Certificate-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; Certificate-based

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

Introduction

In 1984, Shamir [1] introduced the concept of identity-based cryptography (IBC) to solve the certificate management problem. In an identity-based signature scheme, an entity's public key is derived directly from its identity, such as identity number, email address, and IP address associated with a user. Private keys are generated for users by a trusted third party called private key generator (PKG). Although IBC eliminates the need for certificates, the key escrow problem is inherent. Because the PKG knows any user's private key, it may impersonate any user or decrypt any cipher texts. Moreover, the users' private keys must be sent over secure channels. Kang et al.[2] proposed the security notion of certificate-based signature (CBS). They also proposed two concrete certificate-based signature schemes and a certificate-based proxy signature scheme. Unfortunately, Li et al. [3] pointed out that one of their schemes was insecure against key replacement attack and proposed a new efficient certificate-based signature scheme. Li et al. [4,5] presented a forward-secure certificate-based signature scheme and a certificate-based key-insulated signature respectively. Nevertheless, the above schemes require pairing operations. The pairing computation is considered as expensive comparing with normal operations such as modular exponentiations in finite fields. Research on cryptography protocol without pairing is mainly focused on certificateless encryption. In 2005, Baek et al. [6] proposed the first certificate-less encryption scheme without pairing. Unfortunately, their scheme exists one drawback that the security proof only holds for a weaker security model in which the Type I adversary is not allowed to replace the public key associated with the challenge identity. Sun et al. [7] eliminated this limitation and constructed a strongly secure certificate-less encryption scheme without pairing. Selvi et al. [8] constructed an efficient certificate-less sign-cryption scheme without pairing. However, certificate-less encryption scheme suffers from the denial of decryption (DoD) attack. In order to solve the above problem, Lai and Kou [9] proposed a self-generated-certificate public key encryption without pairing, which captured the DoD Attack. Liu et al. [10] first proposed a certificated-based signature scheme without pairings and another certificate-based signature scheme whose security can be proven in the standard model. However, Zhang [11] showed that the scheme without pairings was insecure and gave an improved scheme with pairings. Ming and Wang [12] proposed a certificate-based signature scheme without pairings. Li et al. [13] showed that the scheme is subject to universal forgery for a Type II adversary and constructed a new certificate-based signature scheme. Under the discrete logarithm assumption, the scheme is existentially unforgeable against adaptive chosen message and identity attacks in the random oracle model. Recently, Rong et al. [14] proposed a certificate-based signature scheme. The scheme does not need any bilinear pairing computation, just needs compute Jacobi symbol, quadratic residue and power exponentiation. In this paper we propose a new certificate-based 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 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 Rong et al.'s scheme. In Section 3, a certificate-based signature scheme based on cubic residues is proposed.

Brief Review of Rong et al.'s Scheme

Rong et al.'s scheme is composed of 5 algorithms, called Setup, *UserKeyGen, CertGen,Sign and Verify.*

Setup: Generate two primes p_{CA} and q_{CA} such that $p_{CA} \equiv 3 \bmod 4$ and $q_{CA} \equiv 3 \bmod 4$, then compute $N_{CA} = p_{CA} q_{CA}$. Choose a secure hash function $H_1 : \{0,1\}^{å} \to Z_{CA}$ and a random integer a such that Jacobi symbol $\left(\frac{a}{N_{CA}}\right) = -1$. The system public parameters are *params* $\{N_{CA}, a, H_1\}$ and master secret key is $\{p_{CA}, q_{CA}\}$.

UserKeyGen: Given *params*, select a random user private key $usk_{ID} = \{p_{ID}, q_{ID}\}$ such that $p_{ID} \equiv 3 \bmod 4$ and $q_{ID} \equiv 3 \bmod 4$, and compute the user public key $PK_{ID} = N_{ID} = p_{ID} q_{ID}$. Then choose a secure hash functions $H_2 : \{0,1\}^{å} \to Z_{ID}$ and a random integer b such that Jacobi symbol $(\frac{b}{N_{ID}}) = -1$. Publish $\{N_{ID}, b, H_2\}$.

