A Public-Key Cryptosystem Scheme on Conic Curves over the Ring Z_n

Zhigang Chen, Xinxia Song, Jifang Li
Computer Science and Information Technology College
Zhejiang Wanli University
No.8 South Qian Hu Road Ningbo
CHINA

Abstract: - A public key cryptosystem scheme is proposed that are based on conic curves over the ring Z_n. Our scheme is motivated by KMOV scheme on elliptic curves, but our scheme remove some restrictive condition from KMOV scheme and constructed on conic curves. Its security bases on the difficulty of factoring a composite number n, just like RSA. It can resist some of the known attacks on RSA. We also constructed digital signature and a proxy signature on our scheme. Since encoding and decoding over conic are easily implement, it has enabled our scheme to greatly enhance efficiency. Also, our schemes can be used in the mobile payment system with the limited bandwidth.

Key-Words: - residue class ring Zn, conic curve, public-key cryptosystem, digital signature, proxy signature

1 Introduction

Since the discovery of public-key cryptography by Diffie and Hellman [1], several attempts have been made to find practical public key systems depending on the difficulty of solving some problems. There are three main families of public key cryptosystems based on computational number theory [2]. The first family includes RSA and related variants (Rabin-Williams, LUC, Dickson, elliptic curve embodiments of RSA-like KMOV). The second family is based on Diffie-Hellman-type schemes (ElGamal and variants, Cramer-Shoup) which exploit properties of exponentiation over finite cyclic groups. Finally, the third family is based on high degree residuosity classes (Goldwasser-Micali, Benaloh, Naccache-Stern, Okamoto-Uchiyama and variants).

In this paper, we propose a public key scheme belonging to this first family. Our scheme based on conic curves over ring Zn. In 1998, after Zhang designed a conic group in literature [4], Cao creatively presented the concept of conic curve cryptography in [3]. Later Cao proposed a conic analog of RSA cryptosystem and some improved RSA cryptosystems in [5]. A important conclusion about cryptosystem based on conic curves in [6] is that the efficiency and the security of the public key cryptosystem based on the DLP in conic curve groups are not stronger than those based on the DLP in finite fields. But an exciting characteristic of conic is both encoding and decoding over conic are easily implemented. As an alternative algebra curve technology, we believe conic deserves the further study in cryptography.

In this paper, we propose a public key cryptosystem scheme on conic curves over the ring Zn. Our scheme is motivated by KMOV scheme [8], but it remove some restrictive condition from KMOV scheme and constructed on conic curves. Its security bases on the difficulty of factoring a composite number n, just like RSA. It can resist some of the known attacks on RSA. We constructed digital signature and a proxy signature on our scheme.

The remainder of the paper is organized as follows. Section 2 gives a short introduction to conic curves over a finite field. In section 3, we show some properties of conic curves over a ring, which are used in the succeeding sections. Section 4 proposes a public key cryptosystem scheme on conic curves over the ring Zn. Section 5 describes the signature scheme. Section 6 discusses the security of the proposed scheme, and Section 7 describes a proxy signature scheme.

2 Conic Curves over a Finite Field

Let p be an odd prime and F_p be a finite field of p elements. Let F_p^* be tile multiplication group of F_p.

Then, without loss of generality, we can assume

$$\mathrm{F}_p = \{0,1,\cdots, p-1\},$$

$$\mathrm{F}_p^* = \mathrm{F}_p \setminus \{0\}.$$

Let us further consider the conic over an affine plane $A^2(\mathrm{F}_p)$,

$$C(\mathrm{F}_p): y^2 = ax^2 - bx, a, b \in \mathrm{F}_p^* \quad (1)$$

Obviously, when $x=0$, we have the origin o(0, 0). If $x\neq 0$, let $t=yx^{-1}$ and fill $y=xt$ in the equation (1). Then, we get

$$x(a-t^2)=b, a, b\in \mathrm{F}_p^*. \quad (2)$$

If $a=t^2$, the equation (2) doesn't hold; If $a\neq t^2$, from the equation (2), we will have

$$\begin{aligned} x&=b(a-t^2)^{-1}\\ y&=bt(a-t^2)^{-1}\end{aligned} \quad (3)$$

where $a,b\in \mathrm{F}_p^*$ and $(\ )^{-1}$ denotes the multiplication inverse in F_p^*.

