타원곡선의 이산로그문제에 기반을 둔 Blind signature

Blind Signatures Based on the Elliptic Curve Discrete Logarithm Problem

윤중철
고려대 수학과

임종인
고려대 수학과

서광석
서남대 수학과

서창호
전자통신연구소

Abstract

본 논문에서는 Chaum이 처음으로 제안한 개념인 Blind signature를 타원곡선위에서 이산로그문제를 이용해 구현해보고 ECDSA와 Nyberg, Rueppel의 scheme을 Blind signature로 변형시킨 새로운 signature 를 제시한다.

1 Introduction

Blind signature scheme is a protocol that obtaining a signature for a message m from a signer without her seeing the message. Chaum first introduced the concept of the blind signature and demonstrated that scheme with RSA signature. Blind signature can be used in Electronic Commerce(EC), Digital Money, Electronic Voting System. In particular untraceable payment system is an important application. The one who has a account in a bank requests withdrawl the Electronic Money or the Electronic Coin. The bank signs it

using the blind signature scheme and send it to him. The owner of such coin pay with it, and the payee deposit it at the bank. But the bank cannot trace the coin

Since Diffie and Hellman have introduced the concept of public key cyptography, the intractability of the discrete logarithm problem was recognized as the cryptographic importance.

The discrete logarithm problem is the following: Let G be a group of order n, let α be an element of G. Given elements α and $\beta \in G$, find an integer x, $0 \leq x \leq n-1$ such that $\alpha^x = \beta$, provided such an integer exist.

Various groups have been proposed for cryptographic use, But elliptic curve group is spotlighted because elliptic curve discrete logarithm problem(ECDLP) is harder than problems in any other groups especially than the discrete logarithm problem in the finite field. With maintaining the same level of security, the group is smaller than Z_p^*. Consequently Cryptosystems based on the elliptic curve have equivalent security as compared but shorter key size lengths, smaller bandwith, smaller memory requriment and faster and more ease implementation as compared with conventional cryptosystems. These features are especially attractive for security applications where computational power and integrated circuit space is limited such as smart cards, and wireless devices.

In this paper, we present five blind signature schemes based on elliptic curves. Nyberg-Rueppel scheme is constructed on elliptic curves and ECDSA is blinded. Chaum demonstrated a blind signature using RSA signature. We convert the Chaum's demonstration to the elliptic curve discrete logarithm problem(ECDLP). And Camenisch et al's schemes are constructed on elliptic curves.

This paper is organized as follows. Section 2 introduces the Chaum's demonstration using RSA and propose a new scheme using the ECDLP. Section 3 explains Camenish et al's blind signature schemes over elliptic curves. Section 4 summaries the new schemes based on respectively ECDSA , Nyberg-Rueppel scheme over an elliptic curve.

2 Chaum's blind signature

2.1 Chaum's blind signature using RSA signature

Chaum demonstrated the implementation of this scheme using RSA signatures as follows:

Suppose Bob has a message m that he wishes to have signed by Alice, and he does not want Alice to learn anything about m .

Let (n, e) be Alice's public key and d be her provate key.

Step 1 *Bob generates a random value* r *such that* $gcd(n, r) = 1$ *and sends* $m' = r^e \times m \mod n$ *to Alice.*

Step 2 *Alice returns the signed value,* $s' = (m')^d = (r^e m)^d \mod n$ *to Bob.*

Step 3 *Since* $s' = rm^d \mod n$, *Bob can obtain the true signature by computing* $s = s'r^{-1} \mod n$.

The value m' is blinded by the random value r, and hence Alice can derive no useful information about it. Its security(blindness) depends on the intractability of factoring a large integer, so the signer never knows the message.

2.2 Chaum's Blind signature using ECDLP

The following scheme is an elliptic version of Chaum's blind signature. The original demostration uses the intractability of factoring a large integer, but this scheme use the discrete logarithm problem over the elliptic curve group.

We assume here the followings :
Bob wants to Alice to sign the message m blindly.
$E(F_q)$ is an elliptic curve where $q = p^l$, p is a prime.
$\sharp E(F_q)$ is divided by a large prime n.
P is an element of $E(F_q)$ such that the order of P is n .
d is a private key of Alice.
$Q = dP$, P, n are public keys of Alice.

$M = (m, y)$ is a element of $E(F_q)$. (m is not always a x-coordinate of $E(F_q)$ but the probability that m is a x-coordinate of $E(F_q)$ is $\frac{1}{2}$. so we assume here m is a x-coordinate.)

