, there is algorithm C, which can solve the difficult DLP problem in polynomial time with a non-negligible advantage δ, where

$$\delta = \frac{1}{q_H} \tag{7}$$

System establishment: Assuming that attacker A has compromised the private keys of $t - 1$ users, without loss of generality, these compromised users form a set $\Psi = \{ID_1, ID_2, \cdots, ID_{t-1}\}$, and the rest are not compromised users form a set $T = \{ID_t, ID_{t+1}, \cdots, ID_n\}$. Therefore, attacker A only needs to break any member ID_i in the set T, and he can successfully forges the legal signature of any message.

Prediction simulation stage: Assume that attacker A can perform random prediction simulation, key analysis prediction simulation, and signature prediction simulation respectively. The attacker A constructs a PPT algorithm that can solve the DLP problem with a non-negligible probability. Given $(G_2, P_2, p, \hat{K})$, the simulator M outputs $\hat{D}_{ID_i}$, so that the probability of $P_2^{\hat{D}_{ID_i}} = \hat{K}$ with non-negligible.

1) *Hash query*: When A requests the hash value of $H(L||t||m||z_1||\cdots||z_n, N)$ from M, M checks the request-response list L_1, and if the request is in L_1, it sends the corresponding response to A. Otherwise, M randomly generate a value and send it to A, and then store the request-response in the list L_1.
2) *Extract query*: A gives an identity ID_i $(1 < i < q_E)$, M random selection $x_1, \cdots, x_n \in_R Z_P$, set $t_j = x_j \cdot (H_1(ID_i||hid, N) + x_i)^{-1}$, $D_{ID_i} = \Sigma_{j=1}^{k}[t_j]P_1$. M set $K_i = P_2^{D_{ID_i}}$ and sends it to A. There is only one request exception, so let's set the request as ID^*.
3) *Signature query*: A selects the identities of n users, denoted as $U = \{ID_1, ID_2, \cdots, ID_n\}$, the threshold $t \leq n$, and the message m. Then A specifies a public key set $L' = \{K_1, K_2, \cdots, K_{n'}\}$, set $I' = \{i_1, \cdots, i_{t'}\}$ containing t indexes. M assigns (x_i, K_i) numbered $i \in [1, t]$ to these t indexes (where M does not know the corresponding private key (x_i, K_i)), and use $[t, n]$ to represent other indexes. For the other n-t indexes, M generates a public-private key pair according to the algorithm, and returns the corresponding public key after the j-th query. A requests (m, L', t) identity-based (t, n) threshold ring signature from M.

Forgery stage: the identity-based (t, n) threshold ring signature of M performs the following steps to generate the signature σ'.

1) Randomly generate $c_0, c_i \in_R Z_P$, for $i \notin I'$.
2) Construct f over $GF(p)$ such that $deg(f) = n' - t'$ and $f(0) = c_0, f(i) = c_i$, for $i \notin I'$.
3) For $i \in I'$, compute $c_i = f(i)$.
4) For $i = 1, \cdots, n'$ randomly generate $s_i \in_R Z_P$ and compute $g_1 = e(P_1, P_{pub-e})$, $w_1 = g_1^{s_i}$, $w_2 = g_1^{c_i D_{ID_i}}$, computer $z_i = w_1 \cdot w_2$.
5) Assign c_0 as the value of $H(L'||t||m||z_1||\cdots||z_{n'}, N)$, if leads to a collision, the allenge fails, that is, the value of c_0 has been assigned before. Then, reselect c_0 and repeat this step.
6) Output signature $(S'_1, S'_2, \cdots, S'_n, f')$.

