Identity-based Ring Signature Scheme Based on Cubic Residues

Xuedong Dong[1, a *], Xinxin Liu[2,b]

[1]College of Information Engineering, Dalian University, Dalian 116622, P.R.China

[a]email: dongxuedong@sina.com, [b]email:2368082329@qq.com

Keywords: Identity-based Signature(IBS), ring signature, cubic residues, integer factorization, random oracle model.

Abstract. In order to improve the efficiency of ring-based signature scheme, a new ring-based signature scheme based on cubic residues is proposed. The scheme does not need any bilinear pairing computation which is known to be difficult to computation. The proposed scheme is proved to meet the signer unconditional anonymity. The scheme is also secure against existing forgery on the adaptively chosen message and identity attack under assumption of the hardness of integer factorization.

Introduction

A ring signature can be regarded as a simplified group signature with no manager, no group setup procedure, and no revocation mechanism against signer's anonymity. In a ring signature scheme, the information of all possible signers serves as a part of the ring signature for the signed message. A valid ring signature will convince the verifier that the signature is generated from one of the ring members, without revealing any information about which ring member is the actual signer. Rivest et al. [1] firstly proposed the concept of ring signature. Then many identity-based ring signature schemes from bilinear pairings were proposed [2, 3]. For all these schemes, the performance heavily depends on the cost of computing pairing operations. In [4], it was proposed that an identity-based ring signature scheme based on quadratic residues. The proposed is more efficient than those which are constructed from bilinear pairings. Recently, Guo et al. [5] proposed a identity-based signature scheme based on cubic residues from Eisenstein integer ring. In this paper we propose a new identity-based signature scheme based on cubic residue from integer ring Z. If one selects proper parameters, the computational efficiency of constructing a cubic residue is better than constructing a quadratic residue. The scheme is secure against existing forgery on the adaptively chosen message and identity attack under assumption of the hardness of integer factorization. The proposed scheme is proved to meet the signer unconditional anonymity. The rest of the paper is organized as follows. In Section 2, we give a brief review of Xiong et al.'s scheme. In Section 3, a identity-based signature scheme based on cubic residues is proposed. Section 4 gives the security analysis for the proposed scheme.

Brief Review of Xiong et al.'s Scheme

Xiong et al.'s scheme is composed of 5 algorithms, called *Setup*, *PubKeyGen*, *SeckeyExt*, *Sign* and *Verify*.

Setup: The algorithm takes in security parameters (k,l). Private key generator(PKG) generates two primes p and q and compute $N = pq$, satisfying $pq < 2^k$. Choose a random integer a such that Jacobi symbol $(\frac{a}{N}) = -1$. Compute $d = (N - p - q + 5)/8$ and choose two secure hash functions $H_1 : \{0,1\}^* \to Z_N^*$ and $H_2 : \{0,1\}^* \to \{0,1\}^l$. The system public parameters are *params* $\{N, a, H_1, H_2, l\}$ and master secret key is $\{p, q, d\}$.

PubKeyGen: Given ID_U, PKG computes public key PK_{ID_U} as well as two tags $\{c_1, c_2\}$ as follows.

Compute $c_1 = \begin{cases} 0, & if\ (\dfrac{H_1(ID_U)}{N}) = 1 \\ 1, & if\ (\dfrac{H_1(ID_U)}{N}) = -1 \end{cases}$, $h = a^{c_1} H_1(ID_U)$, $c_2 = \begin{cases} 0, & if\ (\dfrac{h}{p}) = \dfrac{h}{q}) = 1 \\ 1, & if\ (\dfrac{h}{p}) = \dfrac{h}{q}) = -1 \end{cases}$.

A user U with identity ID_U has the public key $PK_{ID_U} = (-1)^{c_2} a^{c_1} H_1(ID_U) (\mathrm{mod}\ N)$.

SeckeyExt: Given PK_{ID_U}, , PKG computes the corresponding private key $SK_{ID_U} \equiv (PK_{ID_U})^{d^l} (\mathrm{mod}\ N)$.

