A New Signature Scheme Based on Cubic Residues

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

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

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

Keywords: Cryptography; Cubic residue; Digital signature

Abstract. Shao et al.'s proposed the first provably secure signature scheme based on both factoring and discrete logarithms by using quadratic residues in 2014. The scheme incorporates both the Schnorr signature scheme and the PSS-Rabin signature scheme. Noting that the computational efficiency of constructing a cubic residue is better than constructing a quadratic residue if one selects proper parameters, we propose a new signature scheme by using cubic residues in order to improve the efficiency.

Introduction

Most public key cryptographic cryptosystems were proposed based on the assumption of one mathematic hard problem, discrete logarithms or integer factorization. If the hard problem becomes easy to be solved, the corresponding cryptosystem will no longer be secure. Several signature schemes were proposed based on the two mathematic hard problems in order to enhance security [1, 2, 3, 4, 5, 6]. C.-S. Laih and W.-C. Kuo [7] proposed a signature scheme based on factoring and discrete logarithms in 1997. However, their schemes require many keys for a signing document. L.-H. Li, S.-F. Tzeng and M.-S.Hwang [8] improved C.-S. Laih and W.-C. Kuo's signature scheme in 2005.Zhang et al. [6] proposed an improved scheme of [8] and claimed that the scheme is provably secure in the radom oracle model. But their proof has not showed that a forgery can be used to solve any given integer factorization problem and any given discrete logarithm problem simultaneously. In fact, the Pollard-Schnorr algorithm [9] can easily forge the signature for any message if the discrete logarithm problem is solved. Recently, Shao et al.'s [10] proposed the first provably secure signature scheme based on integer factoring and discrete logarithms simultaneously by combining the Schnorr signature scheme and the PSS-Rabin signature scheme. It was shown that the new scheme is strong existentially unforgeable under adaptive chosen-message attacks in the random oracle model. Shao et al.'s scheme was constructed by using quadratic residues. In this paper we propose a new signature scheme based on cubic residue. 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 chosen message attacks under assumption of the hardness of integer factorization and discrete logarithms. The rest of the paper is organized as follows. In Section 2, we give a brief review of Shao et al.'s scheme. In Section 3, a new signature scheme based on cubic residues is proposed.

Brief Review of Shao et al.'s Scheme

Shao et al.'s scheme is composed of 3 algorithms, called the key generation algorithm, the signing algorithm and the verification algorithm.

The Key Generation Algorithm. The authority chooses the public parameters: p is a large prime number, q is a prime divisor of $p-1$, g is an element of order q in the group Z_p . Each signer chooses an element x in Z_q , two larger prime numbers, p_1 and q_1 ,and computes $n = p_1 q_1, y \equiv g^x \bmod p$, where $p_1 \equiv 3(\text{mod}4),\ \ q_1 \equiv 3(\text{mod}4)$. And then he chooses a random a satisfying Jacobi symbol $\left(\frac{a}{n}\right) = -1$.

$H:\{0,1\}^{å}\times Z_p \to Z_n$ is a one-way hash function. The private key of the signer is (x, p_1, q_1) , and the public key is (p, q, g, y, n, a, H).

The Signing Algorithm. For a message $m \in \{0,1\}^*$ to be signed, the signer chooses a new random integer $k, 1 < k < q,$ computes $r \equiv g^k \bmod p, s = k - H(m,r)x \bmod q,$ and computes c_1 and c_2, respectively. $c_1 = \begin{cases} 0, & if \left(\frac{H(m,r)}{n}\right) = 1 \\ 1, & if \left(\frac{H(m,r)}{n}\right) = -1 \end{cases}$, $l = a^{c_1} H(m,r)$

$$c_2 = \begin{cases} 0, & if \left(\frac{l}{p_1}\right) = \left(\frac{l}{q_1}\right) = 1 \\ 1, & if \left(\frac{l}{p_1}\right) = \left(\frac{l}{q_1}\right) = -1 \end{cases}$$

Computes e such that $e^2 = (-1)^{c_2} a^{c_1} H(m,r) \bmod n$ by using his private key (x, p_1, q_1) .The signature of the message m is (s, e, c_1, c_2) .