In the unforgeable security model of *Sec.II*, the number of private keys that the adversary needs to know is strictly less than the threshold of the forged threshold ring signature. Suppose that A can obtain the threshold ring signature $\sigma' = (S'_1, S'_2, \cdots, S'_n, f')$ when only knowing the private keys of $t - 1$ members. Because A knows $t - 1$ with the private key of $\{1, 2, 3, \cdots, t - 1\}$ member, the probability of ID^* participating in the signature is

$$\phi = \frac{1}{(n - t + 1)} \tag{8}$$

The probability that A does not query the private key of the ID^* is

$$\alpha = \frac{(q_H - q_E)}{q_H} \tag{9}$$

And the probability of $ID^* \in U$ is

$$\begin{aligned}\beta &= (n - t + 1) \cdot \frac{(q_H - q_E - 1)}{q_H - q_E} \cdot \frac{(q_H - q_E - 2)}{q_H - q_E - 1} \\ &\quad \frac{q_H - q_E - (n - t)}{q_H - q_E - (n - t - 1)} \cdot \frac{1}{q_H - q_E - (n - t)} \\ &= \frac{n - t + 1}{q_H - q_E}\end{aligned} \tag{10}$$

Therefore, the probability of success in M simulation is

$$\begin{aligned}\delta &= \phi \cdot \alpha \cdot \beta \\ &= \frac{1}{(n - t + 1)} \cdot \frac{(q_H - q_E)}{q_H} \cdot \frac{n - t + 1}{q_H - q_E} \\ &= \frac{1}{q_H}\end{aligned} \tag{11}$$

where q_H is the number of times that A queries random prediction hash function, the number of Extract queries as q_E. Since A only queries the polynomial degree of q_H, the probability of success in the simulation is very high.

According to the Heavy-Row lemma [33], another forged threshold ring signature $\sigma'' = (S''_1, S''_2, \cdots, S''_n, f'')$ can be constructed in the random prediction model. From the signature algorithm, when ID_i is not involved in the signature, $f'(i) = f''(i)$. Because $c'_0 \neq c''_0$, so when ID_i participates in the signature, $f'(i) \neq f''(i)$. M can compute the discrete-log

$$D_{ID_i} = \frac{(s'_i - s''_i)}{(c'_i - c''_i)} \; mod \; p \tag{12}$$

That is, the *DLP* problem can be solved with a non-negligible probability, which contradicts the difficulty of the *DLP* problem.

So our new scheme is safe in the random prediction model. ■

C. ANONYMITY

Theorem 4: This threshold ring signature scheme satisfies the requirement of anonymity.

Proof: The polynomial f of degree $n - t$ is uniquely determined by c_i and c_0. Where c_i is randomly generated, and c_0 is the output of the random oracle H. Therefore, f can be regarded as a function randomly selected from the set of all polynomials with degree $n - t$ on $GF(p)$. The distribution of c_i is also uniform on $GF(p)$.

For $i \in \bar{I}$, S_i is independently selected and uniformly distributed on $GF(p)$. For $i \in I$, r_i is independently selected and uniformly distributed on $GF(p)$. Since r_i is independent of c_i and x_i, for all $i \in I$, S_i is also uniformly distributed on $GF(p)$. At the same time, the process of obtaining S_i includes the one-way algorithm of the hash function and the *ECDLP* problem, which makes it computationally infeasible to determine the identity of the signer ID_A.

In addition, for any fixed message m and a set of fixed public keys L, we can see that $(S_1, \cdots, S_n)$ has exactly p^n possible solutions. Since the distribution of these possible solutions is independent and evenly distributed, regardless

TABLE 3. **Definition of related symbols.**

Symbol	Definition	Symbol	Definition
n	number of users	t	a threshold in our scheme
T_M	point multiplication of elements in group	T_B	bilinear pairing operation
T_E	exponential operation	T_H	hash function operation

of which signer is involved, even if the opponent A with all the private keys and unbound computing resources has no advantage to identify among the signers any one instead of random guessing. ■

D. RESIST MALICIOUS KGC ATTACKS

Theorem 5: The signature scheme can resist malicious KGC attacks.

