International Mathematical Forum, 1, 2006, no. 31, 1529 – 1536

A New Elliptic Curve Undeniable Signature Scheme

Tzer-Shyong Chen[1] En-Te Hsu[2] Yuan-Lung Yu[3]

[1]Department of Information Management, Tunghai University

[2]Department of Accountancy, Tunghai University

[3] Department of Computer Science and Information Management,

Hung-Kuang University

E-mail: arden@thu.edu.tw

Abstract

A secure and efficient cryptosystem can be constructed through three primary methods, the discrete logarithm system (e.g. DSA), the integer factorization system (e.g. RSA), and the elliptic curve cryptosystem (ECC) [1][2]. This paper employs the elliptic curve cryptosystem method. The elliptic curve cryptosystem has low computational amount and short key size, both of which benefit a cryptosystem in limited-hardware environment with reduced overheads. The ECC provides a suitable environment for the cryptosystems.

This study presents a new elliptic curve undeniable signature scheme, which is an improved design of the undeniable group signature scheme. The proposed scheme is based on the ECC. Complex parameters have been simplified to reduce time complexity. Hence, the proposed scheme is simpler than the undeniable group signature scheme yet more efficient and more secure.

Key words: Undeniable signature scheme, discrete logarithm, integer factorization, elliptic curve cryptosystem, and cryptography

1. Introduction

The elliptic curve theory was proposed in 1985 by Koblitz [1] and Miller [2]. The theory has since then been widely applied to various cryptosystems. The ECC equips cryptosystems with tight security through its difficult to solve elliptic curve discrete logarithm problem (ECDLP) [2, 3 and 4]. Unlike the integer factorization algorithm and the discrete logarithm problem, the ECDLP is extremely difficult and time consuming to solve. There exists no efficient solution to this problem. Moreover, The ECC consumes a much smaller bit size yet provides a security equal to that provided by the RSA or DSA.

The elliptic curve cryptosystem (ECC) was applied to improve the undeniable signature scheme by Lin and Wu [5, 6]. Lin [7] later employed the ECC on the undeniable signature scheme by Chaum [8] to produce an elliptic-curve undeniable signature scheme. The ECC is also applied to the group-oriented undeniable signature scheme by Harn and Yang [9]. This paper proposes to improve the above schemes through upgrading.

This paper is divided into five sections. Section one introduces the proposal; section two introduces the elliptic curve cryptosystem; the proposal is detailed in section three; section four analyzes the security and efficiency of the proposed scheme; section five draws conclusions.

2. An Introduction to the Elliptic Curve Cryptosystem

The general equation for the elliptic curve is $y^2 = x^3 + ax + b \bmod p$, p is a natural prime number, and the value of a, b should satisfy the discriminate $D = 4a^3 + 27b^2 \neq 0 \bmod p$. Only then could $y^2 = x^3 + ax + b \bmod p$, be used as the decrypting elliptic curve [10].

Before we introduce the addition operation of the elliptic curve [4], we need to first introduce a special point *O*, known as the point of infinity and it satisfies the following properties:

(1) If *P*, *Q* are two points on the elliptic curve, *O* is the point of infinity, then
P + *O* = *O*+*P*=*P*.

(2) *O* = -*O*.

(3) If *Q* is not equal to point (-*P*), then *P* + *Q* = *O*.

(4) If *P*≠*O*, *Q*≠*O*, then *P* + *Q* = -*R*.

According to the addition operation of the elliptic curve, if there are two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ on the elliptic curve, and if *P*≠-*Q*, then $P + Q = (x_3, y_3)$, $x_3 = \lambda^2 - x_1 - x_2 \bmod m$, $y_3 = \lambda(x_1 - x_3) - y_1 \bmod m$, where

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & , \quad if \quad P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} & , \quad if \quad P = Q \end{cases}$$

If there is a point *G* on the elliptic curve, and this point is the base point, then the operation on *nG* has the following properties, 1*G*=*G*, 2*G*=*G* + *G*, 3*G*=*G* + *G* + *G*=2*G* + *G*, ..., (*n*-1)*G*=*G* + *G*+ ... + *G* with a total of (*n*-1) *G*, *nG*=*O*, (*n* + 1)*G*=*G*. Thus the *nG* is *n*×*G* formal, meaning addition operations of the elliptic curve, and not the general multiplication operation, are continuously performed on *n* number of *G*'s.

