A Novel Blind Signature Scheme Based on Nyberg-Rueppel Signature Scheme and Applying in off-line Digital Cash

Debasish Jena, Sanjay Kumar Jena and Banshidhar Majhi
National Institute of Technology Rourkela
Rourkela-769 008, Orissa, India
debasishjena@hotmail.com, {skjena, bmajhi}@nitrkl.ac.in

Abstract

In this paper, a novel Blind Signature Scheme (BSS) based on Nyberg-Rueppel Signature Scheme (NRSS) using Elliptic Curve Discrete Logarithm Problem (ECDLP) has been proposed. Blind signature allows a requester to obtain signature from a signer on any document, in such a way that the authority learns nothing about the message that is being signed. Blind Signatures are useful in protocols that guarantee the anonymity of the participants. As an instance, the application of the scheme in off line digital cash has been described. The proposed scheme can be easily extended to E-voting and others applications where the requester needs a blind signature on the message.

Keywords: *Blind signature, Elliptic Curve, ElGamal, Digital Cash, RSA.*

1. Introduction

With growing importance of sender privacy in various schemes such as “digital cash”, electronic voting protocol, blind signature schemes are gaining momentum. Blind signature is a form of digital signature in which the signer doesn’t have authority over message, as also a third party could able to verify without knowing the secrets of both the parties that are involved in signature.

The electronic payment system is one of the most important applications in electronic commerce. There are two types of system for digital cash, namely, the on-line system and off-line system. In on-line case, the customer needs to interact with a bank (via modem or network) to conduct a transaction with a third party. But in case of off-line system, the customer can conduct a transaction without having to directly involve a bank. In such a scenario, the services need to be authenticated and secure. Non-repudiation is one of the vital aspects where the requester and the service providers can be prohibited of denying the action made on the transaction made between them. Signature scheme is most widely used mechanism for the purpose. But for untraceability property we require a mechanism where, the requester needs to get the authentication in the message from the signer without really exposing the message content to the signer [1,2]. For the aforesaid purpose, blind signature scheme was introduced by David Chaum in 1982 [3] where the content of a message is blinded before sending it to the signer for signature. The signer signs on the blind message using his/her private key and anyone can verify the legitimacy of the signature using signer’s public key. This procedure can be well explained with an example taken from the familiar world of paper documents. The paper analogous of a blind signature can be implemented with carbon paper lined envelopes. Putting a signature on the outside of such an envelope leaves a carbon copy of the signature on a slip of paper within the envelope [3]. Any BSS must satisfy the following properties [3,4,5].

- *Correctness:* the correctness of the signature of a message signed through the signature scheme can be checked by anyone using the signer’s public key.
- *Authenticity*: a valid signature implies that the signer deliberately signed the associated message.
- *Unforgeability*: only the signer can give a valid signature for the associated message.
- *Non-reusability*: the signature of a document can not be used on another document.
- *Non-repudiation*: the signer can not deny having signed a document that has valid signature.
- *Integrity*: ensure the contents have not been modified.
- *Blindness:* the content of the message should be blind to the signer; the signer of the blind signature does not see the content of the message.

0-7695-3068-0/07 $25.00 © 2007 IEEE
DOI 10.1109/ICIT.2007.16

IEEE computer society

- *Untraceability:* the signer of the blind signature is unable to link the message-signature pair even when the signature has been revealed to the public.

Blind signature scheme suggested by Mohammed et al. [6] is based on ElGamal, has been proved by Hwang et al. [7] that it does not satisfy correctness property. In this scheme when the requester obtained the blinded signature from the signer, he/she could not unblind it to acquire the desired signature. Based on Discrete Logarithm Problem (DLP) a blind signature scheme has been suggested by Camenisch et al. [8] which is simpler than the scheme proposed by Lee et al. [9].

In this paper, we propose a new BSS based on variation of Nyberg-Rueppel Signature Scheme [10] using Elliptic Curve Discrete Logarithm Problem (ECDLP). In the Section 2, basic concept of Elliptic Curve is discussed. In Section 3, firstly, the variation of NRSS using ECDLP has been explained and then the proposed BSS scheme is discussed using a communication illustration between a requester and signer. The correctness of the proposed BSS has been made in Section 4. In Section 5, off-line digital cash is explained where proposed BSS is being used. Finally, Section 6 describes the concluding remarks.

2. Elliptic curve over finite field

The use of Elliptic Curve Cryptography was initially suggested by Neal Koblitz [11] and Victor S. Miller [12] and after that many researchers have suggested different application of Elliptic Curve Cryptosystems. Elliptic curve cryptosystems over finite field have some advantages like the key size can be much smaller compared to other cryptosystems like RSA, Diffie-Hellman since only exponential-time attack is known so far if the curve is carefully chosen [13] and elliptic curve discrete logarithms might be still intractable even if factoring and multiplicative group discrete logarithm are broken. ECC is also computationally efficient than the first generation public key systems such as RSA and Diffie-Hellman.