Step 1 *Bob chooses a random value k and compute $M + kP$, then sends $M + kP$ to Alice.*

Step 2 *Alice computes $d(M + kP)$ with his private key d and sends it to Bob.*

Step 3 *Bob computes $d(M + kP) - k(Q)$.*

Since Bob knows $Q = dP$ and k , he can computes $d(M + kP) - k(Q)$.
So,

$$\begin{aligned} d(M + kP) - kQ &= dM + dkP - dkP \\ &= dM \end{aligned}$$

Therefore Bob obtain the signature of Alice for message m. In this scheme, Alice does not know M because of the randomness of k and ECDLP.

3 Camenisch et al's blind sinature using Elliptic curve

Camenisch et al present two new blind signature scheme based on the discrete logarithm problem. One is the blinding of the modified DSA , another is the blinding the Nyberg-Rueppel message recovery scheme. In this paper Camenish et al's scheme is modified based on the elliptic curves.
The assumption of those schemes is same as that of the section 2.2

3.1 Blind signature using the DSA based on the elliptic curve

Step 1 *Alice selects a random number k in the interval $[2, n-1]$, computes $R = kP = (x_1, y_1)$ and sends to Bob.*

Step 2 *Bob chooses an unpredictable number* α, β *such that* $2 \leq \alpha, \beta \leq n-2$ *and computes* $\tilde{R} = \alpha R + \beta P$ *where* $\tilde{R} = (x_2, y_2)$.

Step 3 *Computes* $m' = \alpha m x_1 x_2^{-1} \pmod{n}$ *and sends it to Alice. (If* $x_2 = 0$ *, then go to step II, choose another* α, β*.)*

Step 4 *Alice computes* $\tilde{s} = km' + x_1 d \pmod{n}$ *and sends it to Bob.*

Step 5 *Bob computes* $s = \tilde{s} x_2 x_1^{-1} + \beta m \pmod{n}$.

Step 6 *Bob accepts the signature if* $m^{-1}(sP - x_2 Q) = R$.

The equality of V is as follow;

$$m^{-1}(sP - x_2 Q) = m^{-1}((\tilde{s} x_2 x_1^{-1} + \beta m)P - x_2 dP)$$

Since $\tilde{s} = km' + x_1 d$ and $m' = \alpha m x_1 x_2^{-1}$, $\tilde{s} x_2 x_1^{-1} = \alpha km + x_2 d$.
Hence

$$\begin{aligned} m^{-1}(sP - x_2 Q) &= m^{-1}((\tilde{s} x_2 x_1^{-1} + \beta m)P - x_2 dP) \\ &= m^{-1}((\alpha km + x_2 d + \beta m)P - x_2 dP) \\ &= m^{-1} m(\alpha k + \beta)P \\ &= \alpha(kP) + \beta P \\ &= R \end{aligned}$$

3.2 Blind signature using Nyberg-Rueppel scheme based on the elliptic curve

Step 1 *Alice selects a random number* k *in the interval* $[2, n-1]$*, computes* $R = kP$ *and sends to Bob.*

Step 2 *Bob chooses an unpredictable number* α, β *such that* $2 \leq \alpha, \beta \leq n-2$ *and computes* $\tilde{R} = M + \alpha P + \beta R = (r_1, r_2)$ *and* $m' = r_1 \beta^{-1} \pmod{n}$ *and sends* m' *to Alice.*

Step 3 *Alice computes* $\tilde{s} = m'd + k \pmod{n}$ *and sends* $\tilde{s}$ *to Bob.*

Step 4 *Bob computes* $s = \tilde{s}\beta + \alpha \pmod{n}$. *Bob accepts the signature if* $-sP + r_1(Q) + R = M$.

The equality of IV is as follow;

$$\begin{aligned} -sP + r_1Q + \tilde{R} &= (-\tilde{s}\beta - \alpha)P + r_1(dP) + (M + \alpha P + \beta kP) \\ &= (-\tilde{s}\beta - \alpha + r_1 d + \alpha + \beta k)P + M \end{aligned}$$

Since $\tilde{s} = m'd + k$, $-\tilde{s}\beta = -m'd\beta - k\beta$. Hence

$$\begin{aligned} -\tilde{s}\beta - \alpha + r_1 d + \alpha + \beta k &= -m'd\beta + r_1 d \\ &= -(r_1\beta^{-1})d\beta + r_1 d \\ &= 0. \end{aligned}$$

Therefore $-sP + r_1Q + \tilde{R} = M$.

