International Journal of Pure and Applied Mathematics
Volume 77 No. 3 2012, 443-452
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

ID-BASED SIGNATURE SCHEME USING THE CONIC CURVE OVER Z_n ON TWO HARD PROBLEMS

Nedal Tahat[1] §, E.S. Ismail[2], Feras Bani-Ahmad[3]

[1,3] Department of Mathematics
Faculty of Sciences
The Hashemite University
Zarqa 13133, JORDAN
[2]School of Mathematical
Faculty of Science and Technology
National University of Malaysia
43600, UKM, Bangi, Selangor, MALAYSIA

Abstract: This paper proposes a new identity signature scheme on the conic curve over Z_n. The scheme security is based on the factoring and discrete logarithms simultaneously. The paper gives the representation of the order and base point on $C_n(a, b)$, and introduces the representation of operation by parameters to simplify its calculation. The major advantage of our scheme is that it is very unlikely that the two assumptions can be efficiently solved simultaneously, and therefore offers a longer/higher security than that scheme based on a single cryptographic assumption. Furthermore,the numeric simulation for our scheme is presented. Some possible attacks will be considered, and our security analysis will show that none of them can successfully break any proposed schemes. In addition, our scheme protects the signer from chosen-message attack and also identifies a forged signature.

Key Words: digital signature scheme, identification scheme, conic curve over Z_n, factoring problems, chosen message attack

Received: March 31, 2012

§Correspondence author

1. Introduction

The concept of identity-based (ID-based) cryptosystem was firstly introduced by Shamir [1], in 1984 which can simplify key management procedures of traditional certificate-based cryptography. A major advantage of ID-based signature is that it allows one to sign a message in such a way that any user can verify the signature using the signer's identifier such as email address instead of using his/her digital certificate. Most identification schemes are based on zero-knowledge interactive proofs [6], such as as those in ([2], [3], [5], [7]). A secure digital signature scheme can be constructed using an interactive identification scheme and a hash function. When the identification scheme is converted to a signature scheme, the verifier's role is replaced by the hash function. A digital signature scheme resulting from the above paradigm has equal complexity as the starting identification scheme. Popescu proposed an identification scheme [14] based on the elliptic curve discrete logarithm problem. Given the superior security and efficiency, the work applies the identification scheme proposed by Popescu [14] to develop a digital signature scheme. Such a signature scheme, involving the hash function, achieves to resist the security from the chosen-message attack and to prevent the signature from forgery. But unfortunately then Yang and Chang [9] showed that their scheme is not secure. However, all developed identification based signature schemes in the literature are based on single hard problems, like factoring, discrete logarithm, or elliptic curve discrete logarithm problem such as ([4], [8], [11], [13], [14]). The security of these schemes is usually based on one assumption: there exists a hard problem that is difficult to be solved. To design a more secure signature scheme, which based on two hard problems, has attracted significant interests. The security of the signature scheme is supported by two hard problems, even if one problem is solved, as long as another problem remains difficult to be resolved, the signature is still considered secure. Recently, cryptography based on the conic curve has raised the concern of many researchers. In 1996, Mingzhi Zhang [10] firstly introduced the addition operator $\oplus$ on $C_p(a,b)$, and proved that the rational points of $(C_p(a,b),\oplus)$ is an Abel group. Zhenfu Cao [15] proposed a public key cryptosystem based on the conic curve over F_p. In 2005, Qi Sun [12] proposed a public key cryptosystem based on the conic curve $C_n(a,b)$ over the remaining class ring Z_n , and gave analogues of the RSA and ElGamal cryptosystem on $C_n(a,b)$. The idea to design signature scheme on the conic curve over Z_n based on two hard problems is novel and useful. In this paper, we will propose an identity signature scheme on the conic curve over Z_n based on the factorization and discrete logarithm problem simultaneously.

1.1. Conic Curves over Z_n

Let p be an odd prime and F_p be a finite field of p elements. Let $F_p^{\square}$ be tile multiplication group of F_p . Then, without loss of generality, we can assume

$$F_p = \{0, 1, 2, ..., p-1\},\ F_p^{\square} = F_p \backslash \{0\}$$

Let us further consider the conic over an affine plane $A^2(F_p)$,

$$C(F_p) : y^2 = ax^2 - bx \ \text{ where } a, b \in F_p^{\square} \tag{1}$$

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

$$x(a - t^2) = b \ \text{ where } a, b \in F_p^{\square} \tag{2}$$

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

$$x = b(a - t^2)^{-1}, y = bt(a - t^2)^{-1}, \text{where } a, b \in F_p^{\square} \tag{3}$$