For any $t\in \mathrm{F}_p$ and $t^2\neq a$, let $P(t)$ be the point (x,y) over $C(\mathrm{F}_p)$ established by the equation (3). Moreover, an ideally defined point o, namely the point at infinity $P(\infty)$, is also recognized as a point over $C(\mathrm{F}_p)$.

Let

$$H=\{t\in \mathrm{F}_p; t^2\neq a\}\cup\{\infty\}$$

then, $P: H\to C(\mathrm{F}_p)$ is a one-to-one map.

According to [4], let us define the addition $\oplus$ of elements in $C(\mathrm{F}_p)$.

$\forall P(t)\in C(\mathrm{F}_p)$ and $t\in H$,such that

$$P(t)\oplus P(\infty)=P(\infty)\oplus P(t) \quad (4)$$

Assume $P(t_1)$, $P(t_2)$ $\in$ $C(\mathrm{F}_p)$,where $t_1, t_2\in H$ and $t_1, t_2\neq\infty$,such that

$$P(t_1)\oplus P(t_2)=P(t_3) \quad (5)$$

where

$$t_3\begin{cases}(t_1t_2+a)(t_1+t_2)^{-1}, t_1+t_2\neq 0,\\ \infty, t_1+t_2=0.\end{cases}$$

Obviously, $t_3\in H$, and operation $\oplus$ is commutative.

Any $P(t)\in C(\mathrm{F}_p)$, negative element

$$\begin{aligned} -P(\infty)&=P(\infty),\\ -P(t)&=P(-t).\end{aligned} \quad (6)$$

And then, from (4) ~ (6), we can easily prove $\forall\ P(t_1), P(t_2), P(t_3)\in C(\mathrm{F}_p)$,

$$(P(t_1)\oplus P(t_2))\oplus P(t_3)=P(t_1)\oplus(P(t_2)\oplus P(t_3)) \quad (7)$$

Therefore, $(C(\mathrm{F}_p),\oplus,P(\infty))$ is a finite abelian group. And $\left|C(\mathrm{F}_p)\right|$ can be defined as,

$$\left|C(\mathrm{F}_p)\right|=\begin{cases}p-1, (\frac{a}{p})=1,\\ p+1, (\frac{a}{p})=-1.\end{cases}$$

where $(\frac{a}{p})$ is Legendre Symbol.

An exciting characteristic of conic is both encoding and decoding over conic are easily implemented. Denote H\{ ∞ } as H*, and assume a message $m\in$ H*, let's demonstrate how to code it.

Encoding:

$$P(m)=(X_m, Y_m),$$

$$\begin{cases}X_m=b(a-m^2)^{-1}(\mathrm{mod}\, n)\\ Y_m=bm(a-m^2)^{-1}(\mathrm{mod}\, n)\end{cases}$$

Decoding:

$$m=Y_m\cdot X_m^{-1}(\mathrm{mod}\ p)$$

3 Conic Curves over the ring Z_n

We now consider conic curves over the ring Z_n, where n is an odd composite squarefree integer.

Similar to the definition of $C_p(a,b)$, an conic curve $C_n(a,b)$ can be defined as the set of pairs $(x,y)\in Z_n^2$ satisfying $y^2\equiv ax^2-bx$ (mod n).

Obviously, $o(0,0)\in C_n(a,b)$. Accord to [7], all the points of $C_n(a,b)$ can be obtained by $C_p(a,b)\times C_q(a,b)$, hence the order of $C_n(a,b)$ can be obtained by the use of $C_p(a,b)$ and $C_q(a,b)$. We have:

Proposition 1: If $(\frac{a}{p})=-1$, $\left|C_n(a,b)\right| = (p+1)(q+1)$.

The proof we refer to [7].

By the map ϕ in [7], the add operation is defined by using of the add operation of conic curve on finite field F_p, i.e. $C_n(a,b)\ \underline{\phi}\ C_p(a,b)\times C_q(a,b)$, for any two points $P, Q\in C_n(a,b)$,

$$P\oplus Q=\phi^{-1}(P_p\oplus Q_p, P_q\oplus Q_q). \quad (8)$$

$(C_n(a,b),\oplus)$ constructs a finite Abel group in [7], where $\oplus$ is defined as equation (8).