2.1. Elliptic curve groups over F_q

A non-super singular Elliptic curve E over F_q can be written as:

$$E : y^2 \bmod q = (x^3 + ax + b) \bmod q \qquad \cdots\cdots(1)$$

where $(4a^3 + 27b) \bmod q \neq 0$

The point P in the Elliptic curve is described by the coordinates (x, y) where $x, y \in F_q$ that satisfy the equation (4) together with a "point of infinity" denoted by O form an abelian group $(E, +, O)$ whose identity element is O.

2.1.1. Addition of two distinct points *P* and *Q*. The negative of the point $P = (x_1, y_1)$ is the point $-P = (x_1, -y_1)$. If $P(x_p, y_p)$ and $Q(x_q, y_q)$ are two distinct points such that P is not $-Q$, then

$$P + Q = R \qquad \cdots\cdots(2)$$

where $R = (x_r, y_r)$

$s = (y_p - y_q)/(x_p - x_q) \bmod \quad q$

where s is the slope of the line passing through P and Q

$x_r = (s^2 - x_p - x_q) \bmod \quad q \; and$

$y_r = (-y_p + s*(x_p - x_r)) \bmod q$

3. Proposed BSS scheme

In this section, firstly the variation NRSS using ECDLP is explained. Subsequently we propose a novel efficient and low computation BSS.

3.1. Modified NRSS using ECDLP

Initially the curve parameters (*q,FR,a,b,G,n,h*) must be agreed upon by signer and receiver. Signer must have a key pair suitable for elliptic curve cryptography, consisting of a private key d_B (a randomly selected in the interval [1,n-1]) and a public key Q where $Q = d_B G$ .When a signer wants to send a signed message m to receiver, he/she must generate a digital signature (r, s) as follows:

Select k randomly between [1, n-1] and generate $R, r \; and \; s$ as:

$R = mkG$

$wher \quad R = (x_R, y_R)$

$r = x_R \bmod \quad n \quad and \quad r != 0$

$s = rd_B + mk \quad \bmod n \quad and \; s != 0$

After receiving (r, s) from signer, the receiver can verify the correctness of the signature on the message by using following equation:

$$sG = rQ + R \qquad ......(3)$$

3.1.1. Correctness. The verifier only verifies the pair (r, s) and message m by using the above equation. The correctness of the equation $sG = rQ + R$ is as follows:

$$s = rd_B + mk$$
$$\Rightarrow sG = rd_B G + mkG$$
$$\Rightarrow sG = rQ + R$$

3.2. Blind signature scheme

Digital signature scheme based on discrete logarithms uses a random number k which is different in each signature [14,15]. This valuable property makes two signatures on the same message different, which is not true in case of RSA based signature scheme. The underlying principles of the new blind signature scheme are explained using a banking example where the requester needs a document to be signed by the signer without disclosing contents of the document. The different phases of the signature scheme are explained below.

A. Initially Signer should do the following

- Signer will select d_B randomly in the interval of [0, n-1] as secret key and compute Q as public key. Where $Q = d_B G$.
- Select $\tilde{k}$ randomly and computes
  $$\tilde{R} = \tilde{k}G, \quad \tilde{R} = (\tilde{x}_r, \tilde{y}_r) \qquad \cdots\cdots(4)$$
  $$\tilde{r} = \tilde{x}_r \bmod n$$
- It will send $\tilde{R}$ to requester.

B. After receiving the above value Requester should request for signature by computing the values as follows:

- Customer select two integer α and β randomly.
- Compute the following value
  $$R = m\alpha G + \tilde{R}\beta \qquad \cdots\cdots(5)$$
  $$where\, R = (x_R, y_R)$$
  $$r = x_R \quad \bmod \quad n$$
- Compute the blind message as
  $$\tilde{m} = r\beta^{-1} \quad \bmod\, n \qquad \cdots\cdot(6)$$
- Sends blind messages $\tilde{m}$ to Bank for signature

C. Signer should do the followings

- The Signer receives blind message from requester and treats it as any ordinary message since the Signer does not recognize the blinding. The Signer computes $\tilde{s}$ as
  $$\tilde{s} = \tilde{m}d_B + \tilde{k} \quad \bmod \quad n \qquad \cdots\cdots(7)$$
- After computing the blind messages $\tilde{s}$, Signer sends it to Requester as signature

D. Requester should do the followings to recover the real signature s after receiving the blinded signature $\tilde{s}$ from the Signer:

- Compute the *s* as follows
  $$s = \tilde{s}\beta + \alpha m \quad \bmod \quad n \qquad \cdots\cdots(8)$$
- Now the complete signature pair of the message *m* is *(r, s) and R* which are known to Requester but not to the Signer.
- Verification by the Requester or any one can be done by the following equation
  $$G = u_1 Q + u_2 R \qquad \ldots\ldots(9)$$
  $$where\ u_1 = rw \bmod n$$
  $$u_2 = w \bmod n$$
  $$w = s^{-1} \bmod n$$

