Identity-based signature scheme based on quintic residues

Xue-Dong Dong[†] and Yuan Gao
College of Information Engineering, Dalian University,
Dalian, Liaoning 116622, China
[†]E-mail: dongxuedong@sina.com
www.dlu.edu.cn

We propose a new method to compute a quintic root of a quintic residue. Then we give a new identity-based signature scheme by the method. The scheme is secure against existential forgery on the adaptive chosen message and identity attacks assuming the hardness of factoring. The scheme is the first identity-based signature scheme based on quintic residues.

Keywords: Cryptography; Quintic residue; Identity-based signature; Provable security.

1. Introduction

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 telephone number 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). Shamir [1] firstly proposed an IBC in 1984. 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. 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. Wang et al.[8] 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 that of constructing a quadratic residue. Dong et al.[9] showed that Wang et al.'s scheme cannot resist the users' conspiracy attack and proposed a modified identity-based signature scheme based on cubic residues. The schemes in [8] and [9] are only suitable for primes p and q, where $p \equiv 2(\mathrm{mod}\,3)$ and $q \equiv 4(\mathrm{mod}\,9)$ or $q \equiv 7(\mathrm{mod}\,9)$.In this paper, we propose a novel method to compute a quintic root of a quintic residue and then give a new identity based

signature scheme by the method. The scheme is secure against existential forgery on the adaptive chosen message and identity attacks assuming the hardness of factoring. The scheme is the first identity based signature scheme based on quintic residues. The scheme is suitable for primes p and q, where $p \neq 1(\bmod 5)$, $q \equiv 1(\bmod 5)$ and $q \neq 1(\bmod 25)$.The rest of the paper is organized as follows. In Section 2, we give some preliminaries. In Section 3, an identity-based signature scheme based on quintic residues is proposed. In Section 4, we give security analysis of the scheme. Finally, a conclusion is drawn in Section 5.

2. Preliminaries

Definition 2.1. If there exists an integer x such that $x^5 \equiv a \pmod{p}$, where $a \in Z$ and $(a, p) = 1$,then a is called a quintic residue modulo p.

Lemma 2.1. Suppose that $5 \mid (p-1)$. Then a is a quintic residue modulo p if and only if $a^{(p-1)/5} \equiv 1 \pmod{p}$.

Lemma 2.2. If $(5, p-1) = 1$ and $(a, p) = 1$. Then a is a quintic residue modulo p.

Proof. Since $(5, p-1) = 1,$ there are integers s and t such that $5s + (p-1)t = 1.$ Then $a \equiv a^{5s+(p-1)t} \equiv a^{5s} \pmod{p}$ by Euler's theorem. Thus, a is a quintic residue modulo p. □

Lemma 2.3. Let $p \neq 1(\bmod 5)$, $q \equiv 1(\bmod 5)$ and $q \neq 1(\bmod 25)$ be primes. Then there is an integer a such that $a(p-1)(q-1)/5 \equiv -1(\bmod 5)$.

Proof. Since $p \neq 1(\bmod 5)$, $q \equiv 1(\bmod 5)$ and $q \neq 1(\bmod 25)$,we have $(5, p-1) = 1$, $(5, (q-1)/5) = 1.$ Thus, $(5, (p-1)(q-1)/5) = 1$ and therefore there is an integer a such that $a(p-1)(q-1)/5 \equiv -1(\bmod 5)$. □

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

Theorem 2.1. Let $p \neq 1(\bmod 5)$, $q \equiv 1(\bmod 5)$ and $q \neq 1(\bmod 25)$ be primes, $N = pq$ and δ a quintic residue modulo N. Then $\delta^{5d} \equiv \delta(\bmod N),$ where $d = [a(p-1)(q-1)+5]/25$ and $a(p-1)(q-1)/5 \equiv -1(\bmod 5)$. A 5^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. By lemma 2.3, there is an integer a such that $a(p-1)(q-1)/5 \equiv -1(\bmod 5).$ Thus, we have $a(p-1)(q-1)$ $\equiv -5(\bmod 25)$ and therefore $a(p-1)(q-1)+5 \equiv 0(\bmod 25)$.This shows