For any $t \in F_p$ and $t^2 \neq a$, let $p(t)$ be the point (x, y) over $C(F_p)$ 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 $C(F_p)$. Let $H = \{t \in F_p; t^2 \neq a\} \cup \{\infty\}$ then , $P : H \longrightarrow C(F_p)$ is a one-to-one map. According to [4], let us define the addition $\oplus$ of elements in $C(F_p)$. $\forall P(t) \in C(F_p)$ and $t \in H$ such that

$$P(t) \oplus P(\infty) = P(\infty) \oplus P(t) \tag{4}$$

Assume $P(t_1), P(t_2) \in C(F_p)$, where $t_1, t_2 \in H$ and $t_1, t_2 \neq \infty$, such that

$$P(t_1) \oplus P(t_2) = P(t_3) \tag{5}$$

where

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

Obviously, $t_3 \in H$ and operation $\oplus$ is commutative.
Any $P(t) \in C(F_p)$, negative element

$$-P(\infty) = P(\infty),\ \ -P(t) = P(-t) \tag{6}$$

And then, from (4),(5) and (6), we can easily prove

$$\forall\ P(t_1), P(t_2), P(t_3) \in C(F_p)$$

$$(P(t_1) \oplus P(t_2)) \oplus P(t_3) = P(t_1) \oplus (P(t_2) \oplus P(t_3)) \tag{7}$$

Therefore, $(C(F_p), \oplus, P(\infty))$ is a finite abelian group. And $|C(F_p)|$ can be defined as,

$$|C(F_p)| = \begin{cases} p-1, & (\frac{a}{p}) = 1 \\ p+1, & (\frac{a}{p}) = -1 \end{cases}$$

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

2. The Proposed Scheme

Our proposed ID-based signature scheme consists of four phases: (1) initialization, (2) key generation , (3)signature generation, and (4) signature verification. In the work, the zero-knowledge based identification scheme by Popescu [5] is transformed into a digital scheme through conversion of one-way hash function. The details of the proposed scheme are depicted as follows.

2.1. System Initialization Phase

The system initialization phase proceeds with the following commonly required parameter over the conic curve domain.

- Choose a conic curve $C_n(a, b)$ over Z_n is defined by the solutions (x, y) of the congruence equation $y^2 = ax^2 - bx (\mathrm{mod}\, n)$, where modulus $n = pq$, and $(a, n) = (b, n) = 1$, p and q are large different odd primes
- $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1, p+1 = 2r, q+1 = 2s, r$ and s are odd primes.
- The order of $C_n(a, b)$ is:

  $$N_n = lcm\{|C_p(a, b)|, |C_q(a, b)|\} = \{p+1, q+1\} = 2rs$$

  where lcm represents the function of calculating the least common multiple, $C_p(a, b)$ and $C_q(a, b)$ are the orders of the conic curve over finite field F_p respectively.
- $h(.)$ cryptographic hash function where the output is t-bit length. We assume here that $t \geq 72$ for the digital signature is enough [7].

2.2. Key Generation Phase

The signer generates the individual public key, as follows

1. $B = (x_B, y_B)$ be the base point of $C_n(a, b)$ and let the order be $N_n = 2rs$;
2. Choose $v \in Z^{*}_{N_n}$ as the private key, calculate $Y = vB$ as the public key;
3. Let $H(m)$ be the collision free one-way hash function value of the message m, the message m was embedded in the conic curve through plaintext embedding algorithm, get the point $P(m) = (x_m, y_m)$, where

$$x_m = \frac{b}{a - m^2} \pmod{n},\ y_m = \frac{bm}{a - m^2} \pmod{n}$$

4. Publish (n, a, b, B, Y), but keep (v, N_n) privately.

2.3. Signature Generation Phase

Signer generates the signature for the message m, as follows.

1. Randomly select number $r \in Z^{*}_{N_n}$
2. Computes

$$\begin{aligned} R &= P(m) \oplus rB = (x_1, y_1) \\ u &\equiv x_1 (\bmod N_n) \\ uB &= (x^{*}, y^{*}),\ \text{assume } (x^{*}, y^{*}) \text{ is } B^{*} \end{aligned}$$

3. Convert the message $P(m)$ and the value R into one integer w using hash function operation $w = H(P(m), R) \in [1, 2^t]$
4. Computes $s = (r + u\, w\, v) (\bmod N_n)$
5. Send the signature (w, s, u, B^{*}) to the verifier.

