

A Certificateless Signature Scheme Based on Quadratic Residues

Xuedong Dong^{1,a,*}, Shuo Han^{1,b}, Zhimin Li^{2,c}

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

²College of Computer Engineering, Huaihai Institute of Technology, Lianyungang 222005, P.R.China

^adongxuedong@sina.com, ^b2368082329@qq.com, ^c43161326@qq.com

Keywords: Identity-based cryptography; Certificateless signature scheme; Quadratic residue based cryptography.

Abstract: In the identity-based cryptography, the user's public key can be computed from her/his identity and the user's secret key is generated by the key generation centre. However, the identity-based cryptography suffers from the key escrow problem, i.e. the key generation centre knows all user's secret keys. This paper proposes a certificateless signature scheme based on quadratic residues. In this scheme, a user's private key is a combination of a partial private key generated by the key generation centre and a secret value chosen by the user. Then the key escrow problem in the identity-based cryptography is solved. This scheme is secure in the random oracle model under the hardness assumption of computational the problems of discrete logarithm and large integer factorization.

1. Introduction

In traditional public key cryptography, a trusted third party generates a digital certificate for each user. The purpose of the digital certificate is to ensure the binding between the public key and the owner's identity. Thus there is the certificate management problem in the system. To solve the problem, Shamir [1] proposed the identity-based (ID-based) cryptography in which the user's public key can be computed from her/his identity and the user's secret key is generated by the key generation centre (KGC). There is a shortcoming with the key escrow problem in the ID-based cryptography since the KGC knows all user's secret keys. In 2003, Al-Riyami et al. [2] proposed a certificateless signature (CLS) scheme in which a user's private key is a combination of a partial private key generated by the KGC and a secret key chosen by the user. Then the key escrow problem in the ID-based cryptography is solved. In 2009, Du and Wen [3] proposed an efficient and provably-secure CLS scheme from bilinear pairings. In 2011, He et al. [4] proposed a CLS scheme without bilinear pairings; Ma et al. [5] proposed a CLS scheme against key replacement attack also in 2011. Tso et al. [6] proposed a CLS scheme against realistic adversaries. In 2012, Zhang and Mao[7] proposed a RSA-based CLS scheme. In the other direction, Chai et al. [8] gave an ID-based signature scheme based on quadratic residues in which KGC generates all the user's secret keys. Qiu and Chen [9] proposed an identity based signature scheme based on quadratic residue problem. In this scheme there are the trusted authority and the mediated signer. The trusted authority generates the public parameters of the system, the mediated signer and users together produce a signature for a message. In this paper, we present a new CLS scheme based on quadratic residue problem. In this scheme, a user's private key is a combination of a partial private key generated by the KGC and a secret value chosen by the user. Then the key escrow problem is solved. This scheme is secure in the random oracle model under the hardness assumption of computational the problems of discrete logarithm and large integer factorization. The paper is organized as follows. Section 2 gives preliminary results on quadratic residues. In Section 3 a new CLS scheme is proposed. Section 4 gives analysis of security. Finally, we give concluding remarks in Section 5.

2. Preliminaries

Definition 1. If there exists an integer x such that $x^2 \equiv a \pmod{N}$, where $a, N \in \mathbb{Z}$ and $(a, N) = 1$, then a is called a quadratic residue modulo N .

The Jacobi symbol is used to determine whether a is a quadratic residue modulo N or not.

Theorem 1. [8] Suppose that p and q are distinct large prime and $N = pq$, a is a quadratic residue modulo N . Then $a^{2^d} \equiv a \pmod{N}$, where $d = (N - p - q + 5) / 8$.

Thus, a square root of a could be efficiently computed as $\tau = a^d \pmod{N}$. Without knowing the factorization of modulus N one cannot get the square root of a quadratic residue.

The hardness assumption of factoring: Suppose that p and q are distinct large prime and $N = pq$. The factoring problem is always assumed to be (t, ε) -hard in the sense that there is no algorithm that can output p and q with probability over ε in polynomial time t (with respect to some security parameter k).

Besides, let a be a quadratic residue modulo N , and s_1 and s_2 be its two square roots. If $s_1 \neq s_2 \pmod{N}$, then $N = pq$ can be factored by computing $(s_1 + s_2, N)$ or $(s_1 - s_2, N)$.

The hardness assumption of the discrete logarithm problem (DLP): Let G be cyclic multiplicative group of prime order q , g a generator of any order q . given g and g^a , where $1 < a < q$, compute unknown a . It is assumed to be computationally hard by any polynomial-time bounded algorithm to solve the discrete logarithm problem.

3. The Proposed CLS Scheme

3.1 Scheme Description

We now propose a new CLS scheme consisting of the following polynomial-time algorithms.