CertGen: Given public parameters $\{N_{CA}, a, H_1\}$ and master secret key $\{p_{CA}, q_{CA}\}$, user identity ID and user public key N_{ID}. Compute $h_1 = H_1(N_{ID} \| ID)$:

$$U_0 = \begin{cases} 0, & \text{if } (\frac{h_1}{N_{CA}}) = 1 \\ 1, & \text{if } (\frac{h_1}{N_{CA}}) = -1 \end{cases} \qquad V_0 = \begin{cases} 0, & \text{if } (\frac{a^{U_0} h_1}{p_{CA}}) = (\frac{a^{U_0} h_1}{q_{CA}}) = 1 \\ 1, & \text{if } (\frac{a^{U_0} h_1}{p_{CA}}) = (\frac{a^{U_0} h_1}{q_{CA}}) = -1 \end{cases}$$

Then compute $Cert_{ID}$ such that $Cert_{ID}^2 \equiv (-1)^{V_0} a^{U_0} h_1 \bmod N_{CA}$ and send $\{Cert_{ID}, U_0, V_0\}$ to the user with the identity ID.

Sign: For message $m \in \{0,1\}^{å}$, choose a random number $0 < r < N_{CA}$ and compute $R \equiv r^2 \bmod N_{CA}, h_2 = H_2(N_{ID} \| ID \| m \| R)$

$$U_1 = \begin{cases} 0, & \text{if } (\frac{h_2}{N_{ID}}) = 1 \\ 1, & \text{if } (\frac{h_2}{N_{ID}}) = -1 \end{cases} \qquad V_1 = \begin{cases} 0, & \text{if } (\frac{b^{U_1} h_2}{p_{ID}}) = (\frac{a^{U_1} h_2}{q_{ID}}) = 1 \\ 1, & \text{if } (\frac{b^{U_1} h_2}{p_{ID}}) = (\frac{a^{U_1} h_2}{q_{ID}}) = -1 \end{cases}$$

The user with the identity ID computes $r_1 \equiv r Cert_{ID}^{h_2} \bmod N_{ID}$ and computes $r_2^2 \equiv (-1)^{V_1} b^{U_1} h_2 \bmod N_{ID}$. Then send $\delta = \{r_1, r_2, U_1, V_1, U_0, V_0\}$ to verifiers.

Verify: Given message and signature pair (m, δ), a verifier first computes $R_1 = r_1^2, R_2 = r_2^2$, $h_2^{'} \equiv R_2((-1)^{V_1} b^{U_1})^{-1} \bmod N_{ID}$, and then computes $R^{'} \equiv R_1((-1)^{U_0} a^{V_0} h_1)^{-h_2^{'}} \bmod N_{CA}$. Finally, checks the equation $H_2(N_{ID} \| ID \| m \| R^{'}) = h_2^{'}$. If the equality holds, output accept; otherwise, reject.

Certificate-based 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. [8] Suppose that $3 \mid (p-1)$. Then a is a 3th residue modulo p if and only if $a^{(p-1)/3} \equiv 1 \pmod{p}$.

Lemma 2. [8] 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.[17] 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 certificate-based signature scheme based on cubic residues. The scheme is composed of 5 algorithms, called *Setup, UserKeyGen, CertGen,Sign and Verify*.

Setup: The algorithm takes in security parameters (k, l).Generate two primes p_{CA} and q_{CA} such that $p_{CA} \equiv 2 \pmod 3$ and $q_{CA} \equiv 4 \pmod 9$ or $7 \pmod 9$, satisfying $p_{CA} q_{CA} < 2^k$, then compute $N_{CA} = p_{CA} q_{CA}$.Choose a secure hash function $H_1 : \{0,1\}^{\text{å}} \to Z_{CA}$ and a random integer a such that $a^{(q-1)/3} \not\equiv 1 \pmod q$. Let $\beta = (q-1)/3$, and $\xi = a^{\beta} \pmod q$ .The system public parameters are $params\{N_{CA}, a, H_1\}$ and master secret key is $\{p_{CA}, q_{CA}\}$.