The procedure of these schemes are same as that of Camenisch et al's, so by the thoerems of Camenisch et al's the message is not unveiled to the signer by these schemes.

4 Blinding the original schemes

In the following , two new blind signature scheme based on the elliptic curve is presented. Although above two schemes use the DSA and Nyberg-Rueppel scheme , they slightly modified those schemes and blind the modified schemes. But we proposed here blind signature using the original ECDSA and Nyberg-Rueppel schemes. It is a slight modification, but we think this modification is sufficient to blind the message because blinding factor uses the ECDLP.

4.1 Blind ECDSA

The following scheme is a blind version of ECDSA. We assume here same situation as in section 2.2.

Step 1 *Bob chooses a random number* α, *computes* $m^{\alpha} \pmod{n}$ *and* $m^{\alpha}P = (x_1, y_1)$ *and sends* $m' = x_1 \pmod{n}$ *to Alice. (Here if* $m' = 0$, *then Bob chooses another random number* α.*)*

Step 2 *Alice select a statistically unique and unprectictable integer k in the interval* $[2, n-2]$.

Step 3 *Compute* $R = kP = (x_2, y_2)$ *and* $r = x_2 \pmod n$. *If* $r = 0$, *then go to step 2.*

Step 4 *Compute* $s = k^{-1}\{h(m') + dr\} \pmod n$, *where* h *is a Secure Hash Algorithm(SHA-1). If* $s = 0$, *then go to step 2.*

Step 5 *The signature for the message* m' *is the pair* (r, s). *Alice sends them to Bob.*

Step 6 *Bob verify that* r *and* s *are integers in the interval* $[1, n-1]$.

Step 7 *Computes* $w = s^{-1} \pmod n$ *and* $h(m')$.

Step 8 *Computes* $u_1 = h(m')w \pmod n$ *and* $u_2 = rw \pmod n$.

Step 9 *Computes* $u_1P + u_2Q = (x_0, y_0)$ *and* $v = x_0 \pmod n$.

Step 10 *Bob accepts the signature if* $v = r$.

4.2 Blind Nyberg-Rueppel scheme

The following scheme is a blind version of Nyberg-Rueppel scheme. We assume here same situation as in section 2.2.

Step 1 *Bob selects a random number* α *in the interval* $[2, n-1]$, *computes and sends to Alice* $M = m^{\alpha}P$.

Step 2 *Alice chooses a statistically indepent and unpredictably number* k *such that* $2 \leq k \leq n-2$.

Step 3 *Computes* $R = M + kP = (r_1, r_2)$, $s = r_1 d + k \pmod n$ *and sends* (R, s) *to Bob.*

Step 4 *Bob accepts the signature if* $-sP + r_1Q + R = M$.

The equality of IV is as follow;

$$\begin{aligned} -sP + r_1Q + R &= (-r_1d - k)P + r_1(dP) + M + kP \\ &= (-r_1d - k + r_1d + k)P + M \\ &= M \end{aligned}$$

When the scheme is applied to real world, It is probable that the messages have similar pattern. So By powering m with a random number α, the message is randomized. Therefore the blindness of the message is higher.

5 Security of the schemes

The proposed schemes cannot prevent the bad behavior of the message sender, so we consider only the behavior of the signer.(Because of this disadvantage, several variation of the original schemes have been proposed e.g. partially blind signature).

The secure blind signature scheme should satisfy the following conditions; The blind message m should not be unveiled to the signer.

If the signer succeed to let the blind message be unblind, then this is euqivalent to solving the ECDLP. So the proposed schemes are secure.

6 Conclusion

We proposed five modified scheme based on the elliptic curve and examine the security of the schemes. These schemes use the blinding factor based on the ECDLP. Now we are studying the partially blind signature using the elliptic curves

References

[1] J. Camenisch, J. M. Piveteau, M. Stadler, *Blind Signatures Based on the Discrete Logarithm Problem*, Proc. EUROCRYPT 94, pp. 428-432.

[2] D. Chaum,*Blind Signature Systems*, Crypt 83,Plenum, p153

[3] N. Koblitz, *Elliptic Curve Cryptosystems*, Vol. 48, Math. of Comp., 1987, pp. 203-209.

[4] A. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publications, 1993.

[5] K. Nyberg, R. A. Rueppel, *A New Signature Scheme Based on the DSA Giving Message Recovery*,1st ACM Conference on computer and Communications Security.

[6] A. Menezes, S. A. Vanstone, *Elliptic Curve Cryptosystems and Their Implementations*, J. of Cryptology, 1990.