A Modified Identity-based Signature Scheme Based on Cubic Residues

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

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

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

Keywords: Cryptography; Cubic residue; Digital signature; Identity-based

Abstract. Wang *et al.* [Z.Wang, L.Wang, S.Zheng, Y.Yang and Z.Hu, International Journal of Network Security, 14(2012)33-38] proposed an identity-based signature scheme based on cubic residues. But the scheme is insecure because it cannot withstand a conspiracy attack by users. To overcome this security vulnerability, this paper proposes a novel method to compute a cubic root of a cubic residue. Then a modified identity-based signature scheme based on cubic residues is proposed. The security analysis results show that the modified scheme can resist the conspiracy attack.

Introduction

Shamir [1] firstly proposed an identity-based cryptography(IBC) in 1984.In an identity-based signature scheme, an entity's public key is derived directly from its identity, such as an e-mail address, or a social security number associated with a user. The private key is computed and issued secretly to the user by a trusted third party called private key generator (PKG). The main advantage of IBC is that it drastically reduces the needs for certificates. Boneh and Franklin [2] developed an identity based encryption scheme(BF-IBE) based on Weil pairing which is usually considered to be involved heavy computation. Very a few identity-based signature (IBS) schemes are without pairings. Saeednia [3] proposed an identity-based society oriented signature scheme with anonymous signers. Shao [4] showed that the scheme proposed by Saeednia is insecure. Lee and Liao [5] proposed an IBS scheme based on discrete logarithm problem. Qiu and Chen [6] presented an IBS scheme based on quadratic residues which is a combination of identity based and mediated cryptography. Chai et al. [7] proposed a new IBS scheme based on quadratic residues in 2007. They proved that their scheme is secure in the random oracle. Enos et al. [8] extended an ID based signcryption scheme to a compartmented scheme. C.Meshram [9] proposed to integrate forward security into ID-based encryption. Wang et al.[10] proposed an identity-based signature scheme based on cubic residues. If one selects proper parameters, the computational efficiency of constructing a cubic residue is better than constructing a quadratic residue. Unfortunately, according to our security analysis, their scheme cannot resist the users' conspiracy attack. To overcome this security weakness, we propose a novel method to compute a cubic root of a cubic residue and a modified scheme. The security analysis result shows that the modified scheme can resist the conspiracy attack. The scheme is also secure against existing forgery on the adaptively chosen message and identity attack under assumption of the hardness of integer factorization. The rest of the paper is organized as follows. In Section 2, we give a brief review of Wang et al.'s scheme and analyze its weakness. In Section 3, a modified identity-based signature scheme based on cubic residues is proposed. In Section 4, we give security analysis of the modified scheme. Finally, a conclusion is drawn in Section 5.

Brief Review of Wang et al.'s Scheme and an Attack

*Definition 1.*If there exists an integer x such that $x^3 \equiv a \pmod p$, 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 $a^{(p-1)/3} \equiv 1(\bmod p)$.

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

ID-based signature scheme is composed with 4 algorithms, called *Setup*, *Extract*, *Sign* and *Verify*.

Setup(k,l): Taking the security parameters (k,l),this algorithm will be carried out by the PKG as follows:

1) Generate randomly two same length distinct prime numbers p and q, such that $p \equiv 2(\bmod 3)$, $q \equiv 4(\bmod 9)$ or $7(\bmod 9)$, satisfying $pq < 2^k$, then compute $N = pq$.

2) Select a non-cubic residue a modulus q .

3) Compute $\eta = (q-1)/3(\bmod 9)$, and $\lambda = \eta(\bmod 2)+1$.

4) Compute $\beta = (q-1)/3$, and $\xi = a^{\eta\beta}(\bmod q)$.

5) Select $h_1():\{0,1\}^* \to Z_N^*, h_2():\{0,1\}^* \to \{0,1\}^l$ as two hash functions. The master key of PKG is set to be $MK = (p,q,\beta)$, and the public parameters of PKG are $PP = (N, h_1(), h_2(), a, \eta, \lambda)$.