that $d=[a(p-1)(q-1)+5]/25$ is an integer. $\delta^{5d} \equiv \delta^{a(p-1)(q-1)/5+1} \equiv \delta(\delta^{(p-1)})^{a(q-1)/5} \equiv \delta(\mathrm{mod}\, p)$ and $\delta^{5d} \equiv \delta^{a(p-1)(q-1)/5+1} \equiv \delta(\delta^{(q-1)/5})^{a(p-1)} \equiv \delta(\mathrm{mod}\, q)$ since δ is a quintic residue modulo q. Thus, $\delta^{5d} \equiv \delta(\mathrm{mod}\, N)$ and $\delta^{d}(\mathrm{mod}\, N)$ is a quintic root of δ. A 5^l th root of δ could be efficiently computed as $\tau = \delta^{d^l}(\mathrm{mod}\, N).$ □

Remark 2.1. Without knowing the factorization of modulus N one cannot get the quintic root of a quintic residue.

3. An identity-based signature scheme based on quintic residues

We now propose an identity-based signature scheme which is established on quintic residues. The scheme is composed with 4 algorithms, namely Setup, Extract, Sign and Verify. The algorithms are constructed as follows:

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 $p \neq 1(\mathrm{mod}\, 5)$, $q \equiv 1(\mathrm{mod}\, 5)$ and $q \neq 1(\mathrm{mod}\, 25)$, satisfying $pq < 2^k$,then compute $N = pq$.

2) Select a non-quintic residue a modulo q.

3) Compute $\beta = (q-1)/5$, and $\xi = a^{\beta}(\mathrm{mod}\, q)$. Then the multiplicative order of ξ in Z_q^* is 5.

4) Select an $z \in Z_N^*$ 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 $\omega = h_1(ID)^{\beta}(\mathrm{mod}\, q)$.

2) Compute $c = \begin{cases} 0, \omega = 1 \\ 1, \omega = \xi^4 \\ 2, \omega = \xi^3 \\ 3, \omega = \xi^2 \\ 4, \omega = \xi \end{cases}$

and compute $H(ID) = a^c h_1(ID) (\mathrm{mod}\, N).$

Remark 3.1. Since $\omega^5 = 1 (\mathrm{mod}\, q),$ the subgroup generated by ω and the subgroup generated by ξ are both the cyclic group with order 5 in the finite field Z_q .However, the cyclic group with order 5 in the finite field Z_q has only one. Therefore, we have $\omega = \xi^i$ for some $0 \le i \le 4.$

Remark 3.2. $H(ID)$ is a quintic residue modulo N .

In fact, $H(ID)^{(q-1)/5} = H(ID)^{\beta} = a^{c\beta} h_1(ID)^{\beta} = \xi^c \omega = 1 (\mathrm{mod}\, q).$ Thus, by Lemma 2.1 $H(ID)$ is a quintic residue modulo q . Since $p \neq 1 (\mathrm{mod}\, 5)$, by Lemma 2.1 $H(ID)$ must be a quintic residue modulo p and therefore $H(ID)$ is a quintic residue modulo N .

3) Compute a $5^l th$ root of $H(ID)^{d^l} (\mathrm{mod}\, N)$ of $H(ID)$ and let $S_{ID} = z^{d^{l-1}} H(ID)^{d^l} (\mathrm{mod}\, N).$ 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 $R = r^{5^l} (\mathrm{mod}\, N).$

2) Compute $\sigma = h_2(R, M) (\mathrm{mod}\, N)$.

3) Compute $Z = r S_{ID}^{\sigma} (\mathrm{mod}\, N)$.

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 $H_1(ID) = h_1(ID) (\mathrm{mod}\, N), H_2(ID) = a h_1(ID) (\mathrm{mod}\, N),$ $H_3(ID) = a^2 h_1(ID) (\mathrm{mod}\, N),$ $H_4(ID) = a^3 h_1(ID) (\mathrm{mod}\, N),$ $H_5(ID) = a^4 h_1(ID) (\mathrm{mod}\, N)$.

2) Check whether $\sigma = h_2(Z^{5^l} / (z^5 H_i(ID))^{\sigma} (\mathrm{mod}\, N), M)$ holds or not, where $i \in \{1, 2, 3, 4, 5\}.$ If one equation holds, the algorithm outputs "valid". Otherwise, the algorithm outputs "invalid".