The Verification Algorithm. Any verifier can verify the signature by checking

$$\frac{e^2}{(-1)^{c_2} a^{c_1}} \bmod n = H\left(m, g^s y^{((\frac{e^2}{(-1)^{c_2} a^{c_1}}) \bmod n) \bmod q}\right).$$

The verification equation can be regarded as the variants of either the Schnorr signature or the Rabin signature

New Signature Scheme Based on Cubic Residues

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

Lemma 2. [11] Let $p \equiv 2 \pmod 3$ and $q \equiv 4 \pmod 9$ or $7 \pmod 9$ 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 $N = pq$ than to construct a quadratic residue modulo $N = pq$ 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.[*12] Let $p \equiv 2 \pmod 3$ and $q \equiv 4 \pmod 9$ or $7 \pmod 9$ be primes, $N = pq$ and δ a cubic residue modulo N . Then $\delta^{3d} \equiv \delta \pmod N$ where $d = [2(p-1)(q-1)+3]/9$ if $q \equiv 4 \pmod 9$ and $d = [(p-1)(q-1)+3]/9$ if $q \equiv 7 \pmod 9$.

A 3^l th root of δ could be efficiently computed as $\tau = \delta^{d^l} \pmod N$. We now propose a new signature scheme based on cubic residues. The scheme is composed of 3 algorithms, called the key generation algorithm, the signing algorithm and the verification algorithm.

The Key Generation Algorithm. The authority chooses the public parameters: p is a large prime number, q is a prime divisor of $p-1$, g is an element of order q in the group Z_p . Each signer

chooses an element x in Z_q, two larger prime numbers, p_1 and q_1, and computes $n = p_1 q_1, y \equiv g^x \bmod p$, where $p_1 \equiv 2(\bmod 3)$ and $q_1 \equiv 4(\bmod 9)$ or $7(\bmod 9)$. And then she/he chooses a random $0 \neq a \in Z_{q_1}$ satisfying $a^{(q_1-1)/3} \neq 1(\bmod q_1)$, that is, a is not a cubic residue modulo $n = p_1 q_1$ by Lemma 1 and Lemma 2. $H : \{0,1\}^* \times Z_p \to Z_n^*$ is a one-way hash function. The private key of the signer is (x, p_1, q_1), and the public key is (p, q, g, y, n, a, H).

The Signing Algorithm. For a message $m \in \{0,1\}^*$ to be signed, the signer chooses a new random integer $k, 1 < k < q,$ computes $r \equiv g^k \bmod p, s = k - H(m,r)x \bmod q.$ Let $\beta = (q_1 - 1)/3, \omega = H(m,r)^\beta (\bmod q_1),$

$\xi = a^\beta (\bmod q_1).$ The signer computes c as follows.

$$c = \begin{cases} 0, & \omega = 1 \\ 2, & \omega = \xi \\ 1, & \omega = \xi^2 \end{cases}$$

Remark 1. $\omega = 1$ or $\omega = \xi$ or $\omega = \xi^2$ .In fact, $\xi^3 = a^{3\beta} \equiv a^{q_1 - 1} \equiv 1(\bmod q_1)$ by Euler theorem. Similarly, $\omega^3 = H(m,r)^{3\beta} \equiv H(m,r)^{q_1 - 1} \equiv 1(\bmod q_1)$. Thus, $\langle \omega \rangle = \{1, \omega, \omega^2\}$ and $\langle \xi \rangle = \{1, \xi, \xi^2\}$ are both a cyclic group with order 3 in $Z_{q_1}^*$. However, the cyclic group with order 3 in $Z_{q_1}^*$ is the same. Therefore, $\omega = 1$ or $\omega = \xi$ or $\omega = \xi^2$.