Extract(ID,MK,PP): Given ID, PKG computes the corresponding private key S_{ID} as follows:

1) Compute $\omega = h_1(ID)^{\lambda\beta}(\bmod q)$.

2) Compute $c = \begin{cases} 0, & \omega = 1 \\ 1, & \omega = \xi \\ 2, & \omega = \xi^2 \end{cases}$ and compute $H(ID) \equiv a^c h_1(ID)(\bmod N)$.

3)Compute S_{ID} as cubic root of $H(ID)^{-1}$. $S_{ID} = H(ID)^{\frac{2^{\eta-1}(p-1)(q-1)-3}{9}}(\bmod N)$. $S_{ID}^3 H(ID) \equiv 1(\bmod N)$.

Sign(M, S_{ID} *,PP)*: To sign a message M, a user does as follows:

1) Randomly select $r \in Z_N$, compute $R = r^3(\bmod N)$.

2) Compute $Z = rS_{ID}^{h_2(R,M)}(\bmod N)$. The return signature is $Sig = (Z,R)$.

Verify(PP,Sig,ID): Given a signature $Sig = (Z,R)$ on a message M, a verifier should verify the signature only by the signer's ID:

1) Compute $H_1(ID) = h_1(ID)(\bmod N), H_2(ID) = ah_1(ID)(\bmod N), H_3(ID) = a^2 h_1(ID)(\bmod N)$.

2) Check whether $Z^3 H_i^{h_2(R,M)}(ID) = R(i \in \{1,2,3\})$ holds or not. If one of $i \in \{1,2,3\}$ holds, output “valid” otherwise, output “invalid”.

The weaknesses of Wang et al.'s scheme: The Wang et al.'s scheme cannot resist the conspiracy attack by users. Suppose that a user A with public key $H(ID_A)$ and a user B with public key $H(ID_B)$ respectively have the private keys S_{ID_A} and S_{ID_B}. Then they can cooperate to get a pare of keys $(H(ID_C), S_{ID_C})$, where $H(ID_C) = H(ID_A)H(ID_B)$ and $S_{ID_C} = S_{ID_A} S_{ID_B}$, since $S_{ID_C}^3 H(ID_C) \equiv S_{ID_A}^3 S_{ID_B}^3 H(ID_A)H(ID_B) \equiv 1(\bmod N)$. In particular, $(H(ID_A)^n, S_{ID_A}^n)$ is valid keys. Then, they conspirators can sign any message they like without taking responsibility.

A Modified Identity-based Signature Scheme Based on Cubic Residues

We now give a novel method to compute a cubic root of a cubic residue.

Theorem 1.Let $p \equiv 2(\bmod 3)$ and $q \equiv 4(\bmod 9)$ or $7(\bmod 9)$ be primes, $N = pq$ and δ a cubic residue modulus N. Then $\delta^{3d} \equiv \delta(\bmod N)$, where $d = [2(p-1)(q-1)+3]/9$ if

$q \equiv 4(\bmod 9)$ and $d = [(p-1)(q-1)+3]/9$ if $q \equiv 7(mod 9)$. A $3^l th$ root of δ could be efficiently computed as $\tau = \delta^{d^l} (\bmod N)$.

