Abstract— A small size group signature scheme based on RSA cryptosystem is described in this paper. Due to the special algebraic structure of RSA, one public key and two corresponding private keys are available. The two private keys are used as signature keys for group members. The signature operation includes an ordinary RSA signature and a zero knowledge proof about signature key. Compared with most group schemes, it has low computational cost as to signature and verification.

I. INTRODUCTION

In 1991, Chaum and van Heyst [5] proposed the idea of group signature. Afterwards, many group signature schemes are presented, such as the scheme of Camenisch and Stadler [3]. We notice that, most of the group signature schemes are based on the discrete logarithm problem. Such schemes have much cost than that of ordinary signature schemes in respect of signature and verification operation.

RSA cryptosystem [7] is the most well-known public cryptosystem, and it is widely used from the transport of symmetric-key encryption keys, the encryption of small data, to the e-commerce in practice. The security of the RSA cryptosystem is based on the problem of factoring very large numbers, and the RSA problem. The computation cost of RSA cryptosystem is small: it requires only one modular exponentiation. Even in the version against adaptive chosen ciphertext attack, RSA-OAEP [2], the increased cost is two computations of hash function.

The rest of this paper is organized as follows. Section 2 recalls the basic background and notions needed for the paper. Section 3 presents the new group signature scheme based on RSA cryptosystem. In Section 4, we focus on the security analysis of the scheme. Finally, the paper concludes in Section 5.

II. BACKGROUND AND NOTATIONS

A. Number Theory

Definition 1. (Carmichael Function) \( \lambda(n) \) is the smallest integer \( k \), such that

\[ a^k = 1 \pmod{n} \]

for all \( a \) relatively prime to \( n \).

Theorem 1. (Euler) If \( a \in Z_n^* \), then

\[ a^{\phi(n)} = 1 \pmod{n} \]

where \( \phi(n) \) is Euler totient function.

Corollary 1. If \( a \in Z_n^* \), then

\[ a^{k\phi(n)+1} = a \pmod{n} \]

where \( k \) is any integer.

Theorem 2. (Carmichael [4]) If \( a \in Z_n^* \), then

\[ a^{\lambda(n)} = 1 \pmod{n} \]

Corollary 2. If \( a \in Z_n^* \), then

\[ a^{k\lambda(n)+1} = a \pmod{n} \]

where \( k \) is any integer.

Corollary 3. If \( p, q \) are two different primes, \( n = p \times q \), then \( 2 \mid \lambda(n) \mid \phi(n) \), and \( \lambda(n) \) is the proper factor of \( \phi(n) \).

B. RSA Cryptosystem

1) Key Generation:

For Simplification, assume the user is Alice

- Alice chooses two large prime numbers \( p \) and \( q \),
- computes \( n = p \times q \) and \( \phi(n) = (p - 1)(q - 1) \)
- Alice chooses an integer \( e \), which is coprime to \( \phi(n) \), then computes \( d \) such that \( ed = 1 \pmod{n} \)
- Alice publishes \((n, e)\) as her public key, keeps \((n, d)\) as her private key.

2) Signature Generation:

Let the message be \( m \) or \( \text{Hash}(m) \), then the signature \( s \) is computed as follows, where \( \text{Hash(.)} \) is a one-way collision resistant hash function.

\[ s = md \pmod{n} \]
3) **Signature Verification:**
To verify message $m$ and the signature $s$, the receiver computes
\[ a = s^e \pmod n \]
and compares $m$ with $a$. If they are equal, $s$ is the signature of $m$, otherwise refuses the signature.

C. **Group signature**

In brief, a group signature scheme allows a member of a group to sign messages anonymously on the group’s behalf. In the case of later dispute, a designated group manager, $M$, can reveal the signer’s identity. A (generalized) group signature scheme for group $G$ and group manager $M$ consists of four procedures:

1) **Setup:**
A probabilistic interactive protocol between the group manager $M$ and the members of $G$. On input $G$ this protocol outputs the group’s public key $y$, a secret key to each group member $P$ of $G$, and an opening secret key $x$ to the group manager $M$.

2) **Sign:**
A probabilistic protocol executed by group member $P$. On input of a message $m$, the group’s public key $y$, and the secret key of $P$, this protocol outputs a signature $s$ of $m$.

3) **Verify:**
On input a message $m$, a signature $s$, and the group’s public key $y$, this algorithm outputs yes if and only if the signature is correct.

4) **Open:**
An algorithm that takes as input a message $m$, a signature $s$, the group public key $y$, and the revocation secret key $x$. If $s$ is a valid group signature of $m$ with respects to $y$, the algorithm output a proof that $s$ is indeed the signature of $m$ by some group member $P$.

D. **Zero Knowledge Non-interactive Proof of Knowledge**

A zero knowledge proof of knowledge [6] is an interactive method for one party to prove to another that his knowledge of some secret, without revealing anything else. We give the formal definition as follows:

**Definition 2.** (non-interactive proof system): A pair of probabilistic machines, $(P; V)$, is called a non-interactive proof system for a language $L$ if $V$ is polynomial time and the following conditions hold:

1) **Completeness:** For every $x \in L$
\[ Pr[V(x, R, P(x, R)) = 1] \geq \frac{2}{3} \tag{1} \]
where $R$ is a random variable uniformly distributed in $\{0, 1\}^{\text{poly}(|x|)}$

2) **Soundness:** For every $x \notin L$ and every machine $P'$
\[ Pr[V(x, R, P'(x, R)) = 1] \leq \frac{1}{3} \tag{2} \]

where $R$ is a random variable uniformly distributed in $\{0, 1\}^{\text{poly}(|x|)}$