*Sign:*Let $L = \{ID_1, \mathbf{L}, ID_n\}$ be the set of identities of all users and $m \in \{0,1\}^{\text{å}}$ the message to be signed. The user with identity ID_s carries out the following steps to give an identity-based ring signature on behalf of the group L. For ID_i, execute *PubKeyGen* to get $\{PK_{ID_i}, c_{i1}, c_{i2}\}$. Choose random numbers $0 < r_i < N$ and compute $R_i \equiv r_i^{2^l} mod N, h_i = H_2(L \| m \| R_i)$ for $i \in \{1, \mathbf{L}, n\} - \{s\}$. Choose random numbers $0 < r_s < N$ and compute $R_s^{\text{å}} \equiv r_s^{2^l} \bmod N, h_s^{\text{å}} = H_2(L \| m \| R_s^{\text{å}})$ and $R_s \equiv PK_{ID_s}^{h_s^{\text{å}}} \prod_{i \neq s} (R_i PK_{ID_i}^{h_i})^{-1} \bmod N$. Compute $h_s = H_2(L \| m \| R_s)$ and $V = (SK_{ID_s})^{h_s + h_s^{\text{å}}} \bmod N$. The returned ring signature is $s = \{L, m, V, \bigcup_{i=1}^{n} R_i\}$.

Verify: A verifier can check the validity of the signature pair $s = \{L, m, V, \bigcup_{i=1}^{n} R_i\}$ as follows.

For ID_i, execute *PubKeyGen* to get $\{PK_{ID_i}, c_{i1}, c_{i2}\}$. Compute $h_i = H_2(L \| m \| R_i)$ for $i \in \{1, \mathbf{L}, n\}$. Finally, checks the equation $V^{2^l} \equiv \prod_{i=1}^{n} (R_i PK_{ID_i}^{h_i}) \bmod N$. If the equality holds, output accept; otherwise, reject.

Identity-based Ring Signature Scheme Based on Cubic Residues

*Definition 1.*If there exists an integer x such that $x^3 \equiv a (\mathrm{mod}\ p)$, where $a \in Z$ and $(a, p) = 1$, then a is called a 3th residue modulo p.

Lemma 1. [6] Suppose that $3 | (p-1)$. Then a is a 3th residue modulo p if and only if $a^{(p-1)/3} \equiv 1 (\mathrm{mod}\ p)$.

Lemma 2. [6] Let $p \equiv 2 (\mathrm{mod}\ 3)$ and $q \equiv 4 (\mathrm{mod}\ 9)$ or $q \equiv 7 (\mathrm{mod}\ 9)$ be primes, $N = pq$. Then a is a cubic residue modulo $N = pq$ if and only if a is a cubic residue modulo q.

When we construct a quadratic residue y modulo $N = pq$, y should be a quadratic residue both modulo p and modulo q. However, if we choose proper p and q, it is easier to construct a cubic residue modulo N than construct a quadratic residue modulo N by Lemma 2.The following theorem gives a novel method to compute a cubic root of a cubic residue. Without knowing the factorization of modulus N one can not get the cubic root of a cubic residue.

Theorem 1.[7] Let $p \equiv 2 (\mathrm{mod}\ 3)$ and $q \equiv 4 (\mathrm{mod}\ 9)$ or $q \equiv 7 (\mathrm{mod}\ 9)$ be primes, $N = pq$ and d a cubic residue modulo N. Then $d^{3d} \equiv d (\mathrm{mod}\ N)$, where $d = [2(p-1)(q-1)+3]/9$ if $q \equiv 4 (\mathrm{mod}\ 9)$ and $d = [(p-1)(q-1)+3]/9$ if $q \equiv 7 (\mathrm{mod}\ 9)$. A 3^l th root of d could be efficiently computed as $t = d^{d^l} (\mathrm{mod}\ N)$.

We now propose a certificate-based signature scheme based on cubic residues. The scheme is composed of 5 algorithms, called *Setup, PubKeyGen, SeckeyExt,Sign* and *Verify*.

Setup: The algorithm takes in security parameters (k,l). Private key generator(PKG) generates two primes p and q such that $p \equiv 2(\bmod 3)$ and $q \equiv 4(\bmod 9)$ or $q \equiv 7(\bmod 9)$, satisfying $pq < 2^k$, then compute $N = pq$. Choose secure hash functions $H_1 : \{0,1\}^{\ast} \to Z_{CA}^{\ast}$, $H_2 : \{0,1\}^{\ast} \to \{0,1\}^t$, and a random integer a such that $a^{(q-1)/3} \not\equiv 1(\bmod q)$. Let $b = (q-1)/3$, and $x = a^b (modq)$. The system public parameters are *params* $\{N, a, H_1\}$ and master secret key is $\{p, q\}$.