Proof. We first show that d is an integer. If $q \equiv 4(\bmod 9)$, then $2(p-1)(q-1)+3 = 2(3t+1)(9s+3)+3 = 9k+9$ and $d = [2(p-1)(q-1)+3]/9$ is an integer. If $q \equiv 7(\bmod 9)$, then $(p-1)(q-1)+3 = (3t+1)(9s+6)+3 = 9k+9$ and $d = [2(p-1)(q-1)+3]/9$ is also an integer. Next, since δ is a cubic residue modulus N, there is $x \in Z$ such that $x^3 \equiv \delta(\bmod N)$. Therefore, if $q \equiv 4(\bmod 9)$, then by Euler's theorem $\delta^{3d} \equiv \delta^{[2(p-1)(q-1)]/3+1} \equiv \delta x^{2(p-1)(q-1)} \equiv \delta(\bmod N)$. If $q \equiv 7(\bmod 9)$, then $\delta^{3d} \equiv \delta^{[(p-1)(q-1)]/3+1} \equiv \delta x^{(p-1)(q-1)} \equiv \delta(\bmod N)$. Since $\tau^{3^l} = \delta^{3^l d^l} \equiv \delta^{(3d)^l} \equiv \delta^{\overbrace{(3d)(3d)\cdots(3d)}} \equiv \delta(\bmod N)$, a $3^l th$ root of δ could be efficiently computed as $\tau = \delta^{d^l} (\bmod N)$.

Remark 1. Without knowing the factorization of modulus N one can not get the cubic root of a cubic residue.

We now propose a modified identity-based signature scheme which is established on cubic residues. The scheme is composed with 4 algorithms, namely *Setup*, *Extract*, *Sign* and *Verify*.

Setup (k,l): This algorithm will be carried out by the PKG. The algorithm takes in security parameters (k,l).

1) Generate randomly two same length distinct prime numbers 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 $N = pq$.

2) Select a non-cubic residue a modulus q.

3) Compute $\beta = (q-1)/3$, and $\xi = a^{\beta} (\bmod q)$. Then the multiplicative order of ξ in Z_N^* is 3.

4) Select a $z \in Z_N^*$ such that $(z,N)=1$ and select $h_1() : \{0,1\}^* \to Z_N^*$, $h_2() : Z_N^* \times \{0,1\}^* \to Z_N^*$ as two hash functions.

The master key of PKG is set to be $MK = (p,q,\beta)$, and the public parameters of PKG are $PP = (N, h_1(), h_2(), a, z, l)$.

Extract(ID,MK,PP): Given ID, PKG computes the corresponding private key S_{ID} as follows:

1) Compute $\omega = h_1(ID)^{\beta} (\bmod q)$.

2) Compute $c = \begin{cases} 0, & \omega = 1 \\ 2, & \omega = \xi \\ 1, & \omega = \xi^2 \end{cases}$ and $H(ID) = a^c h_1(ID) (\bmod N)$.

Remark 2. Since $\omega^3 = 1(\bmod q)$, the subgroup generated by ω and the subgroup generated by ξ are both the cyclic group with order 3 in the finite field Z_q. Therefore, we have $\omega = 1$ or $\omega = \xi$ or $\omega = \xi^2$.

Remark 3. $H(ID)$ is a cubic residue modulus N. In fact, $H(ID)^{(q-1)/3} = H(ID)^{\beta} = a^{c\beta} h_1(ID)^{\beta} = \xi^c \omega = 1(\bmod q)$ .Since $p \equiv 2(\bmod 3)$, $H(ID)$ must be a cubic residue modulus p and therefore $H(ID)$ is a cubic residue modulus N.

3) Compute a $3^l th$ root $H(ID)^{d^l} (\bmod N)$ of $H(ID)$ and let $S_{ID} = z^{d^{l-1}} H(ID)^{d^l} (\bmod N)$. PKG secretly returns S_{ID} to the user with *ID*.

Sign(M, S_{ID},PP): To sign a message M, a user does as follows:

1) Randomly select $r \in Z_N^*$ and compute $R = r^{3^l} (\bmod N)$.

2) Compute $\sigma = h_2(R, M)(\bmod N)$.

3) Compute $Z = rS_{ID}^{\sigma}(\bmod N)$.

The return signature is $Sig = (Z, R)$.

