Asian Journal of Information Technology 2 (3): 130-134, 2003

Schnorr Blind Signature Based on Elliptic Curves

Ming-Hsin Chang, I-Te Chen, I-Chen Wu and Yi-Shiung Yeh
Department of Computer Science and Information Engineering
National Chiao-Tung University,Hsinchu, Taiwan 300, R.O.C.

Abstract: The blind signature with untraceability is widely used in on-line voting and electronic cash applications. The elliptic curve cryptosystems, based on elliptic curve logarithm over a finite field, have some advantages than other systems. In this paper, we design a new blind signature scheme on elliptic curves that inherits from Schnorr blind scheme. And we will compare proposed schemes to them which based on discrete logarithms with storage requirements and performance.

Key words: Schnorr Blind Signature, Elliptic Curve Cryptosystem and Unlinkability

Introduction

With the growing importance of the mobile transaction, the blind signature scheme (Chaum, 1983; Chaum, 1988 and Okamoto,1992) has become a very active research area. The blind signature, Schnorr blind signature scheme (Okamoto,1992 and Schnorr, 1989) as examples with untraceability is widely used in on-line voting and electronic cash (Chaum, 1983 and Chaum, 1988) applications. When submitting an on-line vote, we would like to vote an anonymously such that no one knows whom we are voting to. Similarly, when you make a purchase, the vender gets the electronic cash from him to give legitimately without knowing him you. It requires the low computation or small memory space like the mobile devices or the smart cards in both clients and servers of mobile environments. Due to the constraint of devices, the low computation and the less memory crypto-scheme are urgently needed. To match this point, an elliptic curve cryptosystem (ECC as short) (ANSI,1997; Bellare and Rogaway, 1993; IEEE, 1997; ElGamal, 1985; Koblitz, 1994; Koblitz, 1983; Menezes, 1993 and Miller,1985) plays an import role in our paper.

Schnorr blind signature (Schnorr, 1989) scheme based on the intractable of the discrete logarithm problem. It is secure in the random oracle model. The blinded scheme first introduced by Okamoto (Okamoto,1992). We proposed a new blind signature scheme that inherits Schnorr blind signature scheme on ECC such that the properties of randomness, unlinkability and unforgability are still preserved. The performance and the storage space requirement of the modified one are much improved than the old one.

We first review the elliptic curves and Schnorr blind signature. A new blind signature scheme is proposed. The security and performance analyses of the proposed scheme. We give a remarkable conclusion.

Preliminaries: Due to our scheme inherits Schnorr blind scheme and based on ECC, we give brief of the elliptic curves (Koblitz, 1994; Koblitz, 1983 and Menezes, 1993) and Schnorr blind scheme proposed by Okamoto (Okamoto,1992 and Schnorr, 1989).

Brief of Elliptic Curves: Elliptic curves can provide versions of public-key cryptosystems that are faster and use the small length of keys, while providing an equivalent level of security. We give a quick introduction to the theory of elliptic curves (Koblitz, 1994 and Koblitz, 1983). For simplicity, we shall set a limit of elliptic curves over Z_p, where p is a prime number. An elliptic curve E over Z_p, denoted $E(Z_p)$, is the set of points (x, y), , satisfying the equation $y^2 = x^3 + ax + b$ where and $4a^3 + 27b^2 \neq 0 \pmod{p}$, together with a special point , called the point at infinity.

The group operation for an elliptic curve $E(Z_p)$ is called addition. In the contrast, the group operation for a traditional discrete logarithm in the group Zp^* is called multiplication. Table 1 shows the correspondence between notation for two groups Zp^* and $E(Z_p)$ (ANSI,1997).

Review of Schnorr Blind Signature: Schnorr blind signature scheme was first introduced in (Okamoto, 1992). The protocol requires three rounds of interaction between signer and recipient shown in Fig. 1. The recipient wants to have message m blindly signed by the signer. The protocol is described as follows. Assume that the signer's private key is $-x$ and his public key is where p is a great prime number, q is a prime factor of p-1 and q is an element.

Step 1. The signer selects a random number and sends to the recipient.

Step 2. The recipient selects random numbers and computes. Finally he sends back with. Where $H(*)$is a hash function.