Proof: For the signature algorithm, let the adversary A_1 be the malicious KGC in this scheme, it knows the system master key ks and his own ke_j. In this signature scheme, because multiple KGC jointly maintain the system parameters required by the scheme, ks is jointly agreed by all KGC, and ke_j only knows it, and the user signature private key $D_{ID_i} = [d_2][\sum_{j=1}^{k} ke_j]P_1$ knows that each KGC cannot get the user private key $D_{ID_i} = [\sum_{j=1}^{k} t_j]P_1$. In this case, you can only find $D_{ID_i} = [d_2][ke_j]P_1$ related to the ke_j you hold, and there is an *ECDLP* problem, which makes it difficult for the adversary to find $[\sum_{j=1}^{k} t_j]P_1$ based on $S_i = (r_i - c_i)D_{ID_i}$ and $[ke_j]P_1$. Therefore, as long as there is any trusted KGC, this solution can resist malicious KGC attacks. ■

E. RESIST MALICIOUS USER ATTACKS

Theorem 6: The signature scheme can resist malicious user attacks.

Proof: In the standard SM9, the following phenomena may occur. Assume that there is a malicious user A. Knowing that the message m has been tampered with to m', A still signs the message m' and conducts a transaction with user B. In the entire transaction, B cannot find that message m has been tampered with. Thus, A made a fraudulent transaction with B. In order to prevent this phenomenon from happening, this scheme introduces the threshold ring signature on the basis of SM9. Assign the signature power to t (threshold) users. Suppose there are t-1 or less than t-1 malicious members in the ring colluding. These members respectively show their private keys (no more than t-1), and try to obtain $f(0)$ and $f(i)$ related to other members in the ring by reconstructing the secret polynomial $f(x)$. However, since $f(x)$ is a polynomial of degree n-t, it can only be successfully recovered when greater or equal to t members' private keys are known. Therefore, members less than or equal to t-1 cannot obtain member private keys through collusion. ■

F. FORWARD AND BACKWARD SECURITY

Theorem 7: The signature scheme has forward and backward security.

Proof: When the system parameters of the threshold ring signature scheme need to be updated, KGC needs to renegotiate ks and determine the master private key P_{pub-e} according to the ke_j held by each, and issue new key pairs to all users. The previous system parameters are retained, and the ring member node can verify the signature before the update based on the parameters in effect at the time. As for the system parameters, ks and ke_j are randomly selected, so there is no connection between them before and after the update, and the adversary cannot forge the key before the update according to the key at the current stage. If the adversary holds the key before the update, it is also impossible to forge the correct signature at the current stage. ■

G. NON-REPUDIATION

Theorem 8: The algorithm has non-repudiation characteristics.

Proof: Because this scheme can guarantee that the signature has strong unforgeability and extremely high key security. Therefore, once a legal signature appears, the ring member cannot deny that the signature is signed by the t ring member on behalf of the entire ring. ■

VI. PERFORMANCE COMPARISON

First, give the corresponding character definitions, see Table 3. In the above T_E, T_M, T_B, T_H operations, the T_B bilinear pairing operation consumes more resources, so the main comparison is the number of times the operation is used in the scheme. It can be seen from Table 4 that our scheme does not have the advantage of the reference [23] in terms of calculation volume. This is because this scheme introduces a threshold ring signature, which will inevitably increase the consumption of computing resources. However, it can be seen from Table 5 that our scheme has higher security and can resist two types of attacks at the same time. Compared with reference [28], in the whole signature process, although this scheme has increased T_M by n-t times, T_E has increased by n-t-1 times. However, T_H and T_B are reduced by 2n-1 and n-1 times, respectively. Since, compared to T_B and T_H, the resource consumption of T_M and T_E is negligible. Therefore, the calculation efficiency of this scheme is improved.

However, in recent years, as the level of software and hardware in computers continues to improve, their computing capabilities are also increasing. We believe that the improvement of security is more important than the improvement of efficiency. The anonymity of the SM9 [4] identification cryptographic is based on the computational anonymity. Yang *et al.* [27] introduces the concept of group signature, allowing any member of the group to anonymously sign messages on behalf of the entire group. Only when the group administrator turns on the group signature, the true identity of the signer can be revealed. The anonymity is improved compared to SM9. References [25], [28], [29] introduced

TABLE 4. Efficiency analysis of (t, n) threshold ring signature based on SM9.