Verify(PP,Sig,ID): Given a signature $Sig = (Z, R)$ on a message M, a verifier should verify the signature only by the signer's *ID*:

1) Compute $H_1(ID) = h_1(ID)(\bmod N), H_2(ID) = ah_1(ID)(\bmod N), H_3(ID) = a^2 h_1(ID)(\bmod N)$.

2) Check whether

$\sigma = h_2(Z^{3^l} / (z^3 H_i(ID))^{\sigma}(\bmod N), M)$ holds or not, where $i \in \{1, 2, 3\}$. If one equation holds, the algorithm outputs "valid". Otherwise, the algorithm outputs "invalid".

Remark 4. By Theorem 1, we have $Z^{3^l} \equiv r^{3^l} S_{ID}^{3^l \sigma} \equiv r^{3^l} z^{d^{l-1} 3^l \sigma} H(ID)^{d^l 3^l \sigma} \equiv R(z^3 H(ID))^{\sigma})(\bmod N)$. So, the signature is valid if and only if $\sigma = h_2(Z^{3^l} / (z^3 H_i(ID))^{\sigma}(\bmod N), M)$ holds for some $i \in \{1, 2, 3\}$.

Security analysis of the modified scheme

The above modified scheme can resist the conspiracy attack by users. Suppose that a user A with public key $H(ID_A)$ and a user B with public key $H(ID_B)$ respectively have the private keys S_{ID_A} and S_{ID_B}. Since $S_{ID_A} S_{ID_B} = z^{d^{l-1}} H(ID_A)^{d^l} z^{d^{l-1}} H(ID_B)^{d^l} \not\equiv z^{d^{l-1}} H(ID_A)^{d^l} H(ID_B)^{d^l}$ $(\bmod N)$, $(H(ID_A) H(ID_B), S_{ID_A} S_{ID_B})$ is a not valid key. As a result, in the modified scheme, the conspirators cannot get more useful information then a player does. Therefore the modified scheme withstands conspiracy attack and overcomes the weakness in the previously Wang *et al.*'s scheme. As in [10], the modified scheme is also secure against forgery on the adaptive chosen message and identity attacks assuming the hardness of integer factorization.

Conclusion

In this paper, we have pointed out a security leak of Wang *et al.*'s scheme and further proposed a novel scheme, which not only keeps the merits of the previous scheme, but also remedies the security weakness.

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] A. Shamir, Identity based cryptosystems and sig- nature schemes, Advance in Cryptology-Crypto'84, LNCS 196, Springer-Verlag, 1984, 47-53.

[2] D. Boneh, M. Franklin, Identity-based encryption from Weil pairing, Advance in Cryptology-CRYPTO 2001, LNCS 2193, Springer-Verlag, 2001,213-229.

[3] S.Saeednia, An identity-based society oriented signature scheme with anonymous signers, Information Processing Letters, 2002,83(3), 295-299.

[4] Z. Shao, Cryptanalysis of an identity-based society oriented signature scheme with anonymous signers, Information Processing Letters,2003, 86(6), 295-298.

[5] W. B. Lee, K. C. Liao, Constructing identity-based cryptosystems for discrete logarithm based cryptosystems, Journal of Network and Computer Applications, 2004,27, 191-199.

[6] W. D. Qiu, K. F. Chen, Identity oriented based on quadratic residues, Applied Mathematics and Com- putation, 2005,168, 235-242.

[7] Z. C. Chai, Z. F. Cao, X. L. Dong, Identity-based signature scheme based on quaratic residues, Science in China Series F: Information Sciences, 2007, 50(3),373-380.

[8] G. Enos, Y. Zheng, An ID-based signcryption scheme with compartmented secret sharing for unsigncryption, Information Processing Letters, 2015,115(2),128-133.

[9] C.Meshram, An efficient ID-based cryptographic encryption based on discrete logarithm problem and integer factorization problem, Information Processing Letters, 2015,115(2), 351-358.

[10] 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, 2012,14(1),33-38.