Theorem 1: Let A$\in C_n(a,b)$, the order of A is the minimal positive integral k such that kA=0, and denote $o(A)=k$. $\forall A=(x,y)\in C_n(a,b)$,there is a unique point A in $C_p(a,b)\times C_q(a,b)$ response to the point (A_p,A_q) and the order of A

$$o(A)= lcm(o(A_p),o(A_q)).$$

Corollary: let p, q two distinctness large prime and n=pq, such that $(\frac{a}{p})=(\frac{a}{q})=-1$, and $p+1=2r$, $q+1=2s$, where both r and s are prime, then there exist one point G in the curve $C_n(a,b)$, which order $N_n=2rs$.

The above proof can be found in [7].

Theorem 2: Let conic curve $C_n(a,b)$, where $n=pq$ (p,q: prime). Let $N_n=lcm(\#C_p(a,b), \#C_q(a,b))$, then for any $P\in C_n(a,b)$ and any integer k, we have:

$$(k\cdot N_n+1)\cdot P\equiv P \pmod n.$$

Proof: By the above Theorem, for any $P\in C_n(a,b)$, there exist a unique point corresponding (P_p,P_q) in $C_p(a,b)\times C_q(a,b)$, and $o(P)=lcm(o(P_p), o(P_q))$, clear $o(P)\mid N_n$, so we have shown the above identity。

4 A Public Key Cryptosystem Scheme on Conic Curves over the Ring Z_n

In this section, we propose a public key cryptosystem scheme on conic curves over the ring Z_n. Let a, b$\in$ Z_n be two parameters. The conic curves equation, denoted by $y^2\equiv ax^2-bx \pmod n$, satisfy the following condition:

(1) $(a,n)=(b,n)=1$

(2) $n=pq$, where p and q are two large different primes.

(3) $(\frac{a}{p})=(\frac{a}{q})=-1$.

Key Generation: User U chooses large primes p and q. U computes the product $n=pq$, and N_n = $lcm(\#C_p(a,b),\#C_q(a,b))=lcm(p+1,q+1)$. U chooses an integer e which is coprime to N_n, and computes an integer d such that

$$ed\equiv 1 \pmod{N_n}.$$

U 's secret key is d and (p, q, $\#C_p(a,b)$, $\#C_q(a,b)$, N_n). U 's public key is (n,e).

Encryption: A plaintext M =(m_x, m_y) is an integer pair, where $m_x\in Z_n$, $m_y\in Z_n$. Let M =(m_x, m_y) be a point on the conic curve $C_n(a,b)$. Sender A encrypts the point M by encryption function E(•) with the receiver' s public key e and n as

$$C=E(M)=e\cdot M,$$

and sends a ciphertext pair C =(C_x, C_y) to a receiver B.

Decryption: Receiver B decrypts a point C by decryption function D(•) with his secret key d and public key n as

$$M=D(C)=d\cdot C.$$

Because $d\cdot C=d\cdot e\cdot M=(k\cdot N_n+1)\cdot M=M$.

An addition operation on the points of an conic curve over the ring Zn can be defined that makes it into an abelian group. Compared with KMOV scheme on elliptic curves, our scheme is not need special conic curves over the ring Z_n to construct public key cryptosystem. This has enabled our scheme to have a more extensive application. In addition, some operations on the conic curves will be relatively easy, it has enabled our scheme to greatly enhance efficiency.

5 A Signature Scheme

The conic curves equation and parameters are described above. Before signing a message m, a hashing function HASH() should be applied. HASH(m) embedded on $C_n(a,b)$ is a point M.

Alice release as public parameters n, a, b and e. Then she computes the point Q =(s, t) on $C_n(a,b)$ according to

$$Q=(s,t)=d\cdot M.$$

The signature for the message m is the pair (s,t), which can be checked by computing

$$M=e\cdot Q$$

on $C_n(a,b)$ and extracting the message m from M (because $(ed)\cdot M=M$).