Remark 3.3. By Theorem 2.1, we have

$$Z^{5^l} \equiv r^{5^l} S_{ID}^{5^l \sigma} \equiv r^{5^l} z^{d^{l-1} 5^l \sigma} H(ID)^{d^l 5^l \sigma} \equiv R(z^5 H(ID))^{\sigma}) (\mathrm{mod}\, N).$$

So, the signature is valid if and only if

$\sigma = h_2(Z^{5^l} / (z^5 H_i(ID))^{\sigma} (\mathrm{mod}\, N), M)$ holds for some $i \in \{1, 2, 3, 4, 5\}.$

4. Security analysis

Consider the following game between an adversary A and a challenger C in order to define the security formally.

1) The challenger C generates the master key MSK and the public parameter PP. C gives PP to A.

2) A makes the following queries adaptively:

• Extraction queries. The challenger C responds by running Extract algorithm to generate the private key S_{ID} corresponding to the public key ID issued by A.

• Signature queries. A gives an identity ID and a message M to C. C runs Sign() algorithm, and gives the signature to A.

• Hash queries. A gives a string $M \in \{0,1\}^*$ to C. C computes the value of hash function, and returns the value to A.

3) At last, A outputs a fake signature

$$Sig = (Z, R, \sigma = h_2(R, M)(\mathrm{mod}\, N))$$

on the message $M \in \{0,1\}^*$, under the condition that A did not issue an extraction query on ID or a signature query on $M \in \{0,1\}^*$ under ID before. A wins the game if the fake signature is recognized as valid by C. The advantage of A is defined to be $Adv^{EF}_{IDSig,A}(k) = \Pr\{$ forged signature is valid $\}$,where EF means existential forgery, IDSig is the identity based signature scheme, and k is the security parameter. An identity based signature scheme is $(t, q_H, q_{sig}, \varepsilon)$-secure against existential forgery on adaptive chosen message and identity attacks, if no adversary has an advantage more than ε winning the above game, where the adversary runs in time at most t, making at most q_H hash queries and q_{sig} signature queries.

Theorem 4.1. If the factoring problem is (t', ε')-hard, then our scheme is $(t, q_{h_2}, q_{sig}, \varepsilon)$ -secure against existential forgery on the adaptively chosen message and ID attack, which satisfying:

$$\varepsilon' \geq 6(\varepsilon - q_{sig}(q_{h_2} + q_{sig}) \cdot 2^{-k})^2 / \pi^2 (q_{h_2} + 1) - 6 \cdot 2^{-l} \cdot (\varepsilon - q_{sig}(q_{h_2} + q_{sig}) \cdot 2^{-k}) / \pi^2$$

$t' = 5t + O(k^2 \cdot l + k^5)$, where l and k are security parameters.

Proof. The proof is similar to that of [7] and [8] .

5. Summary

In this paper, we first propose a novel method to compute a quintic root of a quintic residue. Then, we construct an efficient identity-based signature scheme from quintic residues. Finally, we formally prove that our scheme is secure against existential forgery on the adaptive chosen message and identity attacks assuming the hardness of factoring.

Acknowledgement

This research is supported by the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

1. A. Shamir, Identity based cryptosystems and signature schemes, Advance in Cryptology-Crypto'84,LNCS 196, (Springer-Verlag,1984) pp.47-53.
2. D. Boneh, M. Franklin, Identity-based encryption from Weil pairing, Advance in Cryptology-CRYPTO 2001, LNCS 2193, (Springer-Verlag,2001) pp.213-229.
3. S.Saeednia, An identity-based society oriented signature scheme with anonymous signers, Information Processing Letters, **83(3)**, 295-299(2002).
4. Z. Shao, Cryptanalysis of "an identity-based society oriented signature scheme with anonymous signers", Information Processing Letters, **86(6)**, 295-298(2003).
5. W. B. Lee, K. C. Liao, Constructing identity-based cryptosystems for discrete logarithm based cryptosystems, Journal of Network and Computer Applications, **27**, 191-199(2004).
6. W. D. Qiu, K. F. Chen , Identity oriented based on quadratic residues, Applied Mathematics and Computation, **168**, 235-242(2005).
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, **50(3)**, 373-380(2007).
8. 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(1)**, 33-38(2012).
9. X.D. Dong and X.X. Liu, A modified identity-based signature scheme based on cubic residues, Advances in Computer Science Research,**39,** 1039-1043(2015).