Table 1: Correspondence between Z_p^* and $E(Z_p)$

Discrete Logarithm Problem	Given $g \in Zp^*$ and $h = g^a \bmod p$, find a	Given $P \in E(Z_p)$ and $Q = aP$, find a
Group	Zp^*	$E(Z_p)$
Group elements	Integer $\{1,2,\ldots,p-1\}$	Point (x, y) on E plus
Group operation	Multiplication modulo p	Addition of points
Notation	Elements: g, h	Multiplication:
	Inverse: g^{-1}	Division: g/h
	Exponentiation: g^a	Elements: P,Q
	Addition: $P+Q$	Negative: $-P$
	Subtraction: $P-Q$	Multiple: aP

Step 3. The signer creates a signature $s = k + ex \bmod q$ on the message m and sends it back to the recipient.

In the verification, the recipient checks whether the equation $g^s y^e = r \bmod p$ is valid. If it is valid, the recipient accepts signature as $S^1 = S + \alpha \bmod q$, otherwise rejects it. The blind signature is an unknown signature of the unknown message m.

Proposed Schnorr Blind Signature on ECCs: Assume that there is an ECC $E(F_p)$ and the parameters p q is a primer factor of p-1. In Fig. 2, the protocol between signer and recipient is described as follows.

Initialization Scheme: A signer selects two points $(P_1, P_2) \in E(F_p)$ with order q and two random numbers $(d_1, d_2) \in Z_q$ to be the secret keys. The signer computes the two points and

$$Q_1 = -d_1P_1 \text{ and } Q_2 = d_2P_2 \quad (1)$$

Where $(Q_1, Q_2) \in E(F_p)$.

Signature Scheme: There are three rounds in the signature scheme. The signer signs an unknown message m blindly. Let the point

$$Q = (x_Q, y_Q) = Q_1 + Q_2. \quad (2)$$

Step 1 The signer chooses two numbers $(r_1, r_2) \in Zq^*$ securely and computes
$U = r_1P_1 + r_2P_2$ (3)
and sends U to the recipient.

Step 2. On receiving U, the recipient selects two random numbers and computes

$$R^1 = (r^1, y_k) = U + \alpha(P_1 + P_2) + \gamma Q \text{ and } e^1 = (m, r^1) \quad (4)$$

Then, the recipient sends following to the signer.

$$e = e^1 + \gamma \quad (5)$$

Step 3. Consequently, the signer sends following to the recipient.

$$y_1 = r_1 + ed_1 \bmod q \text{ and } y_2 = r_2 + ed_2 \bmod q \quad (6)$$

The blind signature on the unknown message m is

$$\text{Where } y_1^1 = y_1 + \alpha \bmod q \text{ and } y_2^1 = y_2 + \alpha \bmod q. \quad (7)$$

Verification Scheme: On receiving the signature, $(r^1, y_1 y_2^1)$ the recipient validates it by checking
$e^1 = H(m, x_y)$

$$\text{where} (x_w y_v) = y_1^1 p_1 + y_2^1 p_2 + e^1 Q \quad (8)$$

In the following, we show the proposed scheme works correctly.

Theorem 1. (Correctness): *If the tuple (r_1, y_1^1, y_1^2) is a proposed blind signature on ECCs of the message m, it will pass the verification.*

Proof: From Eq(4) and Eq(8), we have

$(r', y_R^1) = R^1 = U + \alpha(P_1 + P_2) + \gamma Q$ and
$(x_w y_v) = (y_1^1 p_1 + y_2^1 p_2 + e^1 Q)$.