PubKeyGen: Given public parameters $\{N, a, H_1\}$ and ID_U PKG computes the public key and a tag c as follows:

Compute $h_1 = H_1(ID_U)$, $w = h_1^b (\bmod q)$ and $c = \begin{cases} 0, & w = 1 \\ 2, & w = x \\ 1, & w = x^2 \end{cases}$. A user U with identity ID_U has the public key $PK_{ID_U} = a^c h_1 (\bmod N)$. Then compute $Cert_{ID} \equiv V^{d^l} \bmod N$, where d as in Theorem 1.Send $\{Cert_{ID}, c\}$ to the user with the identity ID.

Remark 1. PK_{ID_U} is a cubic residue modulo N [7].

SeckeyExt: Given PK_{ID_U} PKG computes the corresponding private key $SK_{ID_U} \equiv PK_{ID_U}^{d^l} \bmod N$ .PKG secretly send $\{SK_{ID_U}, c\}$ to the user with the identity ID_U .

Sign: Let $L = \{ID_1, \mathbf{L}, ID_n\}$ be the set of identities of all users and $m \in \{0,1\}^{\ast}$ the message to be signed. The user with identity ID_s gives an identity-based ring signature on behalf of the group L. For ID_i , execute *PubKeyGen* to get $\{PK_{ID_i}, c_i\}$. Choose random numbers $0 < r_i < N$ and compute $R_i \equiv r_i^{3^l} \bmod N, h_i = H_2(L \| m \| R_i)$ for $i \in \{1, \mathbf{L}, n\} - \{s\}$. Choose random numbers $0 < r_s < N$ and compute $R_s^{\ast} \equiv r_s^{3^l} \bmod N, h_s^{\ast} = H_2(L \| m \| R_s^{\ast})$ and $R_s \equiv PK_{ID_s}^{h_s^{\ast}} \prod_{i \neq s} (R_i PK_{ID_i}^{h_i})^{-1} \bmod N$. Compute $h_s = H_2(L \| m \| R_s)$ and $V = (SK_{ID_s})^{h_s + h_s^{\ast}} \bmod N$. The returned ring signature is $s = \{L, m, V, \bigcup_{i=1}^{n} R_i\}$.

Verify: A verifier can check the validity of the signature pair $s = \{L, m, V, \bigcup_{i=1}^{n} R_i\}$ as follows.

For ID_i, execute *PubKeyGen* to get $\{PK_{ID_i}, c_i\}$. Compute $h_i = H_2(L \| m \| R_i)$ for $i \in \{1, \mathbf{L}, n\}$. Finally, checks the equation $V^{3^l} \equiv \prod_{i=1}^{n} (R_i PK_{ID_i}^{h_i}) \bmod N$. If the equality holds, output accept; otherwise, reject.

Remark 2. Since $PK_{ID_s}^b = (a^c h_1)^b \equiv a^{cb} w \equiv x^c w \equiv 1(\bmod q)$, it is a cubic residue modulo N. By Theorem 1, $PK_{ID_s}^{3^l d^l} \equiv PK_{ID_s} \bmod N$. So, $V^{3^l} \equiv (SK_{ID_s})^{3^l h_s + 3^l h_s^{\ast}} \equiv PK_{ID_s}^{d^l 3^l (h_s + h_s^{\ast})} \equiv PK_{ID_s}^{h_s + h_s^{\ast}} \equiv PK_{ID_s}^{h_s} PK_{ID_s}^{h_s^{\ast}} \equiv PK_{ID_s}^{h_s} R_s \prod_{i \neq s} (R_i PK_{ID_i}^{h_i}) \equiv \prod_{i=1}^{n} (R_i PK_{ID_i}^{h_i}) \bmod N$. Thus, $V^{3^l} \equiv \bigcup_{i=1}^{n} (R_i PK_{ID_i}^{h_i}) \bmod N$ if and only if the signature is valid.

