Advances in Engineering Research (AER), volume 130
5th International Conference on Frontiers of Manufacturing Science and Measuring Technology (FMSMT 2017)

Two Signature Schemes Based on Quintic Residues

Xuedong DONG[a], Yuan GAO[b]

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

[a]email:dongxuedong@sina.com, [b]email : 1069957580@qq.com

Keywords: Cryptography, Quintic residue, Certificate-based signature, Identity-based ring signature, Provable security.

Abstract. We propose a new certificate-based signature scheme and an identity-based ring signature scheme based on quintic residues in order to improve the efficiency of computation. The schemes do not need any bilinear pairing computation which is known to be difficult to computation. The schemes are secure against existential forgery on the adaptive chosen message and identity attacks assuming the hardness of factoring.

Introduction

Many signature schemes require pairing operations. The pairing computation is considered as expensive comparing with normal operations such as modular exponentiations in finite fields.Liu et al. [1] first proposed a certificated-based signature scheme without pairings. However, Zhang [2] showed that the scheme without pairings was insecure and gave an improved scheme with pairings. Ming and Wang [3] proposed a certificate-based signature scheme without pairings. Li et al. [4] 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. Rong et al. [5] 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. Dong et al. [6] proposed a certificate-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. On the other hand, a ring signature can be regarded as a simplified group signature with no manager, no group setup procedure, and no revocation mechanism against signer's anonymity. In a ring signature scheme, the information of all possible signers serves as a part of the ring signature for the signed message. A valid ring signature will convince the verifier that the signature is generated from one of the ring members, without revealing any information about which ring member is the actual signer. In [7], an identity-based ring signature scheme was proposed based on quadratic residues. The proposed signature scheme is more efficient than those which are constructed from bilinear pairings. Dong et al. [8] proposed an identity-based ring signature scheme based on cubic residues. The schemes in [6] and [8] are only suitable for primes p and q, where $p \equiv 2 (\bmod 3)$ and $q \equiv 4 (\bmod 9)$ or $q \equiv 7 (\bmod 9)$ .In [9], we proposed a novel method to compute a quintic root of a quintic residue and then gave a new identity based signature scheme by the method. 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 $q \neq 1 (\bmod 25)$. In this paper we propose a new certificate-based signature scheme and an identity-based ring signature scheme based on quintic residues in order to improve the efficiency of computation. The rest of the paper is organized as follows. In Section 2, we give some preliminaries. In Section 3, a certificate-based signature scheme is proposed based on quintic residues. In Section 4, we give an identity-based ring signature scheme.

Preliminaries

Definition 1[9]. If there exists an integer x such that $x^5 \equiv a(\bmod p)$, where $a \in Z$ and $(a,p)=1$,then a is called a quintic residue modulo p.

Lemma 1[9]. Suppose that $5|(p-1)$. Then a is a quintic residue modulo p if and only if $a^{(p-1)/5} \equiv 1(\bmod p)$.

Lemma 2[9]. If $p \neq 1(\bmod 5)$ and $(a,p)=1$. Then a is a quintic residue modulo p.

Lemma 3[9]. 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 $a(p-1)(q-1)/5 \equiv -1(\bmod 5)$.

Theorem 1[9]. Let $p \neq 1(\bmod 5)$, $q \equiv 1(\bmod 5)$ and $q \neq 1(\bmod 25)$ be primes, $N = pq$, δ a quintic residue modulo q and $(\delta, p)=1$. 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 $\tau = \delta^{d^l}(\bmod N)$.

Remark 1. Without knowing the factorization of modulus N one cannot get the quintic root of a quintic residue.