We claims that $r^1 = x_v$ as the followings:

$$(x_w y_v) = y_1^1 p_1 + y_2^1 p_2 + e^1 Q$$

From Eq(7)(8)(9), we have

$$= (y_1 + \alpha) p_1 + (y_2 + \alpha) p_2 + e^1 Q)$$
$$= (r_1 + ed_1 + \alpha) p_1 + (r_2 + ed_2 + \alpha) p_2 + e^1 Q$$
$$= (r_1 + e^1 d_1 - \gamma d_1 + \alpha) p_1 + (r_2 + e^1 d_2 - \gamma d_2 + \alpha) p_2 + e^1 Q$$
$$= r_1P_1 + e^1 d_1P_1 - \gamma d_1P_1 + \alpha P_1 + r_2P_2 + e^1 d_2P_2 - \gamma d_2P_2 + \alpha P_2 + e^1 Q$$

Replace Q and U by Eq(1)(2)(3)

$$= (r_1P_1 + r_2P_2) + \alpha(P_1 + P_2)\gamma(-d_1P1 - d_2P_2) - e'(-d_1P_1 - d_2P_2) + e^1$$

Q
$=U+\alpha(P_1+P_2)+\gamma Q- e^1 Q+e^1 Q$
$=U+\alpha(P_1+P_2)+\gamma Q$
$=(r\ ,y_R)$
The above equation can get $r^1=x_v$ and the recipient validates the signature by $e^1=H(m,X_v)$ The signature (r^1,y_1^1,y_2^1) on the message m is valid. Q.E.D.

Security Analysis: Some security of the proposed blind signature on ECCs. We will show the properties of randomness, unlinkability and unforgability as follows. In the proposed scheme, attackers are infeasible to sign a valid signature (r^1,y_1^1,y_2^1) on behalf of the original signer. The signer chooses random numbers (r_1,r_2) and sends $U=r1P1+r2P2$ to the user. To get the random numbers (r_1,r_2) from U is computationally infeasible. Moreover, e^1 is a hash function and γ is a random number. To remove random (r_1,r_2) from signature (r^1,y_1^1,y_2^1) is infeasible, so the signature has randomness property.
The unlinkabiliy property is the signer cannot find the corresponding signature from the record that he ever signed. For each signature i process the signer may record referred a set (U_i,e_i,y_{1i},y_{2i}) during the instance of the protocol. The signer cannot specify the corresponding signature (r_i,y_{1i},y_{2i}).
On the i-th process, the signer have $(y_1=y_{1i}-\alpha_i),(y_2=y_{2i}-\alpha_i)$ and ei and they are blinded by α_i and γ_i respectively. Therefore, the signer cannot specify the corresponding signature (r_i',y_{1i}',y_{2i}') from every .
The attackers may try to derive some forgery signature message $\tilde{m}$. All of the attackers fail on the proposed scheme. First, the attackers given will signature can set a signature (r',y_1',y_2') , because it is untraceable to get $(d1, d2)$ and computationally infeasible to get $(r1, r2)$ from $U=r_1P_1+r_2P_2$. Secondly, given a valid signature (r',y_1',y_2') on message m, it is unable to get another message $\tilde{m}$ with getting pass the verification of signature (r',y_1',y_2') since it is hard to find e' from hash function H with

Implementation and Performance: In the practical views, an ECC whose order is a *160*-bit prime offers approximately the same level of security as discrete logarithm system with a *1024*-bit prime with *160*-bit exponential. The following comparisons on storage requirement and performance are based those parameters.

Storage Requirement: In Table 2, we give a rough comparison of the storage requirements in bits for the proposed blind signature on ECCs and Schnorr blind signature on discrete logarithm cryptosystems. The storage space of system parameters is $(1024*3)=3072$ bits for parameters p, q and g in discrete logarithm cryptosystems, but only $(160*5)=800$ bits for parameters a, b, p and q in ECCs. The key pair take $(1024+160)=1184$ bits in discrete logarithm cryptosystems and only