Setup: The algorithm takes in security parameters (k, l) . KGC generates two distinct large primes $p \equiv 3 \pmod{8}$ and $q \equiv 7 \pmod{8}$, satisfying $pq < 2^k$, then computes $N = pq$. Choose secure hash functions $H_0 : \{0, 1\}^* \rightarrow \mathbb{Z}_N^*$, $H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^l$. The system public parameters are $params \{N, H_0, H_1\}$ and the system secret key is $\{p, q, d\}$, where $d = (N - p - q + 5) / 8$.

Partial Key Extract: For a user with identity id , KGC computes $H_0(id)$. If $(\frac{H_0(id)}{N}) = -1$, let $c = 1$. If $(\frac{H_0(id)}{N}) = 1$, let $c = 0$. c is called the tag of the user with identity id . For convenience of computation, a user with identity id should bind the id with the user's tag c . KGC calculates $d_{id} = [2^c H_0(id)]^d \pmod{N}$ as the partial private key of a user with identity id .

Set Secret Value: The user randomly chooses x_{id} and sets it as the secret value.

Set Public Key: For a user with identity id , the public key of the user is $PK_{id} = H_0(id)^{x_{id}} \pmod{N}$.

Set Private Key: For a user with identity id , the private key of the user is (x_{id}, d_{id}) .

Sign: Taking a message m , and system public parameters $params \{N, H_0, H_1\}$, the private key (x_{id}, d_{id}) as inputs, the user gives a signature as follows.

1) The user randomly chooses two numbers t_1 and t_2 , computes $T_1 = [2^c H_0(id)]^{t_1} \pmod{N}$, $T_2 = H_0(id)^{t_2} \pmod{N}$ and $h = H_1(m, id, T_1, T_2, PK_{id})$. If $2 \nmid (t_1 - h)$, then the user reselects two numbers t_1 and t_2 until $(t_1 - h)$ is an odd number.

2) The user computes $W_1 = d_{id}^{t_1 - h} \pmod{N}$ and $W_2 = t_2 - x_{id}h$.

3) The user outputs $\omega = (W_1, W_2, h)$ as the signature of the message m .

Verify: After receiving a signature $\omega = (W_1, W_2, h)$ on the message m from the signer with id , the tag c and public key PK_{id} , a verifier executes in the following way.

1) The verifier computes $T_1' = [2^c H_0(id)]^h W_1^2 \pmod{N}$ and $T_2' = PK_{id}^h H_0(id)^{W_2} \pmod{N}$.

2) The verifier checks whether $H_1(m, id, T_1', T_2', PK_{id})$ and h are equal. If they are equal, the verifier accepts the signature. Otherwise, she/he will reject the signature.

3.2 Correctness Analysis

The correctness of the proposed scheme can be verified as follow:

Let $p \equiv 3 \pmod{8}$ and $q \equiv 7 \pmod{8}$ are distinct large primes and $N = pq$. Then

$$\left(\frac{2}{N}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{q}\right) = -1.$$

That is, 2 is a quadratic nonresidue modulo $N = pq$. If $\left(\frac{H_0(id)}{N}\right) = -1$, let $c = 1$. If

$\left(\frac{H_0(id)}{N}\right) = 1$, let $c = 0$. Then $\left(\frac{2^c H_0(id)}{N}\right) = \left(\frac{2^c}{N}\right)\left(\frac{H_0(id)}{N}\right) = 1$, thus $2^c H_0(id)$ is a quadratic residue modulo $N = pq$.

Therefore, $[2^c H_0(id)]^{2d} \equiv 2^c H_0(id) \pmod{N}$ by Theorem 1. We have $T_1' = [2^c H_0(id)]^h W_1^2 \equiv [2^c H_0(id)]^h d_{id}^{2(t_1-h)} \equiv [2^c H_0(id)]^h [2^c H_0(id)]^{2d(t_1-h)} \equiv [2^c H_0(id)]^{t_1} \pmod{N} = T_1$ since $[2^c H_0(id)]^{2d} \equiv 2^c H_0(id) \pmod{N}$. Moreover

$T_2' = PK_{id}^h H_0(id)^{W_2} \equiv H_0(id)^{hx_{id} + t_2 - x_{id}h} \equiv H_0(id)^{t_2} \pmod{N} = T_2$. Thus, the signature $\omega = (W_1, W_2, h)$ is valid if and only if $H_1(m, id, T_1', T_2', PK_{id}) = h$.

4. Security Analysis

CLS schemes should have confidentiality (under adaptive chosen ciphertext attack) and non-forgery (under adaptive selection message attack). There are two kinds of attackers in a CLS scheme.

Type I Adversary: The attacker A_I can replace a user public key arbitrarily but cannot get the system secret key of KGC. The attacker A_I imitates an illegal user's attack.

Type II Adversary: The attacker A_{II} can get the system secret key of KGC but cannot replace a user public key. The attacker A_{II} mainly imitates KGC which can generate some keys for users.