Compute $V = a^c H(m,r)(\bmod n)$. Let $e = V^d (\bmod n)$, where $d = [2(p_1 - 1)(q_1 - 1) + 3]/9$ if $q_1 \equiv 4(\bmod 9)$ and $d = [(p_1 - 1)(q_1 - 1) + 3]/9$ if $q_1 \equiv 7(\bmod 9)$. The signature of the message $m \in \{0,1\}^*$ is (s, e, c).

Remark 2. $V = a^c H(m,r)(\bmod n)$ is a cubic residue modulo n. In fact, $V^{(q_1-1)/3} = \xi^c \omega \equiv 1(\bmod q_1)$. Therefore, $V = a^c H(m,r)(\bmod n)$ is a cubic residue modulo n by Lemma 1 and Lemma 2.

The Verification Algorithm. Any verifier can verify the signature by checking

$$\frac{e^3}{a^c}(\bmod n) = H\left(m, g^s y^{((\frac{e^3}{a^c}) \bmod n) \bmod q} (\bmod p)\right).$$

Remark 3. Since $V = a^c H(m,r)(\bmod n)$ is a cubic residue modulo n, $e^3 = V^{3d} \equiv V \equiv a^c H(m,r)(\bmod n)$ by Theorem 1, $\frac{e^3}{a^c}(\bmod n) = H\left(m, g^s y^{((\frac{e^3}{a^c}) \bmod n) \bmod q} (\bmod p)\right)$ if and only if the signature is valid.

Summary

Using a novel method to compute a cubic root of a cubic residue, we have proposed a new signature scheme. Under assumption of the hardness of discrete logarithm and integer factorization, our scheme can be shown to be existentially unforgeable against chosen message attacks in the random oracle model as in [10]. The proposed scheme is more efficient than existing schemes in terms of computational cost.

Acknowledgements

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

References

[1] W.-H. He, Digital signature schemes based on factoring and discrete logarithms, Electronics Letters, 37 (2001), 220-222.

[2] Z. Shao, Comment on signature schemes based on factoring and discrete logarithms, Electronics Letters, 38 (2002), 1518-1519.

[3] H. Qian, Z. Cao, H. Bao, Cryptanalysis of Li-Tzeng-Hwang's of improved signature scheme based on factoring and discrete logarithms, Applied Mathematics and Computation, 166 (2005), 501-505.

[4] Z. Shao, Security of a new digital signature scheme based on factoring and discrete logarithms, Computer Mathematics, 82 (2005), 1215-1219.

[5] E. S. Ismail, N. M. F. Tahat and R. R. Ahmad, A new digital signature schemes based on factoring and discrete logarithms, Journal of mathematics and statistics, 4 (2008), 223-226.

[6] J. Zhang, Q. Geng and S. Gao, Cryptanalysis of a digital signature scheme based on factoring and discrete logarithms, Journal of computational information systems, 5 (2009), 1193-1200.

[7] C.-S. Laih and W.-C. Kuo, New signature scheme based on factoring and discrete logarithms, IEICE Transaction on Fundamentals on Cryptography and Information Security,E80-A 1 (1997), 46-53.

[8] L.-H.Li, S.-F. Tzeng,M.-S.Hwang, Improvement of signature scheme based on factoring and discrete logarithms, Applied Mathematics and Computation, 161 (2005),49-54.

[9] J. M. Pollard and C. Schnorr, An efficient solution of the congruence $x^2 + ky^2 = m(\mathrm{mod}\, n)$, IEEE Trans., IT-33(1987), 702-709.

[10] Z. Shao and Y. Gao, A provably secure signature scheme based on factoring and discrete logarithms, Appl. Math. Inf. Sci. 8(2014), No. 4, 1553-1558.

[11] 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.

[12] X. Dong X. Liu, A modified identity-based signature scheme based on cubic residues, Proceedings of 4th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering, 1039-1043(2015),Atlantis Press.