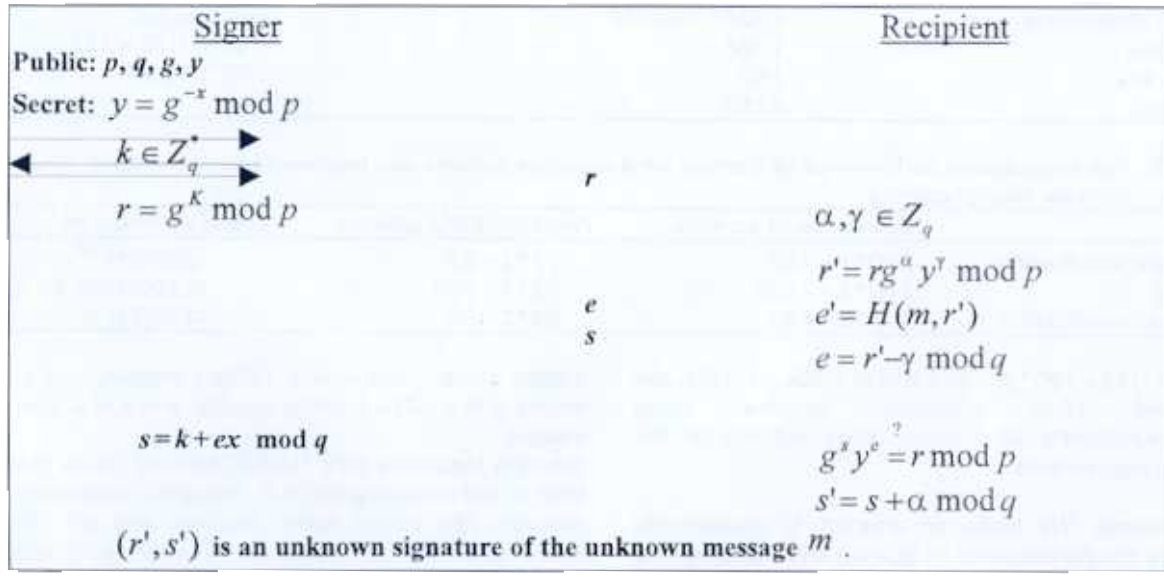

Fig. 1: Schnorr Blind Scheme

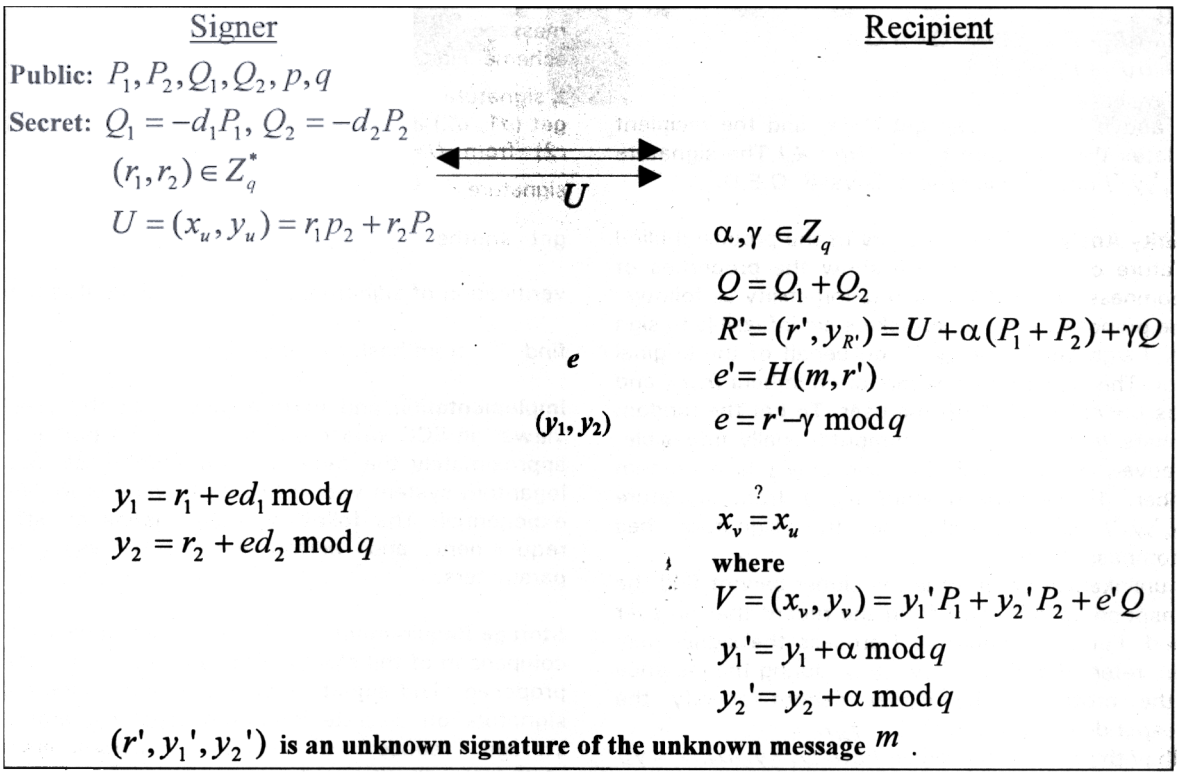

Fig. 2: Proposed Blind Scheme

Table 2: The storage requirements of Schnorr blind scheme and proposed blind scheme in bits