Certificate-based Signature Scheme Based on Quintic Residues

We now propose a certificate-based signature scheme based on quintic 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 $p_{CA} \neq 1(\bmod 5)$, $q_{CA} \equiv 1(\bmod 5)$ and $q_{CA} \neq 1(\bmod 25)$, satisfying $p_{CA}q_{CA} < 2^k$, then compute $N_{CA} = p_{CA}q_{CA}$.Choose a secure hash function $H_1:\{0,1\}^\star \to Z^*_{N_{CA}}$ and a random integer a such that $a^{(q_{CA}-1)/5} \not\equiv 1(\bmod q_{CA})$ and $(a, p_{CA}) = (a, q_{CA}) = 1$,where $Z^*_{N_{CA}}$ is the multiplicative group of integers modulo N_{CA} **.**Let $\beta = (q_{CA}-1)/5$, and $\xi = a^\beta (\bmod q_{CA})$ .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 $p_{ID} \neq 1(\bmod 5)$, $q_{ID} \equiv 1(\bmod 5)$ and $q_{ID} \neq 1(\bmod 25)$ satisfying $N_{ID} = p_{ID}q_{ID} < N_{CA}$.The user public key is $PK_{ID} = N_{ID}$. Then choose a secure hash functions $H_2:\{0,1\}^\star \to Z^*_{N_{ID}}$ and a random integer b such that $b^{(q_{ID}-1)/5} \not\equiv 1(\bmod q_{ID})$ and $(b, p_{ID}) = (b, q_{ID}) = 1$. 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 $h_1 = H_1(N_{ID} \| ID)$, $\omega = h_1^\beta (\bmod q_{CA})$.

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 $V = a^c h_1 (\bmod N_{CA})$. Then compute $Cert_{ID} \equiv V^{d^l} \bmod N_{CA}$,

where $d = [s(p_{CA}-1)(q_{CA}-1)+5]/25$, and $s(p_{CA}-1)(q_{CA}-1)/5 \equiv -1(\bmod 5)$ as in Theorem 1. Send $\{Cert_{ID}, c\}$ to the user with the identity ID.

Remark 2. Since $\omega^5 = 1(\bmod q_{CA})$, the subgroup generated by ω and the subgroup generated by ξ are both the cyclic group with order 5 in the finite field $Z_{q_{CA}}$ .Therefore, we have $\omega = \xi^i$ for some $0 \le i \le 4$.

Remark 3. V is a quintic residue modulo p_{CA} and q_{CA}.

In fact, $V^{(q_{CA}-1)/5}=V^{\beta}=a^{c\beta}h_1^{\beta}=\xi^c\omega=1(\bmod q_{CA})$. Thus, by Lemma 1 V is a quintic residue modulo q_{CA}. Since $p_{CA}\neq 1(\bmod 5)$, by Lemma 2 V must be a quintic residue modulo p_{CA}.

Sign: For message $m\in\{0,1\}^{\star}$, choose a random number $0<r<N_{CA}$ and compute $R\equiv r^{5^l}\bmod N_{CA}$, $h_2=H_2(N_{ID}\,||\,ID\,||\,m\,||\,R)$.

Let $\omega_1=h_2^{\beta_1}(\bmod q_{ID}),\xi_1=b^{\beta_1}$, where $\beta_1=(q_{ID}-1)/5$.

Compute $c_1=\begin{cases}0,\omega_1=1\\1,\omega_1=\xi_1^4\\2,\omega_1=\xi_1^3\\3,\omega_1=\xi_1^2\\4,\omega_1=\xi_1\end{cases}$ and compute $V_1=b^{c_1}h_2(\bmod N_{ID})$.

The user with the identity ID computes $r_1\equiv rCert_{ID}^{h_2}\bmod N_{CA}$ and computes $r_2\equiv V_1^{w^l}\bmod N_{ID}$, where $w=[t(p_{ID}-1)(q_{ID}-1)+5]/25$ and $t(p_{ID}-1)(q_{ID}-1)/5\equiv -1(\bmod 5)$ as in Theorem 1.

Then send $\tau=\{r_1,r_2,c,c_1\}$ to verifiers.