6 Security

The security of our scheme over conic curves is based on the difficulty of factoring n. In this section, we

discuss the security of these schemes from various viewpoints.

The original RSA schemes can be broken if one can determine order of the multiplicative groups. It is known that finding $\phi(n)=(p-1)(q-1)$ is computationally equivalent to factoring n. In our proposed schemes, a similar relationship holds.

Theorem 3: Let N_n be $lcm(p+1,q+1)$. Finding N_n is computationally equivalent to factoring the composite number n.

The security of the original RSA scheme is also based on the difficulty of finding the secret multiplier key d. We have the following relationship.

Theorem 4: Solving a secret key d from public keys e and n is computationally equivalent to factoring a composite number n.

The encryption-decryption functions E(•) and D(•) for our scheme are homomorphic for addition as $E(M_1+M_2)=E(M_1)+E(M_2)$ and $D(M_1+M_2)=D(M_1)+D(M_2)$, for any points M_1 and M_2 on the same conic curve. The probability that randomly chosen integer pairs M_1 and M_2 are on the same conic curve is as negligibly small. Thus, passive attacks using homomorphism seem to be ineffective against our scheme.

Consider an active attack(a chosen-plaintext attack) using homomorphism. Suppose an attacker A wants to make a victim B sign a plaintext $M=(m_x, m_y)$ without B's consent. A generates another message M' with B's public keys (e_B, n_B) and random integer r,

$$M' = M + e_B \cdot (r \cdot M),$$

and sends M' to B. B makes a signature S' for M' with his secret key d_B:

$$S' = d_B \cdot M' = d_B \cdot (M + e_B \cdot (r \cdot M)).$$

Then, A computes a signature S for M from S' by

$$S = S' - r \cdot M .$$

Using this technique, A can forge B's signatures without B's secret key. To counter this attack, a randomization of a plaintext with a hashing function should be applied.

Isomorphism Attacks are same as homomorphism attacks.

7 A Proxy Signature Scheme

The concept of the proxy signatures was introduced by Mambo *et al.*[9]. As the proxy signatures in areas such as e-commerce and e-money has a good application prospects, it has triggered extensive research. Based on the above public key cryptography, we propose a Proxy Signature Scheme.

The conic curves equation and parameters are described above. It is assumed that a signer Alice asks a proxy signer Bob to carry out signing for her. (n_A, e_A) is the public key of original signer Alice, and her corresponding private key is (d_A, N_{n_A}), where $N_{n_A} = lcm(\#C_{p_A}(a,b), \#C_{q_A}(a,b))$. (n_B, e_B) is the public key of original signer Bob, and his corresponding private key is (d_B, N_{n_B}), where $N_{n_B} = lcm(\#C_{p_B}(a,b), \#C_{q_B}(a,b))$. e_p is a proxy public key. d_{p_A} is a proxy private key of Alice, and d_{p_A} is a proxy private key of Bob. Furthermore, a universal secure hash function h(•) should be published. The details are as follows.

7.1 System Initialization Phase

Alice carries out the steps in below: (1) First make a warrant m_ω, which records the delegation policy including limits of authority, valid periods of delegation etc. (2) Select a random number $e_p \in (1,\cdots, N_{n_A})$, and compute d_{p_A}, where $\gcd(e_p, N_{n_A}) = 1$, $e_p d_{p_A} \equiv 1 \pmod{N_{n_A}}$. (3) Calculate P_A and α, where $P_A = P(h(m_\omega)) = (x_A, y_A)$, $\alpha = P_A \cdot d_{P_A} \cdot d_A$ (4) Send $(m_\omega, P_A, \alpha, e_p)$ to Bob.

7.2 Proxy Generation Phase

Bob first checks whether $e_p < N_{n_B}$ or $\gcd(e_p, N_{n_B}) = 1$. If it does not, he rejects those and stop.

Bob checks the equation $P_A = \alpha \cdot e_p \cdot e_A$ and $y_A x_A^{-1} \equiv h(m_\omega) \pmod{n_A}$. If it does not, Bob stop. Otherwise he compute d_{p_B}, where $e_p d_{p_B} \equiv 1 \pmod{N_{n_B}}$.