Security analysis

We now consider three security requirements for the proposed scheme: key secrecy, unforgeability and signer anonymity. Given all public information, deducing signer $U's$ private key $SK_{ID_U} \equiv PK_{ID_U}^{d^l} \bmod N$ is computationally infeasible under the intractability of the hardness of integer factorization. Given a message m , a set $L = \{ID_1, \mathbf{L}, ID_n\}$ of identities of ring members, and all public

information, any $U_k \notin L$ cannot compute a valid ring signature. An adversary $U_k \notin L$ may try to compute a valid ring signature for message m via two ways. Firstly, he/she tries to compute V such that $V^{3^l} \equiv \prod_{i=1}^{n}(R_i PK_{ID_i}^{h_i}) \bmod N$. This is a discrete logarithm problem which is considered to be difficult. Secondly, he/she tries to compute h_s such that $V^{3^l} R_s^{-1} \prod_{i\neq s}(R_i PK_{ID_i}^{h_i})^{-1} \equiv PK_{ID_s}^{h_s} \bmod N$, which is again a discrete logarithm problem.Given a message m and the ring signature is $s = \{L, m, V, \prod_{i=1}^{n} R_i\}$, no one finds out who is the actual signer. In fact, $\prod_{i\neq s} R_i$ and $h_s^{\hat{a}}$ are chosen uniformly at random, so $\prod_{i=1}^{n} R_i$ are uniformly distributed.It remains to consider whether $V = (SK_{ID_s})^{h_s + h_s^{\hat{a}}} \bmod N$ leaks the information about the actual signer. ID_s is related to $(PK_{ID_s})^{h_s^{\hat{a}}} \bmod N = (SK_{ID_s})^{3^l h_s^{\hat{a}}} \bmod N$. Any one can compute the $R_s \prod_{i\neq s}(R_i PK_{ID_i}^{h_i}) \equiv PK_{ID_s}^{h_s^{\hat{a}}} \bmod N$. One may compute $R_j \prod_{i\neq j}(R_i PK_{ID_i}^{h_i}) \equiv V^{3^l} (PK_{ID_j}^{h_j})^{-1} \bmod N$ to guess that ID_j is the actual signer. However,

$$R_j \prod_{i\neq j}(R_i PK_{ID_i}^{h_i}) \equiv R_s \prod_{i\neq s} R_i \prod_{i\neq j}(PK_{ID_i}^{h_i}) \equiv PK_{ID_s}^{h_s^{\hat{a}}} \prod_{i\neq s}(R_i PK_{ID_i}^{h_i})^{-1} \prod_{i\neq s} R_i \prod_{i\neq j}(PK_{ID_i}^{h_i}) \equiv PK_{ID_s}^{h_s^{\hat{a}}} PK_{ID_s}^{h_s} PK_{ID_j}^{h_j^{-1}}$$

$$\equiv (SK_{ID_s}^{3^l})^{h_s^{\hat{a}} + h_s} PK_{ID_j}^{h_j^{-1}} \equiv V^{3^l} (PK_{ID_j}^{h_j})^{-1} \bmod N \text{ for all } j \in \{1, 2, \mathbf{L}, n\}.$$

So, for a message m and the ring signature $s = \{L, m, V, \prod_{i=1}^{n} R_i\}$, V is independent and uniformly distributed. Thus, no adversary can guess the actual signer with the probability greater than $1/n$. Similarly as in [4,5], we can prove that the proposed scheme is also secure against existing forgery on the adaptively chosen message and identity attack under assumption of the hardness of integer factorization.

Acknowledgement

This study was supported by the National Nature Science Foundation of China under grant 10171042 and the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

[1] R.Rivest, A.Shamir, and Y.Tauman, How to leak a secret, Advances in Cryptology-Asiacrypt 2001, LNCS 2248, Springer-Verlag, 2001, pp. 552-565.

[2] D.Boneh and M.Franklin, Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto 2001, LNCS 2139, Springer-Verlag, 2001, pp. 213-229.

[3] K. G.Paterson, An identity-based signature from pairings on elliptic curves, Electronics Letters, 38(2002) 1025-1026.

[4] H.Xiong, Z.Qin, and F.Li, Identity-based ring signature scheme based on quadratic residues, High Technology Letters, 15(2009) 94-100.

[5] H.Guo, Dong X., Z.Cao, Identity-based Ring Signature Scheme Constructed by Cubic Residues, Computer Engineering, 39(2013) 111-117.

[6] Z. Wang, L. Wang, S.Zheng, Y.Yang and Z.Hu,Provably secure and efficient identity-based signature scheme based on cubic residues,International Journal of Network Security,14(2012)33-38.

[7] X. Dong, A Modified Identity-based Signature Scheme Based on Cubic Residues, submitted for publication.