3) **Zero Knowledge:** There exists a polynomial $p$ and a probabilistic polynomial time algorithm $M$ such that the ensembles $\{ (x, U_p(x)), P(x, U_p(x)) \} \in L$ and $\{ M(x) \}_{x \in L}$ are computationally indistinguishable, where is $U_m$ a random variable uniformly distributed in $\{0, 1\}^m$

III. **GROUP SIGNATURE SCHEME**

A. **Basic Idea**

Let $e \in Z_n^*, d_1, d_2$ is the reverse of $e$ modular corresponding to $\Phi(n)$ and $\lambda(n)$, in other words
\[ e \cdot d_1 = 1 \pmod n \]
\[ e \cdot d_2 = 1 \pmod n \]

So, there exists integer $l, m$, such that
\[ e \cdot d_1 = l \Phi(n) + 1 \]
\[ e \cdot d_2 = m \lambda(n) + 1 \]

From Corollary 1 and Corollary 2, we have
\[ a^{ed_1} = a \pmod n \]
\[ a^{ed_2} = a \pmod n \]

where $a \in Z_n^*$

Notice that Corollary 3 guarantees if $e$ is coprime to $\Phi(n)$, then $e$ is also coprime to $\lambda(n)$. But $d_1$ is not equal to $d_2$ in general, for they are reverses modular different modulus. If we take $e$ as the public key, then $d_1, d_2$ is the two private keys corresponding public key $e$. Namely the RSA cryptosystem have the property of one public key corresponding to two private keys. Clearly, the operation of encryption and signing are the same with respect to the two key pair $(e, d_1)$ and $(e, d_2)$. Furthermore, if the dealer (group manager) distributes private key $d_1, d_2$ between two users $A$ and $B$ (group members), then the signature generated by $A$ or $B$ can be verified by the same verification algorithm as ordinary RSA signature.

However it will be proved that the signature of message $m$ by $d_1$ and $d_2$ is equal, this is easily shown by the following equation:
\[ m^{d_1} = (a^e)^{d_1} = a^{ed_1} = a = a^{ed_2} = (a^e)^{d_2} = m^{d_2} \pmod n \]

Notice that for $m \in Z_n^*$, there exists $a \in Z_n^*$ satisfying $m = a^e \pmod n$, so the equation holds.

To confirm the identity of the signer, a proof of knowledge of secret key is needed. In the paper, we use the Schnorr [8] scheme based on the discrete logarithm problem.
B. Description of Group Signature

1) Setup:
   - Group manager chooses two primes \( p \) and \( q \), computers \( n = p \times q \) and \( \Phi(n) \).
   - Group manager chooses the public key \( e \), which is coprime to \( \lambda(n) \), computes two secret keys \( d_1 \) and \( d_2 \) such that
     \[
     e \cdot d_1 = 1 \pmod{\Phi(n)}
     \]
     \[
     e \cdot d_2 = 1 \pmod{\phi(n)}
     \]
   - The manager choose a big prime \( k \), and \( g \), the generator of \( Z_k^* \), then computes
     \[
     y_1 = g^{d_1} \pmod{k}
     \]
     \[
     y_2 = g^{d_2} \pmod{k}
     \]
   - The manager transfers the public key \((n, e)\) and \( y_1 \), \( y_2 \) to the designated verifier \( V \) secretly, distributes \((n, d_1)\) and \((n, d_2)\) between group member \( A \) and \( B \) after permuting the two private key pairs randomly.

2) Sign:
   For the sake of simpleness, assume user \( A \)'s secret key is \( d_1 \), then the signature \( \sigma \) of message \( m \) is:
   \[
   \sigma = m^{d_1} \pmod{n}
   \]
   A also supplies Schnorr signature \( \sigma \) of \((r, s)\) with respect to the public key \( y_1 \)
   \[
   g^s = ry_1^{\text{Hash}(\sigma || r)}
   \]

3) Verify:
   After received \((m, \sigma)\) and the proof of knowledge of secrete key \((r, s, y_1)\), \( V \) verifies the signature \((m, \sigma)\) by comparing
   \[
   m = \sigma^e \pmod{n}?
   \]
   At the same time, \( V \) verifies the correctness of Schnorr signature.

4) Open:
   After verifying the correctness of the signature, the group manager directly confirms the identity of the user by comparing \( y_1 \) or \( y_2 \).

IV. ANALYSIS OF SECURITY AND EFFICIENCY

The security of signature is guaranteed by the security of RSA cryptosystem. Furthermore, the Schnorr scheme is provable secure in random oracle model [1]. It should be noticed that Schnorr scheme proposed in the paper might be replaced by any other scheme, which has the property of zero knowledge proof of knowledge.

On the computation efficient, the signature operation is need only one ordinary RSA modular exponentiation and one zero knowledge proof of secret key. The total cost is lower than that of [3], which needs two modular exponentiations and two signatures of knowledge of discrete logarithms. Similarly, the cost of verification operation is also lower than [3].

The only inadequateness is that the size of the group is limited to only two members, due to the algebraic property of RSA cryptosystem, which in some sense hinders its application. Moreover the public key is only known to the verifier.

V. CONCLUSION

This paper proposed a small size group signature scheme based on RSA cryptosystem. The scheme utilizes the special algebraic property of RSA to produce one public key and two corresponding private keys. The cost of signature is the ordinary RSA signature operation plus one zero knowledge proof of knowledge of secret key. The scheme has low computational cost than most group schemes based on the discrete logarithm problem, while remaining the advantage of group scheme.

REFERENCES

[4] R. D. Carmichael. On the numerical factors of the arithmetic forms \( n^2 \pm \beta n + \alpha \). 15:30–70, 1913.