Verify: Given message and signature pair (m,τ), a verifier first computes $R_1\equiv r_1^{5^l}\bmod N_{CA}$, $R_2\equiv r_2^{5^l}\bmod N_{ID}$, $h_2^{'}\equiv R_2(b^{c_1})^{-1}\bmod N_{ID}$, 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 4. Since $V_1^{\beta_1}=(b^{c_1}h_2)^{\beta_1}\equiv b^{c_1\beta_1}\omega_1\equiv\xi_1^{c_1}\omega_1\equiv 1(mod q_{ID})$, it is a quintic residue modulo q_{ID}. By Theorem 1 $V_1^{5^l w^l}\equiv V_1 mod N_{ID}$.

$$h_2^{'}\equiv R_2(b^{c_1})^{-1}\equiv V_1^{5^l w^l}(b^{c_1})^{-1}\equiv V_1(b^{c_1})^{-1}\equiv h_2 mod N_{ID}=h_2,$$
$$R^{'}\equiv R_1((a^c h_1)^{-h_2^{'}}\equiv r_1^{5^l}V^{-h_2^{'}}\equiv(rCert_{ID}^{h_2})^{5^l}V^{-h_2^{'}}\equiv r^{5^l}V^{5^l d^l h_2}V^{-h_2^{'}}\equiv r^{5^l}modN_{CA}=R.$$

Thus $H_2(N_{ID}\,||\,ID\,||\,m\,||\,R^{'})=h_2^{'}$ if and only if the signature is valid.

Identity-based Ring Signature Scheme Based on Quintic Residues

We now propose a identity-based ring signature scheme based on quintic residues. The scheme is composed of 5 algorithms, called *Setup, PubKeyGen, SeckeyExt, Sign* and *Verify*.

Setup: The algorithm takes in security parameters (k,l). Private key generator(PKG) generates two primes p and q such that $p\neq 1(\bmod 5)$, $q\equiv 1(\bmod 5)$ and $q\neq 1(\bmod 25)$, satisfying $pq<2^k$, then compute $N=pq$. Choose secure hash functions $H_1:\{0,1\}^{\star}\to Z_N^{\star}$, $H_2:\{0,1\}^{\star}\to\{0,1\}^t$, and a random integer a such that $a^{(q-1)/5}\not\equiv 1(\bmod q)$ and $(a,p)=(a,q)=1$. Let $\beta=(q-1)/5$, and $\xi=a^{\beta}(modq)$. The system public parameters are *params* $\{N,a,H_1\}$ and master secret key is $\{p,q\}$.

PubKeyGen: Given public parameters $\{N,a,H_1\}$ and ID_U, PKG computes the public key and a tag c as follows:

Compute $h_1=H_1(ID_U)$, $\omega=h_1^{\beta}(\bmod q)$ and $c=\begin{cases}0,\omega=1\\1,\omega=\xi^4\\2,\omega=\xi^3\\3,\omega=\xi^2\\4,\omega=\xi\end{cases}$. A user U with identity ID_U has the public key $PK_{ID_U}=a^c h_1(\bmod N)$. Then compute $Cert_{ID}\equiv V^{d^l}\bmod N$, where $d=[a(p-1)(q-1)+5]/25$ and $a(p-1)(q-1)/5 \equiv -1(\bmod 5)$ as in Theorem 1.Send $\{Cert_{ID}, c\}$ to the user with the identity *ID*.

Remark 5. PK_{ID_U} is a quintic residue modulo p and q.

SeckeyExt: Given PK_{ID_U}, PKG computes the corresponding private key $SK_{ID_U} \equiv PK_{ID_U}^{d^l} \bmod N$ .PKG secretly send $\{SK_{ID_U}, c\}$ to the user with the identity ID_U .

