Annals of the University of Craiova, Mathematics and Computer Science Series
Volume 40(2), 2013, Pages 148–153
ISSN: 1223-6934

A new conic curve digital signature scheme with message recovery and without one-way hash functions

Nedal Tahat

Abstract. In this paper, we present an efficient digital signature scheme with message recovery and without using any one-way hash function and message redundancy. The new scheme is based on conic curve cryptography (CCC) that offers a very high level of security with a small key size. Obviously, the result is a low computational cost and a clear saving in memory and bandwidth. The security of the new scheme is based on two hard problems, the discrete logarithm on conic curve and factorization problem. It provides higher level security than schemes based on a single hard problem. We show in details that the proposed scheme does not involve any modular exponentiation operation in all algorithms.

2010 Mathematics Subject Classification. Primary 60J05; Secondary 60J20.
Key words and phrases. conic curve, finite field, message recovery,One-way hash function, simulated attacks.

1. Introduction

In modern cryptography [1], the security of developed signature schemes is based on the hardness of solving some hard number theoretical problems, such as factoring and discrete logarithms problems ([2], [3]). One common feature of these schemes is that they are depending on a number-theoretical problem and thus their implementation heavily depends on modular exponentiation which is known to be consuming and costly. Conic curve cryptography [4] is a new public key cryptosystem that people put forward in recent years. Compared with elliptic curve cryptography (ECC), conic curve cryptography has the advantages of simpler calculations, the coding and decoding can be carried out more efficiently in the conic curve point group, which is a very exciting feature. Since the discrete logarithm problem based on conic curve point group, or the conic curve discrete logarithm problem (CCDLP), are not easier than the elliptic curve discrete logarithm problem (ECDLP) when the conic curve point group has the same order as elliptic curve point group, the conic curve cryptosystem has become an important research content in cryptography, and has also got much attention from many researchers in the past ten years. However, the idea to design signature scheme on the conic curve over Z_n based on two hard problems is novel and useful. Nyberg and Rueppel scheme in [5] is the first signature scheme with message recovery based on discrete logarithm problem. In message recovery mode, the receiver can recover the original message from the received signature. In contrast to the appendix mode, the message recovery mode has the advantage of smaller communication load and consequently is more efficient in applications. Usually, the message redundancy scheme should be used to resist the forgery attack [6]. However, a lot of researches are made in these areas ([7], [8], [9], [10], [11]). Recently, Mohanty

Received November 15, 2012. Revised December 3, 2013.

and Banshidhar [12] proposed a digital signature with message recovery and without one-way hash function based on discrete logarithm problem (DLP).

In this paper, we propose a new conic curve digital signature with message recovery and without one-way hash function and the security of the new scheme is based on two hard problems; CCDLP and integer factorization problem (FIP). The new scheme offers a longer security than the schemes based on DLP. This is because the probability of solving two hard problems simultaneously by intruder is believable to be negligible. We next discuss and describe the efficiency of our scheme, and show that the proposed scheme does not involve any modular exponentiation operation in all algorithms, this giving an advantage to the scheme.

1.1. The Conic Curves Over a Finite Field. Let p be an odd prime and $\mathbb{F}_p$ be a finite field of p elements. Let $\mathbb{F}_p^*$ be tile multiplication group on $\mathbb{F}_p$. Then, without loss of generality, we can assume

$$\mathbb{F}_p = \{0, 1, ..., p-1\},\ \mathbb{F}_p^* = \mathbb{F}_p \backslash \{0\}.$$

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

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

It's obvious that $C(\mathbb{F}_p)$ includes origin of coordinates $\mathcal{O}(0,0)$. If $x \neq 0$, let $t = yx^{-1}$ and fill $y = xt$ in the equation (1). Then, we get

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

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

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

For any $t \in \mathbb{F}_p$ and $t^2 \neq a$, let $P(t)$ be the point of $C(\mathbb{F}_p)$ satisfying equation (3) Moreover, an ideally defined point $\mathcal{O}$, namely the point at infinity $P(\infty)$, is also recognized as a point over $C(\mathbb{F}_p)$.

Let $H = \{t \in \mathbb{F}_p; t^2 \neq a\} \cup \{\infty\}$. We can define a bijection $P : H \longrightarrow C(\mathbb{F}_p)$ where $\infty \longrightarrow (0,0),\ t \longrightarrow (x_t, y_t),\ t \neq \infty$ and $x_t = b(a - t^2)^{-1},\ y_t = bt(a - t^2)^{-1}$.