UserKeyGen: Given *params*, select a random user private key $usk_{ID} = \{p_{ID}, q_{ID}\}$ such that $p_{ID} \equiv 2 \pmod 3$ and $q_{ID} \equiv 4 \pmod 9$ or $7 \pmod 9$ satisfying $N_{ID} = p_{ID} q_{ID} < N_{CA}$. The user public key is $PK_{ID} = N_{ID}$. Then choose a secure hash functions $H_2 : \{0,1\}^{\text{å}} \to Z_{ID}$ and a random integer b such that $b^{(q-1)/3} \not\equiv 1 \pmod q$. Publish $\{N_{ID}, b, H_2\}$.

CertGen: Given public parameters $\{N_{CA}, a, H_1\}$ and master secret key $\{p_{CA}, q_{CA}\}$, user identity ID and user public key N_{ID}. Compute $h_1 = H_1(N_{ID} \| ID)$, $\omega = h_1^{\beta} \pmod q$ .Compute

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

and compute $V = a^c h_1 \pmod{N_{CA}}$. Then compute $Cert_{ID} \equiv V^{d^l} \bmod N_{CA}$,where d as in Theorem Send $\{Cert_{ID}, c\}$ to the user with the identity ID.

Remark 1. V is a cubic residue modulo N_{CA} [17].

Sign: For message $m \in \{0,1\}^{\text{å}}$, choose a random number $0 < r < N_{CA}$ and compute $R \equiv r^{3^l} \bmod N_{CA}, h_2 = H_2(N_{ID} \| ID \| m \| R)$. Let $\omega_1 = h_2^{\beta} \pmod q, \xi_1 = b^{\beta}$.

Compute $c_1 = \begin{cases} 0, & \omega_1 = 1 \\ 2, & \omega_1 = \xi_1 \\ 1, & \omega_1 = \xi_1^2 \end{cases}$

and compute $V_1 = b^{c_1} h_2 (\mathrm{mod}\, N_{ID})$.

The user with the identity *ID* computes $r_1 \equiv rCert_{ID}^{h_2} \bmod N_{CA}$ and computes $r_2 \equiv V_1^{d'} \bmod N_{ID}$. Then send $\delta = \{r_1, r_2, c, c_1\}$ to verifiers.

Verify: Given message and signature pair (m, δ), a verifier first computes $R_1 \equiv r_1^{3^l} \bmod N_{CA}, R_2 \equiv r_2^{3^l} \bmod N_{ID}$, $h_2' \equiv R_2 (b^{c_1})^{-1} \bmod N_{ID}$, and then computes $R' \equiv R_1 (a^c h_1)^{-h_2'} \bmod N_{CA}$. Finally, checks the equation $H_2(N_{ID} \| ID \| m \| R') = h_2'$. If the equality holds, output accept; otherwise, reject.

Remark 2. Since $V_1^{\beta} = (b^{c_1} h_2)^{\beta} \equiv b^{c_1 \beta} \omega_1 \equiv \xi_1^{c_1} \omega_1 \equiv 1 (mod q_{ID})$, it is a cubic residue modulo N_{ID}. By Theorem1 $V_1^{3^l d^l} \equiv V_1 mod N_{ID}$. $h_2' \equiv R_2 (b^{c_1})^{-1} \equiv V_1^{3^l d^l} (b^{c_1})^{-1} \equiv V_1 (b^{c_1})^{-1} \equiv h_2 mod N_{ID} = h_2$, $R' \equiv R_1 ((a^c h_1)^{-h_2'} \equiv r_1^{3^l} V^{-h_2'} \equiv (rCert_{ID}^{h_2})^{3^l} V^{-h_2'} \equiv r^{3^l} V^{3^l d^l h_2} V^{-h_2'} \equiv r^{3^l} mod N_{CA} = R$ .Thus $H_2(N_{ID} \| ID \| m \| R') = h_2'$ if and only if the signature is valid.

Concluding remarks

Using a novel method to compute a cubic root of a cubic residue, we have proposed a new certificate-based signature scheme based on cubic residue. Under assumption of the hardness of integer factorization, our scheme can be shown to be existentially unforgeable against adaptive chosen message and identity attacks in the random oracle model as in [15]. Compared with [15], our scheme enjoys less operation cost.