For example: A, B both have chosen to use the elliptic curve $y^2 = x^3 + x + 6$ for communicating, taking p as 11, then $D = 4a^3 + 27b^2 \bmod 11 = 8 \bmod 11 \neq 0$, hence it is proved that the points on the elliptic curve are (2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9). If A, B both chose the point (2, 7) as *G* (Generator point), and performs the addition operation of the elliptic curve, then *G*=(2, 7), 2*G*=*G* + *G*=(5, 2), 3*G*=2*G* + *G*=(8, 3), 4*G*=(10, 2), 5*G*=(3, 6), 6*G*=(7, 9), 7*G*=(7, 2), 8*G*=(3, 5), 9*G*=(10, 9), 10*G*=(8, 8), 11*G*=(5, 9), 12*G*=(2, 4), 13*G*=*O*, 14*G*=(2, 7).

3. The Proposed Scheme

Suppose that there are $k \geq 2$ users in a group, and every user of the group has a private key. The users are represented in the sequence of U_1, U_2, U_3,…, U_k, and the proposed scheme is based on the same condition.

3.1. Key Generation Phase

In order to sign a message $M \in [1, n\text{-}1]$, each user in the group generates his/her private key; using the private keys of all the users of the same group, the group public key is calculated as follows:

Step 1: Select an elliptic curve E defined over Z_p. For security reasons, E should be divisible by a large prime number.

Step 2: Select a base point $G \in E(Z_p)$ whose order must be a large prime number, defined as n.

Step 3: Each user in the group selects a random integer $d_i \in [1, n\text{-}1]$ as his/her private key, in which $i = 1, 2, 3, \ldots, k$.

Step 4: Let $Q_1 = d_1 \times G$, then the group public key Q can be calculated as follows through the cooperation of all users.

$$Q = Q_k = d_k \times (Q_{k-1}) = (d_1 d_2 d_3 \ldots d_k \bmod n) \times G$$

3.2. Commitment Phase

Let $Z_1 = (d_1 M \bmod n) \times Q$, then the group undeniable signature Z can be calculated as follows through the cooperation of all users. $Z=Z_k=d_k \times (Z_{k-1})= (d_1 d_2 d_3 \ldots d_k M \bmod n) \times Q = (X_1, Y_1)$.

Afterwards, Z and M is sent to Bob for verification.

3.3. Verification Phase

Step 1: Bob selects two random integers a and $b \in [1, n\text{-}1]$ and computes

$W = a \times Z + b \times Q = (X_2, Y_2)$, then sends W to Alice.

Step 2: After receiving W, let $R_1 = (d_1^{-1} \bmod n) \times W$, then R can be calculated as follows through the cooperation of all users.

$$R = R_k = d_k^{-1} \times (R_{k-1}) = (d_1^{-1} d_2^{-1} d_3^{-1} \ldots d_k^{-1} \bmod n) \times W$$

Step 3: According to R, Bob calculates

$$R' = (aM \bmod n) \times Q + b \times G$$

If $R' = R$, then the group undeniable signature Z and the message M is authentic.

Theorem 1.

In the verification phase, if $R' = R$, the undeniable signature Z and the message M is authenticated.

Proof: For brevity, let $t = d_1d_2d_3\ldots d_k$, therefore

$$
\begin{aligned}
Q = Q_k &= d_k\times(Q_{k-1}) \\
&= (d_1d_2d_3\ldots d_k \bmod n)\times G = (t \bmod n)\times G \\
Z = Z_k &= d_k\times(Z_{k-1}) \\
&= (d_1d_2d_3\ldots d_kM \bmod n)\times Q = (tM \bmod n)\times Q \\
R = R_k &= d_k^{-1}\times(R_{k-1}) \\
&= (d_1^{-1}d_2^{-1}d_3^{-1}\ldots d_k^{-1} \bmod n)\times W = (t^{-1} \bmod n)\times W \\
&= (t^{-1} \bmod n)\times(a\times Z + b\times Q) \\
&= (t^{-1} \bmod n)\times\{a\times[(tM \bmod n)\times Q] + b\times[(t \bmod n)\times G]\} \\
&= (t^{-1} \bmod n)\times[(atM \bmod n)\times Q + (bt \bmod n)\times G] \\
&= (aM \bmod n)\times Q + b\times G \\
&= R'
\end{aligned}
$$

4. Performance an Analysis and Security Issue

4.1. Performance analysis

An analysis of the performance of the proposed scheme is presented in the subsection below. The symbols are defined as follows:

T_{MUL} : time required by modulus operation;

T_{INV} : time required by modulus inverse element operation;

T_{ADD} : time required by the modular addition operation;

T_{EC_MUL} : time required by elliptic curve multiplication operation;

kG is given in reference [10], where *k* is a random 160-bit integer and $G \in E(Z_p)$. *E* is an elliptic curve defined over Z_p and $p \approx 2^{160}$. The time complexity clearly presented in the following relationship:

$$T_{EC\_MUL} \approx 29T_{MUL}$$

$$T_{EC\_ADD} \approx 0.12T_{MUL}$$

Modulus addition and subtraction operation amount is negligible and thus omitted.