A conic $(C(\mathbb{F}_p), \oplus, P(\infty))$ becomes an abelian group under the operation $\oplus$ as shown below:

- For every $P(t) \in C(\mathbb{F}_p)$,

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

- For any $P(t_1), P(t_2) \in C(\mathbb{F}_p)$ where $t_1, t_2 \neq \infty$, $P(t_1) \oplus P(t_2) = P(t_3)$ with

$$t_3 = \begin{cases} (t_1 t_2 + a)(t_1 + t_2)^{-1}, t_1 + t_2 \neq 0, \\ \infty,\ \ t_1 + t_2 = 0. \end{cases} \tag{5}$$

The cardinality of $C(\mathbb{F}_p)$ is given by

$$|C(\mathbb{F}_p)| = \begin{cases} p - 1, (\frac{a}{p}) = 1 \\ p + 1, (\frac{a}{p}) \neq 1 \end{cases}$$

where $(\frac{a}{p})$ denotes the Legendre symbol.
It's evident that $\forall P(t) \in C(\mathbb{F}_p), |C(\mathbb{F}_p)|P(t) = P(\infty)$, when $mP(t) = \underbrace{P(t) \oplus ... \oplus P(t)}_{m}$.

2. The Proposed Scheme

In this section, we propose an efficient digital signature scheme with message recovery and without one-way hash function based CCDLP. The proposed scheme is divided into four phases: the system initialization phase, the key generation phase, the signature generation phase and verification phase.

2.1. System initialization phase. Choose a conic curve $C_n(a,b)$ over $\mathbb{Z}_n$, the curve equation is $C_n(a,b): y^2 = ax^2 - bx(\mathrm{mod}n)$, where $a,b \in \mathbb{Z}_n, n = pq$ and $gcd(a,n) = gcd(b,n) = 1$. p and q are large different odd primes, satisfying the condition $(\frac{a}{p}) = (\frac{a}{q}) = -1$, $p+1 = 2r, q+1 = 2s$, r and s are odd primes. Then, 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 fields $\mathbb{Z}_p$ and $\mathbb{Z}_q$.

2.2. Key Generation phase.

Step 1: Let $G = (x_G, y_G)$ be a base point of $C_n(a,b)$ and let the order be $N_n = 2rs$;

Step 2: Choose $d \in \mathbb{Z}^*_{N_n}$ as the private key, calculate $y = dG(\mathrm{mod}n) = (e,h)$ as the public key;

Step 3: The message $M = (m_x, m_y)$ is an integer pair, where $m_x \in \mathbb{Z}_n, m_y \in \mathbb{Z}_n$. Let $M = (m_x, m_y)$ be a point on the conic curve $C_n(a,b)$.

Step 4: Publish (n,a,b,G,y), but keep d and N_n privately.

2.3. Signature Generation phase. Signer generates the signature for the message M, as follows.

Step 1: Pick randomly an integer $k \in \mathbb{Z}^*_{N_n}$.

Step 2: Computes

$$s_1 = eM = (x_1, y_1), \text{ where } u \equiv x_1(\mathrm{mod}\, N_n) \tag{6}$$

$$s_2 = s_1 \oplus M \oplus (-kG)(\mathrm{mod}n) = (x_2, y_2), \text{where } \delta \equiv x_2(\mathrm{mod}\, N_n) \tag{7}$$

Step 3: Calculates t from

$$u + t \equiv d^{-1}(k - \delta)(\mathrm{mod}\, N_n) \tag{8}$$

Step 4: The signer sends the signature (s_1, s_2, t, u, δ) of M to the verifier.

2.4. Verification phase. After receiving the signature (s_1, s_2, t, u, δ), the verifier performs the following operations.

Step 1: Computes

$$\acute{M} = (-s_1) \oplus s_2 \oplus (u+t)y \oplus \delta G \tag{9}$$

Step 2: Checks whether $s_1 = e\acute{M}(\mathrm{mod}\, n)$. If it holds, then the signature (s_1, s_2, t, u, δ) is indeed the valid signature generated by the signer of the recovered message M.