Sign: Let $L=\{ID_1,\cdots,ID_n\}$ be the set of identities of all users and $m \in \{0,1\}^\star$ the message to be signed. The user with identity ID_s gives an identity-based ring signature on behalf of the group L. For ID_i , execute *PubKeyGen* to get $\{PK_{ID_i}, c_i\}$. Choose random numbers $0<r_i<N$ and compute $R_i \equiv r_i^{5^l} \bmod N, h_i = H_2(L \| m \| R_i)$ for $i \in \{1,\cdots,n\}-\{s\}$. Choose random numbers $0<r_s<N$ and compute $R_s^\star \equiv r_s^{5^l} \bmod N, h_s^\star = H_2(L \| m \| R_s^\star)$ and $R_s \equiv PK_{ID_s}^{h_s^\star} \prod_{i \neq s} (R_i PK_{ID_i}^{h_i})^{-1} \bmod N$. Compute $h_s = H_2(L \| m \| R_s)$ and $V=(SK_{ID_s})^{h_s+h_s^\star} \bmod N$. The returned ring signature is $\sigma=\{L,m,V,\bigcup_{i=1}^n R_i\}$.

Verify: A verifier can check the validity of the signature pair $\sigma=\{L,m,V,\bigcup_{i=1}^n R_i\}$ as follows.

For ID_i, execute *PubKeyGen* to get $\{PK_{ID_i}, c_i\}$. Compute $h_i = H_2(L \| m \| R_i)$ for $i \in \{1,\cdots,n\}$. Finally, checks the equation $V^{5^l} \equiv \prod_{i=1}^n (R_i PK_{ID_i}^{h_i}) \bmod N$. If the equality holds, output accept; otherwise, reject.

*Remark 6.*Since $PK_{ID_s}^{\beta} = (a^c h_1)^\beta \equiv a^{c\beta}\omega \equiv \xi^c \omega \equiv 1(\bmod q)$, it is a quintic residue modulo q. By Theorem 1, $PK_{ID_s}^{5^l d^l} \equiv PK_{ID_s} \bmod N$ and $V^{5^l} \equiv (SK_{ID_s})^{5^l h_s + 5^l h_s^\star} \equiv PK_{ID_s}^{d^l 5^l (h_s+h_s^\star)} \equiv PK_{ID_s}^{h_s+h_s^\star} \equiv PK_{ID_s}^{h_s} PK_{ID_s}^{h_s^\star} \equiv$

So, $PK_{ID_s}^{h_s} R_s \prod_{i \neq s} (R_i PK_{ID_i}^{h_i}) \equiv \prod_{i=1}^n (R_i PK_{ID_i}^{h_i}) \bmod N$. Thus, $V^{5^l} \equiv \bigcup_{i=1}^n (R_i PK_{ID_i}^{h_i}) \bmod N$ if and only if the signature is valid.

Summary

In this paper, we propose a new certificate-based signature scheme and an identity-based ring signature scheme based on quintic residues without pairing operations. Our schemes improve the efficiency of computation. The schemes are the first certificate-based signature scheme and identity-based ring signature scheme based on quintic residues. As in [8], the schemes satisfy security requirements such as key secrecy and unforgeability. We can formally prove that our schemes are secure against existential forgery on the adaptive chosen message and identity attacks assuming the hardness of factoring.

Acknowledgements

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

References

[1] 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.

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

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

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

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

[6] X. Dong, X. Liu, Certificate-based signature scheme based on cubic residues, Advances in Computer Science Research, Atlantis Press, 2015 (39) 367-371.

[7] H.Xiong, Z.Qin, and F.Li, Identity-based ring signature scheme based on quadratic residues, High Technology Letters, 2009 (15) 94-100.

[8] X. Dong, X. Liu, Identity-based ring signature scheme based on cubic residues, Advances in Computer Science Research, Atlantis Press, 2015 (39) 897-900.

[9] X. Dong, Y. Gao, Identity-based signature scheme based on quintic residues , Proceeding of 2nd Annual International Conference on Electronics, Electrical Engineering and Information Science, December 2-4, 2016, Xi'an, Shanxi, China.