We now show that the proposed CLS scheme cannot withstand Type I Adversary if $2|(t_1 - h)$ in the above scheme.

Let A_I be a Type I Adversary. If $2|(t_1 - h)$, then A_I can forge a user's legal signature on any message in the following steps.

1) Choose a random number y_{id} and replace the user public key with $PK_{id}' = H_0(id)^{y_{id}} \pmod{N}$.

2) Randomly choose two numbers t_1 and t_2 , computes $T_1 = [2^c H_0(id)]^{t_1} \pmod{N}$ $T_2 = H_0(id)^{t_2} \pmod{N}$ and $h = H_1(m, id, T_1, T_2, PK_{id}')$.

3) If $2|(t_1 - h)$, let $(t_1 - h) = 2s$, compute $W_1 = [2^c H_0(id)]^s \pmod{N}$ and $W_2 = t_2 - y_{id}h$.

4) Output $\omega = (W_1, W_2, h)$ as the signature of the message m .

Note that $T_1' = [2^c H_0(id)]^h W_1^2 \equiv [2^c H_0(id)]^h [2^c H_0(id)]^{2s} \equiv [2^c H_0(id)]^{t_1} \pmod{N} = T_1$ and

$T_2' = (PK_{id}')^h H_0(id)^{W_2} \equiv H_0(id)^{hy_{id} + t_2 - y_{id}h} \equiv H_0(id)^{t_2} \pmod{N} = T_2$. Thus $\omega = (W_1, W_2, h)$ could pass

the verification of any verifier. Therefore A_i can forge a user's legal signature on any message although A_i does not know the system secret key.

If $(t_1 - h)$ is an odd number, we do have the following theorems in the random oracle model under the hardness assumption of computationally large integer factorization.

Theorem 2. Under the adaptive chosen ciphertext attack, the proposed certificateless scheme is confidentiality. Under the adaptive selection message attack, the proposed certificateless scheme is unforgery.

The proof of Theorem 2 is similar to that of Theorem in [7].

Besides, for different messages to be signed, different random numbers t_1 and t_2 should be used. If the same t_2 is chosen for different messages m_1 and m_2 , then secret value x_{id} can be computed from the following equations:

$$\begin{cases} W_2 = t_2 - x_{id}h \\ W_2' = t_2 - x_{id}h' \end{cases}$$

If the same t_1 is chosen for different messages m_1 and m_2 , then

$$[2^c H_0(id)]^h W_1^2 \equiv [2^c H_0(id)]^{h'} W_1'^2 \equiv [2^c H_0(id)]^h (\text{mod } N) = T_1. \text{ Thus, } \frac{W_1'^2}{W_1^2} \equiv \frac{[2^c H_0(id)]^{h'}}{[2^c H_0(id)]^h} (\text{mod } N).$$

If another square root of $\frac{[2^c H_0(id)]^{h'}}{[2^c H_0(id)]^h}$ was found, then $N = pq$ could be factored with a probability of 1/2.

5. Conclusion

Aiming at the problem of key escrow and certificate management, this paper presents a new signature scheme without certificate and linear pairing based on quadratic residues. This scheme binds the message to the user's identity with hash function, ensuring the security of identity and defending the internal attack. Under the hardness assumption of computational the problems of discrete logarithm and large integer factorization. The scheme is secure in the random oracle model.

References

- [1] A. Shamir, "Identity-based cryptosystems and signature schemes," in Proceedings of Crypto '84, pp. 47-53, 1985.
- [2] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in Proceedings of Asiacrypt '03, pp. 452-473, 2003.
- [3] H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," Computer Standards and Interfaces, vol. 31, no. 2, pp. 390-394, 2009.
- [4] D. He, J. Chen, and R. Zhang, "An efficient and provably-secure certificateless signature scheme without bilinear pairings," International Journal of Communication Systems, vol. 25, no. 11, pp. 1432-1442, 2011.
- [5] C. Ma and J. Ao, "Certificateless group oriented signature secure against key replacement attack," International Journal of Network Security, vol. 12, no. 1, pp. 1-6, 2011.
- [6] R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signatures secure against realistic adversaries," Journal of Supercomputing, vol. 55, no. 2, pp. 173-191, 2011.
- [7] J. Zhang and J. Mao, "An efficient RSA-based certificateless signature scheme," Journal of Systems and Software, vol. 85, pp. 638-642, 2012.

- [8] Z.Chai, Z.Cao and X. Dong, “Identity-based signature scheme based on quadratic residues”, *Sci China Ser F-Inf Sci*, vol. 50, pp. 373-380, 2007.
- [9] W. Qiu and K. Chen, “Identity oriented signature scheme based on quadratic residues,” *Applied Mathematics and Computation*, vol. 168, pp. 235-242, 2005.