3. Security Analysis

The security of our scheme over conic curves is based on the difficulty of factoring n. Now we will show some possible attacks by which intruder may try to take down the proposed signature scheme based on CCDLP.

A. Correctness proof

The correctness of the signature scheme of the message M as shown below

$$\begin{aligned} \acute{M} &= (-s_1) \oplus s_2 \oplus (u+t)y \oplus \delta G \\ &= (-s_1) \oplus s_1 \oplus M \oplus (-kG) \oplus d^{-1}(k-\delta)y \oplus \delta G \\ &= M \oplus (-kG) \oplus d^{-1}(k-\delta)dG \oplus \delta G \\ &= M \oplus (-kG) \oplus (kG) \oplus (-\delta G) \oplus (\delta G) \\ &= M \end{aligned}$$

Therefore, $s_1 = e\acute{M} \,(\mathrm{mod} n)$. Then the verifier accepted the signature.

B. Attack Aiming to recover d

- Attack 1: It is infeasible that an intruder wants to solve k from equation (7) always equivalent the discrete logarithms over $C_n(a, b)$.
- Attack 2: It is infeasible that intruder wants to solve d from equation (8), since it has 3 unknown parameters k, δ and d.

C. Simulated Attacks

Intruder wishes to obtain the private key d from public key $y = dG(modn)$ and the random number k from the $u + t \equiv d^{-1}(k - \delta)(\mathrm{mod}\, N_n)$ which are clearly infeasible because the difficulty of solving CCDLP and factoring N_n. Moreover, the modulus n cannot be factorized through the known parameters the security will be guaranteed. Finding $N_n = 2rs$ is computationally equivalent to factoring the composite number n. In our scheme keep the N_n privately so that the modulus n is difficult to be factorized. Therefore, no matter where do an attacker to conduct attacks, the new scheme is not easy to break. The simulations of two hard mathematical problems are in the following:

(1) If an attacker wants to forge the signature t from $u + t \equiv d^{-1}(k - \delta)(\mathrm{mod}\, N_n)$, he must get the parameter N_n. Assume that the attacker can solve the factoring problem, that is the big integer n can be calculated, the prime factorization p and q, and the parameter N_n can also be calculated. However, as we know the difficulty of discrete logarithm problem on conic curve, so the attacker still cannot solve the problem of getting the private key d by the public key $y = dG(\mathrm{mod}n)$.

(2) If the attacker can solve the CCDLP, assume that he has got private key d from the public key $y = dG(\mathrm{mod}n)$. In order to forge the signature message, he needs to calculate the signature value t from $u + t \equiv d^{-1}(k - \delta)(\mathrm{mod}\, N_n)$. But because of the unpublished parameter N_n the attacker wants to calculate p and q from the public modulus n, and then calculates the parameter N_n he still needs to decompose the big integer n, that is needed to solve factoring problem.

The above simulated attacks show that the new scheme is very fast in the case of two hard mathematical problems cannot be solved at the same time.

D. Attack for parameter Reduction

TABLE 1. The comparison between our scheme and Mohanty's scheme

Items	Our new scheme	Mohanty's scheme
Signature generation	$3T_{cc-add} + 2T_{cc-mul} + T_{mul}$	$2T_{exp} + 2T_{mul}$
Signature verification	$3T_{cc-add} + 2T_{cc-mul}$	$3T_{exp} + 2T_{mul}$

The message recovery equation (9) can be transformed into

$$\acute{M} = (-s_1) \oplus s_2 \oplus \acute{t}y \oplus \delta G \tag{10}$$

where $\acute{t} = t + u$. The parameter in equation (9) cannot be reduced via the parameter reduction attack, which means the new scheme will withstand the parameter reduction attack.

E. Forgery attack

Given the message M, a forger has to solve both equation (6) and equation (9) in order to get the signature (s_1, s_2, t, u, δ). Even if both s_1 and s_2 are known, it is difficulty to solve k and d in equation (8) so it is difficult to get t and the attacker cannot get a signature u and δ because of the unpublished parameter N_n.

4. Efficiency Analysis

Conic curve cryptography [4] is a new public key cryptosystem that people put forward in recent years. Compared with elliptic curve cryptography (ECC), conic curve cryptography has the advantages of simpler calculations, easier achieving encoding and decoding, faster calculating, et al. The results from some scholars show that under the same order, a conic curve of the discrete logarithm problem is not easier than elliptic curve.