2.4. Signature Verification Phase

The verifier confirm the validity of the signature for m, as follows:

1. Determine Z following $Z = sB \oplus (-uwY) \oplus P(m) = (x_1^{'}, y_1^{'})$
2. Compute $x_1^{'}B$ and determine w following $w = H(P(m), Z)$

3. If the resulting $x_1^{'}B = (x^{\square}, y^{\square})$ and $H(P(m), Z) = w$, then validate the signature; otherwise, reject it.

Theorem 1. *If the algorithm for generating keys and signing messages are run smoothly then the validation of signature is correct.*

Proof. We have to show that the signature $(w, s, u, B^{\square})$ satisfies $x_1^{'}B = (x^{\square}, y^{\square})$ and $H(P(m), Z) = H(P(m), R) = w$. Note that

$$\begin{aligned} Z &= sB \oplus (-uwY) \oplus P(m) \\ &= (r + u\,w\,v)B \oplus (-uwY) \oplus P(m) \\ &= (r + u\,w\,v)B \oplus (-uwvB) \oplus P(m) \\ &= rB \oplus P(m) \\ &= R \\ &= (x_1, y_1) \end{aligned}$$

Then we have $R = Z$ and $(x_1, y_1) = (x_1^{'}, y_1^{'})$.
Therefore,

$$x_1^{'}B = (x^{\square}, y^{\square})$$

and

$$H(P(m), Z) = H(P(m), R) = w$$

, then the verifier accepts the signature. □

3. Security Discussion

In this section, we will analyze the security of the our scheme based on two hard problems.

- Discrete Logarithm Problem: Adversary whishes to obtain secret key v using all information that a vailable from the system. In this case, Adversary need to solve $Y = vB$, finding v is difficult. This is also known as the discrete logarithm problems over $C_n(a, b)$
- Integer Factorization Problem: The modulus n cannot be factorized through the known parameters, the security will be guaranteed. Finding N_n is computationally equivalent to factoring the composite number n. In our

scheme keeps the N_n privately so that the modulus n is difficult to be factorized. We suppose N_n publishing, we can see

$$n = pq \text{ and } N_n = 2rs, \text{ where } 2r = p+1, 2s = q+1$$

$$\text{Then } r = \frac{p+1}{2},\ s = \frac{q+1}{2},\ \text{so } N_n = \frac{(p+1)(q+1)}{2}$$

From the above equations, p and q can be obtained, and then the big integer n can be factorized. But in our scheme keeps the N_n privately so that the modulus n is difficult to be factorized.

The case, when Adversary intends to forge an individual signature $(w, s, u, B^{\square})$ for a messag m.

To forge a valid individual signature for a message m, an Adversary randomly selects Z and $x_1^{'}$ to determine $w = H(P(m), Z)$ and $x_1^{'}B = (x^{\square}, y^{\square})$. In addtion to Z and $x_1^{'}$, the Adversary derives the signature $(s, u, B^{\square})$ by the public key n, B and Y following $Z \equiv sB \oplus (-uwY) \oplus P(m) = (x_1^{'}, y_1^{'})$. Such solutions of unknown numbers s and u here also depend on the DLP over $C_n(a, b)$ and factoring problem, and it is infeasible in reasonable computational security.

4. Numerical Simulation of the Scheme

Let $n = 5 \times 13 = 65$ and consider the conic curve

$$y^2 = 2x^2 - x (\mathrm{mod}\, 65)$$

then $a - b \equiv 1 (\mathrm{mod}\, n)$ and choose $p = 5, q = 13$, then $r = \frac{p+1}{2} = 3, s = r = \frac{q+1}{2} = 7$. We Choose the base point $B = P(2) = (32, 64)$ with order $N_n = 2rs = 42$. Choose the private key $v = 9$ and the public key $Y = vB = 9P(2) = P(10)$. Publish the conic curve C, n, the base point B, and the public key Y.

Signature generation:

Assume the message is $m = 880$, according to the plaintext embedding algorithm, then get $P(880) = (38, 30)$.
To sign, the signer selects a random integer $r = 5 < N_n$ and computes the following:

$$R = P(m) \oplus rB$$

$$\begin{aligned} &= P(880) \oplus 5P(2) \\ &= P(880) \oplus (2^2P(2) \oplus P(2)) \\ &= P(880) \oplus P(3) = P(49) = (11, 19) \\ u &\equiv x_1(\text{mod}65) \equiv 11(\text{mod}65) \\ uB &= 11P(2) = P(58) = (47, 61) = B^{\square} \end{aligned}$$

Convert the message $P(880)$ and the value $R = P(49)$ into one integer $w = H(P(880), P(49)) = 4$. Then the signer compute

$$s \equiv (r + u\,w\,v)(\text{mod}\,N_n) \equiv (5 + 11(4)(9))(\text{mod } 42) \equiv 23(\text{mod } 42)$$