Algorithm	Signature calculation	Verification calculation	Total calculation
Sun [23]	nT_E+T_H+2T_B+(n+2t)T_M	(2n)T_E+T_B+(2n+t)T_M	(3n)T_E+T_H+3T_B+(3n+3t)T_M
He [28]	(n+1)T_E+(n+1)T_H+(n)T_B+(2n)T_M	(n)T_E+(2n)T_H+(n+1)T_B+(n)T_M	(2n+1)T_E+(3n+1)T_H+(2n+1)T_B+(3n)T_M
Our scheme	(2n-t)T_E+T_H+T_B+(2n-t)T_M	nT_E+(n+1)T_H+(n+1)T_B+(2n)T_M	(3n-t)T_E+(n+2)T_H+ (n+2)T_B+(4n-t)T_M

TABLE 5. Performance analysis of (t, n) threshold ring signature based on SM9.

Algorithm	Anonymity	Unforgeability	Non-repudiation	Anti-malicious user attacks	Anti-malicious KGC attack
SM9 [4]	Weak	Weak	Weak	×	×
Sun [23]	Weak	Weak	Weak	×	×
Zhang [25]	Weak	Weak	Weak	×	×
Yang [27]	Weak	Weak	Weak	×	√
He [28]	Strong	Weak	Weak	×	×
Mu [29]	Stronger	Strong	Strong	√	×
Our scheme	Stronger	Stronger	Stronger	√	√

Note: × means that the performance is not supported, √ means that the performance is supported

blind signatures, ring signatures, and two-party signatures on the basis of SM9. The development process and principle of digital signatures are easy to understand. Compared with group signatures, ring signatures, and two-party signatures have better performance in terms of anonymity. In this work, we introduce (t, n) threshold ring signatures for the first time, extending the document [29] scheme from a fixed 2 users to a variable n users. It is more difficult to find t or greater than t actual signers among n users. Obviously, forging the signature means that all t or greater than t actual signers' signatures need to be forged, which is also difficult. Therefore, compared with the existing scheme, this scheme has stronger anonymity and unforgeability. Without loss of generality, we can equate unforgeability with non-repudiation, and strong unforgeability means strong non-repudiation. Regarding the security of the scheme, references [4], [23], [25], [28], [29] is unable to resist malicious KGC attacks, this scheme adopts a multi-KGC method to achieve higher security. At the same time, due to the threshold of this scheme, this scheme has the performance of resisting malicious user attacks and has stronger security. As shown in Table 5.

The above analysis shows that the proposed scheme has greater advantages than the existing schemes.

VII. CONCLUSION

Aiming at the problem of low security of existing SM9-based signature schemes, this paper proposed an SM9-based threshold ring signature scheme by adopting a multi-KGC system and embedding a threshold ring signature in the SM9 signature. while this scheme has the characteristics of strong anonymity, unforgeability and non-repudiation, it is also resistant to malicious user attacks and malicious KGC attacks, and has a greater overall security advantage. This scheme extends from a single-user signature to a multi-user signature and increases the application scenarios in SM9, making it possible to be widely used in blockchain, Internet of Things, e-commerce and other fields. According to the common points of threshold ring signatures and blockchains without trusted centers, this scheme can be applied to the privacy protection of blockchain cryptocurrencies as the next stage of research.

REFERENCES

[1] M. Yung, Ed., *Advances in Cryptology—CRYPTO 2002* (Lecture Notes in Computer Science), vol. 2442. Berlin, Germany: Springer, 2002, doi: 10.1007/3-540-45708-9_30.

[2] J. Li, T. H. Yuen, and K. Kim, "Practical threshold signatures without random oracles," in *Proc. Int. Conf. Provable Secur.* Berlin, Germany: Springer, 2007, pp. 198–207.