Acknowledgement

This research was financially supported by the National Natural Sciences Foundation of China under Project Code 10171042 and the Research Project of Liaoning Education Bureau under Project Code L2014490.

References

[1] A. Shamir, Identity-based cryptosystems and signature schemes, in: G.R. Blakely, D. Chaum(Eds.), CRYPTO 1984, vol. 196, LNCS, 1985, pp. 47-53.

[2] B.G. Kang, J.H. Park, S.G. Hahn, A certificate-based signature scheme, in: T. Okamato (Ed.), CT-RSA, 2004, LNCS, vol. 2964, 2004, pp. 99-111.

[3] J.G. Li, X.Y. Huang, Y. Mu, W. Susilo, Q.H. Wu, Certificate-based signature: security model andefficient construction, in: J. Lopez, P. Samarati, J.L. Ferrer (Eds.), EuroPKI 2007, LNCS, vol. 4582, 2007, pp. 110-125.

[4] J.G. Li, Y.C. Zhang, H.Y. Teng, A forward-secure certificate-based signature scheme in the standard model, in: Y. Xiang et al. (Eds.), CSS 2012, LNCS, vol. 7672, 2012, pp. 362-376.

[5] H.T. Du, J.G. Li, Y.C. Zhang, T. Li, Y.X. Zhang, Certificate-based key-insulated signature, in: Y. Xiang et al. (Eds.), ICDKE 2012, LNCS, vol. 7646, 2012, pp. 493-507.

[6] J. Baek, R. Safavi-Naini, W. Susilo, Certificateless public key encryption without pairing, in: J. Zhou et al. (Eds.), ISC 2005, LNCS, vol. 3650, 2005, pp. 134- 148.

[7] Y.X. Sun, F.T. Zhang, J. Baek, Strongly secure certificateless public key encryption without pairing, in: F. Bao et al. (Eds.), CANS 2007, LNCS, vol. 4856, 2007, pp. 194-208.

[8] S. Selvi, S. Vivek, C. Rangan, Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing, in: F. Bao et al. (Eds.), Inscrypt 2009, LNCS, vol. 6151, 2010,pp. 75-92.

[9] J.Z. Lai, W.D. Kou, Self-generated-certificate public key encryption without pairing, in: T. Okamoto, X. Wang (Eds.), PKC 2007, LNCS, vol. 4450, 2007, pp. 476-489.

[10] J.K. Liu, J. Baek, W. Susilo, J. Zhou, Certificate-based signature scheme without pairings or

random oracles, in: T.C. Wu et al. (Eds.), ISC 2008, LNCS, vol. 5222, 2008, pp. 285-297.

[11] J.G. Li, X.Y. Huang, Y.C. Zhang, L.Z. Xu, An efficient short certificate-based signature scheme,Journal of Systems and Software vol.85 (2),2012, pp.314-322.

[12] M.H. Au, J.K. Liu, W. Susilo, T.H. Yuen, Certificate based (linkable) ring signature, in: E. Dawson,D.S. Wong (Eds.), ISPEC 2007, LNCS, vol. 4464, 2007, pp. 79-92.

[13] Y. Ming, Y. Wang, Efficient certificate-based signature scheme, IAS 2009, vol.2, IEEE, 2009, pp. 87-90.

[14] J. Li, Z. Wang, Y. Zhang, Provably secure certificate-based signature scheme without pairings, Information Sciences, vol.233, 2013, pp.313-320.

[15] W.Rong, Y.Guo, Z.Huang, Certificate-based signature scheme from factorization. Computer Engineering and Applications, vol.50 (11),2014, pp.75-80.

[16] 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,

vol.14, 2012, pp.33-38.

[17] X. Dong, X. Liu, A Modified Identity-based Signature Scheme Based on Cubic Residues, the proceeding of The 6th International Conference on Information Technology and Advanced Materials Engineering, November 14-15, 2015, Sanya, Hainan, China.