The main computation amount to generate the signature for new digital signature scheme is $s_1 = eM = (x_1, y_1), s_2 = s_1 \oplus M \oplus (-kG)(\mathrm{mod} n) = (x_2, y_2), u \equiv x_1(\mathrm{mod}\, N_n), \delta \equiv x_2(\mathrm{mod}\, N_n)$ and $u + t \equiv d^{-1}(k - \delta)(\mathrm{mod}\, N_n)$. And the main computation amount to verify the signature is $\acute{M} = (-s_1) \oplus s_2 \oplus (u + t)y \oplus \delta G$ and $s_1 = e\acute{M}(\mathrm{mod}\, n)$. We use the following notation to analyze the efficiency of the new scheme

- T_{mul} is the time complexity for executing the modular multiplication,
- T_{cc-add} is the time complexity for executing the addition of two conic curve points,
- T_{exp} is the time complexity for executing the modular exponentiation,
- T_{cc-mul} is the time complexity for executing the multiplication on conic curve points.

Table 1 shows the comparison of main computation amount of two digital schemes.

From the comparison of Table 1 we can see that the computation amount of the new scheme is reduced comparing with Mohanty's scheme based on DLP. In the proposed scheme, no modular exponentiations are performed by the signer and verifier and it makes the scheme very efficient. CCC devices require less storage, less power, less memory, and less bandwidth than other systems. In our scheme s_1 is computed as

$s_1 = eM(\mathrm{mod}n)$ instead of exponential, so the new scheme can be applicable to large message, hence it is practical.

5. Conclusion

In this paper, we proposed a new conic curve digital signature scheme with message recovery and without one-way hash functions. The security of our scheme relies on the difficulty of solving the factorization and discrete logarithm on conic curve. The proposed scheme requires minimal operations in signing and verifying and thus makes it very efficient. The scheme supports message recovery feature, as message is recovered from the signature and there is no need to send message along with the signature. Clearly, whether it is in terms of security or performance, the proposed scheme is superior to Mohanty's scheme. To the best of our knowledge, this is the first work done on conic curve digital signature scheme with message recovery and without one-way hash functions.

References

[1] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transaction on Information Theory* **22** (1976), no. 6, 557–560.

[2] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transaction on Information Theory* **31** (1985), no. 4, 469-472.

[3] R. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signature and public-key cryptosystem, *Communications of the ACM* **21** (1978), no. 2, 120-126.

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

[5] K. Nyberg and R. A. Rueppel, Message recovery for signature schemes based on the discrete logarithm problem, *in: Advances in Cryptology, EUROCRYPT94, Lecture Notes in Computer Science* 950, Springer (1995), 182-193.

[6] Z. C. Li, Z. X. Li and Y. X. Yang, A new forgery attack on message recovery signature *, Journal of China Institute of Communication* **21** (2000), no. 5,84–87.

[7] L. Kang and X. H. Tang, A New Digital Signature Scheme without one way hash function and message redundancy, *Fifth International Conference on Information, Communications and Signal Processing*, (2005), Bangkok, Thailand, 973–975.

[8] C.C. Chang and Y. F. Chang, Signing a digital signature without using one-way hash functions and message redundancy schemes, *IEEE Commun. Lett.* **8** (2004), no. 8, 485–487.

[9] S.P. Shieh, C.T. Lin, W.B. Yang and H.M. Sun, Digital Multi-signature schemes for authenticating delegates in mobile code systems, *IEEE Trans. Veh. Technol.* **49** (2000), no. 4, 1464–1473.

[10] J. Liu and J. Li, Cryptanalysis and improvement on a digital signature scheme without using one way hash and message redundancy, *International Conference on Information Security and Assurance ISA2008*, Busan 2008, 266–269.

[11] F. G. Zhang, Cryptanalysis of Chang et al:'s signature scheme with message recovery, *Cryptology ePrint Archive, Report* (2004), availlable at http://eprint.iacr.org/2004/213.pdf.

[12] S. Mohanty and B. Majhi, A digital signature scheme with message recovery and without one-way hash function, *IEEE 2010 International Conference on Advances in Computer Engineering (ACE)*, Bangalore, India, 265–267.

(Nedal Tahat) Department of Mathematics, The Hashemite University, Zarqa 13115, Jordan.

E-mail address: nedal@hu.edu.jo