[3] C. A. Melchor, P.-L. Cayrel, P. Gaborit, and F. Laguillaumie, "A new efficient threshold ring signature scheme based on coding theory," *IEEE Trans. Inf. Theory*, vol. 57, no. 7, pp. 4833–4842, Jul. 2011.

[4] J. Zhang and Y. Zhao, "A new multivariate based threshold ring signature scheme," in *Proc. NSS*, 2015, pp. 526–533.

[5] X. D. Liu, W. F. Zhang, and X. M. Wang, "Multi-Authority attribute-based alterable threshold ring signature without central authority," *J. Softw.*, vol. 29, no. 11, pp. 3528–3543, 2018.

[6] Y. L. Ren, D. T. Xu, and X. P. Zhang, "Deletable blockchain based on threshold ring signature," *J. Commun.*, vol. 40, no. 4, pp. 75–86, 2019.

[7] H. Assidi, E. B. Ayebie, and E. M. Souidi, "An efficient code-based threshold ring signature scheme," *J. Inf. Secur. Appl.*, vol. 45, pp. 52–60, Apr. 2019.

[8] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, in Lecture Notes in Computer Science, vol. 196, 1984, pp. 47–53.

[9] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," in *Proc. Symp. Cryptogr. Inf. Secur.*, Okinawa, Japan, 2000, pp. 26–28.

[10] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 2001, pp. 213–229.

[11] F. Yuan and Z. H. Chen, "Summary of SM9 identification cipher algorithm," *Inf. Secur. Res.*, vol. 2, no. 11, pp. 1008–1027, 2016.

[12] China National Cryptography Administration. (Mar. 28, 2016). *National Cryptography Administration Announcement (No.30)*. [Online]. Available: http://www.sca.gov.cn/sca/xxgk/2016-03/28/content_1002815.shtml

[13] M. Yin, "Summary of the research on identity-based cryptographic algorithm SM9," *Inf. Technol. Informatization*, no. 5, pp. 88–93, May 2020.

[14] J. Xuan, D. Wang, Z. Li, and S. Zhang, "Design of secure and independent controllable email system based on identity-based cryptography," in *Proc. 2nd IEEE Int. Conf. Comput. Commun.*, Oct. 2016, pp. 217–222.

[15] Q. F. Wen, W. J. Yang, and Y. Q. Zhang, "Application of SM9 and PKI in e-government e-mail system," *Comput. Appl. Softw.*, vol. 34, no. 4, pp. 105–109, 2017.

[16] X. Y. Cai, H. X. Zhou, and H. H. Zhang, "Security mail solution based on national security algorithm," *Inf. Technol. Standardization*, no. 9, pp. 39–41, Sep. 2018.

[17] S. Park, K. Lee, and D. H. Lee, "New constructions of revocable identity-based encryption from multilinear maps," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 8, pp. 1564–1577, Aug. 2015.

[18] X. T. Ma, W. P. Ma, and X. X. Liu, "A cross domain authentication scheme based on blockchain technology," *Acta Electron. Sinica*, vol. 46, no. 11, pp. 2571–2579, 2018.

[19] F. Qiu, K. Y. Hu, L. M. Zuo, and M. L. Zhang, "Distributed control identity authentication technology based on SM9," *Comput. Appl. Softw.*, vol. 37, no. 9, pp. 291–295+327, 2020.

[20] P. Yang, S. H. Fan, and Y. Zhu, "Design and application of IoT security platform based on SM9 algorithm," *Commun. Technol.*, vol. 53, no. 3, pp. 738–743, 2020.

[21] P. Zhen, Y. Tu, B. Xia, J. Gan, and X. Tang, "Research on the Miller loop optimization of SM9 bilinear pairings," in *Proc. IEEE 17th Int. Conf. Commun. Technol. (ICCT)*, Oct. 2017, pp. 138–144.