7.3 Signature Generation Phase

To sign a message m on behalf of Alice, Bob computes

$$P_B = P(h(m)) = (x_B, y_B)$$

$$\beta = P_B \cdot d_{P_B} \cdot d_B$$

Then (α , β , m_ω , e_p , n_A , P_A , P_B , e_A , n_B , e_B) is a proxy signature of message m .

7.4 Verification Phase

Anyone can check whether (α , β , m_ω , $e_p, n_A, P_A, P_B, e_A, n_B, e_B$) is a valid proxy signature of message m by the follwing equation:

$$P_A = \alpha \cdot e_p \cdot e_A ,$$

$$y_A x_A^{-1} \equiv h(m_\omega) \pmod{n_A},$$

$$P_B = \beta \cdot e_p \cdot e_B ,$$

$$y_B x_B^{-1} \equiv h(m\ ) \pmod{n_B}.$$

If it holds, the signature will be accepted, otherwise rejected.

7.5 Security Discussion

We briefly discuss security of the proxy signature scheme we propose.

Unforgeability: Since β contains Bob's private key and proxy secret key, Only Bob can compute β to generate a valid proxy signature.

Veriflablity: Since α contains Alice's private key and proxy secret key, Bob can not compute α . Alice's agreement on m is also verified explicitly, because Alice's agreement has included in the proxy signature.

Identifiablity: From the verification equations (8), proxy signer Bob's public key information has been explicitly included in a valid proxy signature. Therefore, anyone can determine the identity of the corresponding proxy signer Bob.

Prevention of misuse: Due to using the proxy warrant, the proxy signer Bob can only sign messages that have been authorized by the original signer Alice.

8 Conclusion

In this paper, we first propose a public key cryptosystem scheme on conic curves over the ring Zn, then propose a signature scheme and a proxy signature based on conic curves. Our scheme is motivated by KMOV scheme, but it remove some restrictive condition from KMOV scheme, its security bases on the difficulty of factoring a composite number n, just like RSA. It can resist some of the known attacks on RSA. Since an exciting characteristic of conic is both encoding and decoding over conic are easily implemented, it can be used in the mobile payment system with the limited bandwidth. As an alternative algebra curve technology, we believe conic deserves the further study in cryptography.

This research is supported by the Department of Education of Zhejiang Province under Grant No.20061909.

References:

[1] W. Diffie, M.E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, Vol.22, No.6, 1976, pp. 644-654.

[2] Pascal Paillier, Composite-Residuosity Based Cryptography:An Overview, *RSA Laboratories Cryptobytes*,Vol.5, No.1,2002,pp.20-26.

[3] Z. Cao, A public key cryptosystem based on a conic over finite fields $\boldsymbol{F}_p$, *Advances in Cryptology: Chinacrypt98*, Science Press (in Chinese), 1998, pp.45-49.

[4] M. Zhang, Factoring integers with conics, *Journal of Sichuan University (Natural Science)(in Chinese)*, Vol.33, No.4, 1996, pp. 356-359.

[5] Z. Cao. Conic analog of RSA cryptosystem and some improved RSA cryptosystems. *Journal of Naturul Science of Heilongjiang University (in Chinese)*, Vol.16, No.4, 1999,pp. 15-18.

[6] Z. Dai, D. Pei, J. Yang. et al, Cryptanalysis of a public-key cryptosystem based on conic curves. *CrypTECc99(HongKong)*, 1999.

[7] Q. Sun, W. Zhu, B. Wang, The Conic Curves over Z_n and Public-Key Cryptosystem Protocol, *Journal of Sichuan University (Natural Science)(in Chinese)*, Vol.42, No.3, 2005, pp. 471-478.

[8] K. Koyama, U. Maurer,T. Okamoto,et al, New public key schemes based on elliptic curves over the ring Z_n. *Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology*, Lecture Notes in Computer Science, London:Springer-Verlag, 1991,pp. 252-266.

[9] M. Mambo,K. Usuda, E. Okamoto, Proxy signatures:Delegation of the power to sign messages, *IEICE Transaction Functional*, Vol.E79-A, No.9, 1996, pp. 1338-1354.