Table 1 lists the algorithm and time complexity phase by phase for easier understanding of the efficiency of the proposed scheme. Table 1 also clearly illustrates significant improvement in system performance in terms of time complexity in the proposed scheme.

4.2. Security Issue

The solution to the ECDLP is based on the derivation of *d* in relation to the given *G* and *Q* as follows:

$$Q = d \times G$$

In the above equation, $d \times G$ represents *d* successive additions of point *G* which is operated under the elliptic curve cryptosystem. *Q* is the point derived from $d \times G$ and the variance of *Q* depends on the value of *d*. Therefore an attacker, due to his inability to solve the ECDLP, shall fail to derive the private key and hence unable to forge signatures.

Table 1: Algorithm and time complexity of the proposed scheme

Items		Algorithm ($k \geq 2$ users)	Time Complexity	
			Time Complexity	Rough Estimation
Key Generation	Private Key	d_i ($i = 1, 2, 3, \ldots, k$)	$k\ T_{EC\_MUL}$	$29k\ T_{MUL}$
	Public Key	$Q = Q_k = d_k \times (Q_{k-1}) =$ $(d_1 d_2 d_{3\ldots} d_k \bmod n) \times G$		
Commitment		$Z = Z_k = d_k \times (Z_{k-1}) =$ $(d_1 d_2 d_{3\ldots} d_k M \bmod n) \times Q$	$k\ T_{EC\_MUL}$ $+\ T_{MUL}$	$(29k+1)\ T_{MUL}$
Verification		$W = a \times Z + b \times Q$	$(k+4) T_{EC\_MUL}$ $+\ T_{MUL}$ $+\ 2\ T_{EC\_ADD}$ $+\ k\ T_{INV}$	$29k\ T_{MUL}$ $+117.24 T_{MUL}$ $+\ k\ T_{INV}$
		$R = R_k = d_k^{-1} \times (R_{k-1}) =$ $(d_1^{-1} d_2^{-1} d_3^{-1} \ldots d_k^{-1} \bmod n) \times W$		
		$R' = (aM \bmod n) \times Q + b \times G$		

5. Conclusions

The discrete logarithm system was induced into the elliptic curve cryptosystem (ECC) in Lin’s scheme. This induction served to improve the ECC. The proposed scheme served to improve efficiency and security of Lin’s scheme.

6. Acknowledgement

This work was supported in part by the National Science Council of the Republic of China under contract NSC 93-2213-E-029-030.

7. References

[1] N.K., "*Elliptic Curve Cryptosystems*," Mathematics of Computation, Vol. 48, 1987, pp.203-209.

[2] V.S. Miller, "*Uses of Elliptic Curves in Cryptography*," Advances in Cryptology-Crypto'85, LNCS 218, Springer-Verlag, 1986, pp.417-426.

[3] N.K., *"A Course in Number Theory and Cryptography,"*1994, Second edition, New York, NY: Springer-Verlag.

[4] A Certicom Whitepaper, "*The Elliptic Curve Cryptosystem*," July 2000

[5] C.H. Lin and C.T. Wang, "*A New Undeniable Signature Scheme and Its Application to Group Communication*," Proceeding of National Computer Symposium, 1995, pp.397-403.

[6] C.H. Lin and W.C. Wu, "*An Undeniable Signature Scheme Against Reply Attacks*," Journal of Computers, Vol. 9, No. 1, March 1997, pp.397-403.

[7] C.H. Lin and C.L. Lee, "*Elliptic-Curve Undeniable Signature Schemes*," Proceedings of the Eleventh National Conference on information Security, 2001, pp.331-338.

[8] D.C. and H.V. Antwerpen, "*Undeniable Signatures*," Advances in Cryptology-Crypto'89, August 22-24, 1989, pp.212-216.

[9] L.H. and S.Y., "*Group Oriented Undeniable Signature Schemes Without the Assistance of a Mutually Trusted Party*," Advances in Cryptology- Auscrypt'92, December 1992.

[10] Aleksandar Jurisic and Alfred J. Menezes, Elliptic Curves and Cryptography, http://www.certicom.com.

Received: December 10, 2005