[22] S. Wang, L. G. Fang, and L. B. Han, "Fast implementation of SM9 digital signature and verification algorithms," *Commun. Technol.*, vol. 52, no. 10, pp. 2524–2527, 2019.

[23] H. Sun, X. F. Zheng, and S. Omer, "Efficient provably secure certificateless threshold ring signature scheme," *Bull. Sci. Technol.*, vol. 31, no. 10, pp. 239–243 and 248, 2015.

[24] Z. W. Gan and F. Y. Liao, "Rapid calculation of R-ate bilinear pairing in China state cryptography standard SM9," *Comput. Eng.*, vol. 45, no. 6, pp. 171–174, 2019.

[25] X. F. Zhang and H. Peng, "Blind signature scheme based on SM9 algorithm," *Netinfo Secur.*, vol. 19, no. 8, pp. 61–67, 2019.

[26] Y. Shi, Z. Ma, R. Qin, X. Wang, W. Wei, and H. Fan, "Implementation of an attribute-based encryption scheme based on SM9," *Appl. Sci.*, vol. 9, no. 15, p. 3074, Jul. 2019.

[27] Y. T. Yang, J. L. Cai, X. W. Zhang, and Z. Yuan, "Privacy preserving scheme in block chain with provably secure based on SM9 algorithm," *J. Softw.*, vol. 30, no. 6, pp. 1692–1704, 2019.

[28] D. B. He, C. Peng, and Q. Fan, "A ring signature generation method based on SM9 digital signature algorithm," China Patent 110 912 708 A, Mar. 24, 2020.

[29] Y. H. Mu, H. X. Xu, and P. L. Li, "Secure two-party SM9 signing," *Sci. China, Inf. Sci.*, vol. 63, no. 8, pp. 239–241, 2020.

[30] C. Lin, D. He, X. Huang, X. Xie, and K.-K.-R. Choo, "Blockchain-based system for secure outsourcing of bilinear pairings," *Inf. Sci.*, vol. 527, pp. 590–601, Jul. 2020.

[31] S. S. M. Chow, L. C. K. Hui, and S. M. Yiu, "Identity based threshold ring signature," in *Proc. Int. Conf. Inf. Secur. Cryptol.*, in Lecture Notes in Computer Science, 2005, pp. 218–232.

[32] C. Park and S. Chee, Eds., *Information Security and Cryptology—ICISC 2004* (Lecture Notes in Computer Science), vol. 3506. Berlin, Germany: Springer, 2004, doi: 10.1007/11496618_16.

[33] K. Ohta and T. Okamoto, "On concrete security treatment of signatures derived from identification," in *Proc. Annu. Int. Cryptol. Conf.*, in Lecture Notes in Computer Science, vol. 1462, 1998, pp. 354–369.

SHUANGGEN LIU was born in 1979. He received the Ph.D. degree in cryptography from Xidian University, in 2008. He is currently an Associate Professor with the School of Cyber Security, Xi'an University of Posts and Telecommunications, Xi'an, China. His recent research interests include cryptography and information security. He is a member of the China Computer Federation and the Chinese Association for Cryptologic Research.

KANG CHEN was born in 1996. He is currently a Graduate Student with the Xi'an University of Posts and Telecommunications. He is mainly engaged in the research of digital signatures.

ZIKANG LIU was born in 2001. He is currently pursuing the bachelor's degree with the Xi'an University of Posts and Telecommunications. He is mainly engaged in the research of digital signatures.

TENG WANG received the B.S. degree from the School of Software, Xidian University, China, in 2015, and the Ph.D. degree from the School of Computer Science and Technology, Xi'an Jiaotong University, China, in 2020. She was a Visiting Ph.D. Student with the School of Computer Science and Engineering, Nanyang Technological University, Singapore, from 2018 to 2019. She is currently a Lecturer with the School of Cyberspace Security, Xi'an University of Posts and Telecommunications, China. Her research interests include mobile crowdsensing systems (MCS), privacy-preserving data collection and analysis, and privacy-preserving machine learning.