	Schnorr blind scheme	Proposed blind scheme
System Parameters	*1024*3=3072*	*160*5=800*
Public key	*1024*	*(160+1)*2=322*
Private key	*160*	*160*2=320*
Total bits	*4256*	*1442*

Table 3: The comparative performance of Schnorr blind signature scheme and proposed blind scheme in *1024*-bit modular multiplications

	Schnorr blind scheme	Proposed blind scheme	Speed up ration of
Signature initialization	*240*1=240*	*29*2=58*	*(240/28)* ≈ 4
Signing	*240*5=1200*	*29*7=203*	*(1200/203) 6*
Signature verification	*249*2=480*	*29*2=58*	*(480/58) 8*

*((160+1)*2+160*2)=642* bits in ECCs. Totally, the proposed blind signature scheme takes *(1442/4256)34%* of Schnorr blind scheme in the storage requirement.

Performance: We make an attempt to qualitatively compare the performance of Schnorr blind scheme and the proposed blind scheme. These results are presented in Table 3. Those figures should be in making these comparisons under assuming that (1) *kP* where *E* is an elliptic curve, and *k* is a *160*-bit integer; and (2) , where *p* is a *1024*-it prime number and *k* is a *160*-bit integer.

Discrete logarithm take $(1024/160)^2$ *41* times longer than a field multiplication in Z_p. Roughly, computing *kP* requires *160* elliptic curve doubling and *80* elliptic curve addition and elliptic curve doubling or elliptic curve doubling requires 5 field multiplications. On average, computing *kP* requires the equivalent of *1200* field multiplications or *1200/4129 1024*-bit modular

multiplications. On the other hand, computing g^k mod p requires *240 1024*-bit modular multiplications.

We compare Schnorr blind scheme with the proposed scheme and yield a speed up ration of *((240*1)/(29*2))4* in Initialization scheme, *((240*5)/29*7))6* in Signature scheme and *((240*2)/(29*2))8* in Verification scheme.

References

ANSI X9.62, 1997. "American National Standard for Financial Services - Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA)," draft, ASC X9 Secretariat - American Bankers Association.

Bellare, M. and P. Rogaway, 1993. "Random Oracles are Practical: a Paradigm for Designing Efficient Protocols," Proc. of the lst CCCS. pp: 62-73. ACM press.

Chaum, D. 1983. "Blind Signatures for Untraceable Payments," Advances in Cryptology-Crypto'82, (Plenum, 1983).

Chaum, D. , A. Fiat and M. Naor, 1988. "Untraceable Electronic Cash," Advances in Cryptology-Crypto'88, LNCS 403 (Springer-Verlag, 1990), pp: 319-327.

IEEE P1363, 1997. "Standard Specifications for Public-Key Cryptography," draft.

ElGamal, T., 1985. "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms," IEEE Transactions on Information Theory, IT-31, pp: 469-472.

Koblitz, N., 1994. A Course in Number Theory and Cryptography, 2nd edition, Springer-Verlag.

Koblitz, N., 1983. Elliptic Curve Cryptosystems, Mathematics of Computation, 48, pp: 203-209.

Menezes, A., 1993. Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishes.

Miller, V., 1985. "Uses of Elliptic Curves in Cryptography," Advances in Cryptology Crypto'85, LNCS 218 (Springer-Verlag 1986), pp: 417-426.

Okamoto, T., 1992. "Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes," Advances in Cryptography: Crypto'92, LNCS 740 (Spring-Verlag, 1992), pp: 31-53.

Schnorr, C. P., 1989. "Efficient Identification and Signatures for Smart Cards," Advances in Cryptography: Crypto'89, LNCS 435 (Springer-Verlag, 1990), pp: 235-251.