Then the signature of the message m is $(4, 23, 11, P(58))$

Signature verification:

To verify, the verifier calulates

$$\begin{aligned} Z &= sB \oplus (-uwY) \oplus P(m) \\ &= 23P(2) \oplus (-11(4)P(10)) \oplus P(880) \\ &= 23P(2) \oplus (-44P(10) \oplus P(880) \\ &= 23P(2) \oplus (-44(9P(2)) \oplus P(880) \\ &= 23P(2) \oplus 24P(2) \oplus P(880) \\ &= 5P(2) \oplus P(880) \\ &= P(3) \oplus P(880) \\ &= P(49) \\ &= R = (11, 19) \end{aligned}$$

then we have $R = Z = P(49)$,$(x_1, y_1) = (x_1^{'}, y_1^{'}) = (11, 19)$
and since $H(P(m), Z) = H(P(m), R) = w$, $x_1^{'}B = 11B = B^{\square}$ then the signature is now validated.

5. Conclusion

In this paper, we propose an ID-based signature scheme on conic curve over Z_n. The security of our scheme relies on the difficulty of solving the factorization and discrete logarithm problem simultaneously. Our scheme also is easy to

accomplish for convenient embedding plaintext, computing element order and points in conic curve, and speed up the inverse operation. When the standard binary notation system is adopted to compute the integral multiple of an element of a group, the time can be saved approximately by 1/4. We also analysis its security. The entire process guarantees the security and reliability.

References

[1] A. Shamir, Identity-based cryptosystems and signature schemes, In: *Advances in Cryptology-CRYPTO'84*, Lecture Notes in Computer Science (1984), 47-53.

[2] A. Shamir, How to prove yourself: Practical solutions to identification and signature proplems, *Advances in Cryptology-Proceedings of Crypto'86*, LNCS, **263**, Springer (1987), 186-194.

[3] A.M. Allam, I.I. Ibrahim, I.A. Ali, A.E.H. Elsawy, Efficient zeroknowledg identification scheme with secret key exchange, In: *Proceedings of the 46-th IEEE International Midwest Symposium on Circuits and Systems*, **1** (2003), 516-519.

[4] C.J. Cha, H.J. Cheon. An identity-based signature from gap diffie-hellman groups, In: *PKC* (Ed. Y.G. Desmedt) (2003); *LNCS*, Springer, Heidelberg, **2567**, 18-30.

[5] C. Popescu, An identification scheme based on the elliptic curve discrete logarithm problem, In: *The 4-th International Conference on High-Performance Computing in the Asia-Pacific Region*, **2** (2000), 624-625.

[6] C.P. Schnorr, Efficient signature generation by smart cards, *Journal of Cryptology*, **4**, No. 3 (1991), 161-174.

[7] D.H. Nyang, J.S. Song, Knowledge-proof based versatile smart card verification protocol, *ACM SIGCOMM Computer Communication Review*, **30**, No. 3 (2000), 39-44.

[8] F. Hess, Efficient identity based signature schemes based on pairings, In: *SAC*, LNCS, Springer, Heidelberg (Ed-s: K. Nyberg, H.M. Heys), **2595** (2003), 310-324.

[9] J. Yang, C. Chang, Cryptanalysis of ID-based digital signature scheme on elliptic curve cryptosystem, In: *Eighth International Conference on Intelligent Systems Design and Applications* (2008).

[10] M. Zhang, Factoring integer with conics, *Journal of Sichuan University, Natural Science Edition*, **33**, No. 4 (1996), 356-359, In Chinese.

[11] P.G. Kenneth, ID-based signatures from pairings on elliptic curves, *Cryptology Print Archive, Report*, **2002/004** (2002), http://eprint.iacr.org/.

[12] Q. Sun, W. Zhu, B. Wang, The conic curves over Z_n and public-key cryptosystem protocol, *Journal of Sichuan University, Natural Science Edition*, **42**, No. 3 (2005), 471-478, In Chinese.

[13] R. Sakai, K. Ohgishi, M. Kasahara, Cryptosystems based on pairing, In: *SCIS*, Okinawa, Japan (2000).

[14] Y. Chung, K. Huang, T. Chen, ID-based digital signature scheme on the elliptic curve cryptosytem, *Computer Standards and Interface*, **29** (2007), 601-604.

[15] Z. Cao, A public key cryptosystem based on the conic curve over F_p, *Advances in Cryptology-Chinacypt'98*, Beijing, Science Press (1998), 45-49.