4. Correctness of proposed scheme

The correctness of our scheme can be easily verified as follows. The verifier has only digital signature *(r,s,R)* of message m for verification. The customer extracts the signature by using (8), therefore

$$s = \tilde{s}\beta + \alpha m \quad \bmod \quad n$$
$$= (\tilde{m}d_B + \tilde{k})\beta + \alpha m \quad \bmod \quad n$$
$$= (r\beta^{-1}\, d_B + \tilde{k})\beta + \alpha m \quad \bmod \quad n$$
$$= r\, d_B + \tilde{k}\beta + \alpha m \quad \bmod \quad n$$
$$Finally,$$
$$s = r\, d_B + \tilde{k}\beta + \alpha m \qquad \cdots\cdots(10)$$

Now multiplying both sides of (10) by Generator G we have

$$sG = r\, d_B G + \tilde{k}\beta G + \alpha m G$$
$$\Rightarrow sG = rQ + (\tilde{R}\beta + \alpha m G)$$
$$\Rightarrow sG = rQ + R$$

5. Off-line digital cash

The following procedure explained an untraceable off-line electronic payment protocol assuming that the consumer wants to purchase some goods from the merchant and that both have bank accounts with Bank:

A. Withdrawal Request

- Customer creates an electronic coin and blinds it.
- Customer sends the blinded coin to the Bank with a withdrawal request
- Bank digitally signs the blinded coin.
- Bank sends the signed-blinded coin to customer and debits his/her account.
- Customer unblinds the signed coin.

B. Payment

- Customer gives the coin to the Merchant.
- Merchant verifies the Bank's digital signature.
- Merchant gives customer the merchandise.

C. Deposit

- Merchant sends coin to the Bank.
- Bank verifies its own digital signature for authentication.
- Bank verifies that coin has not already been spent using cut and choose technique.
- Bank enters the coin in the spent-coin database.
- Bank credits Merchant's account.

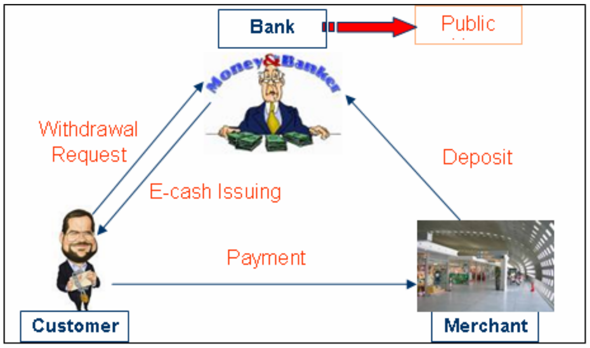

Figure 1. Off-line digital cash

6. Conclusion

This paper suggests a secure and efficient blind signature scheme based on the Elliptic Curve Discrete Logarithm Problem. The scheme utilizes fewer number bits due to inherent property of elliptic curve as compared to its public key counterparts such as RSA. The proposed BSS is suitably illustrated using off-line digital cash. The validity of the proposed scheme has been made.

7. References

[1] D. Chaum, "Blind signatures for untraceable payment", *Advances in cryptology, CRYPTO'82*, Lect. Notes Computer Science, (Springer-Verlag, 1998), pp. 199-203.

[2] D. Chaum,A. Fiat and M. Naor, "Untraceable electronic cash," *Advances in cryptology*, *CRYPTO'RX*, Lect. Notes Computer Science, (Springer-Verlag, 1990), pp. 319-327.

[3] D. Chaum, "Blind Signature Systems," U.S. Patent 4,759,063, 19 Jul 1988.

[4] Chun-I Fan, W.K. Chen, and Y. S. Yeh, "Randomization enhanced Chaum's blind signature scheme," *Computer Communications*, vol. 23, pp. 1677–1680, 2000.

[5] Zuhua Shao, "Improved user efficient blind signatures," *Electronics Letters*, vol. 36, no. 16, pp. 1372–1374, 2000.

[6] E. Mohammed, A. E. Emarah, and K. El-Shennawy, "A blind signatures scheme based on ElGamal signature," in IEEE/AFCEA EUROCOMM 2000 Information Systems for Enhanced Public Safety and Security, pp. 51–53, 2000.

[7] Min-Shiang Hwang and Yuan-Liang Tang Yan-Chi Lai. " 'Comment on' "A Blind Signature Scheme Based On ElGamal Signature"," Technical Report CYUT-IM-TR-2001-010, CYUT, Aug. 2001.

[8] J. L. Camenisch, J. M. Piveteau and M. A. Stadler, "Blind Signatures Based on the Discrete Logarithm Problem," *Advances in Cryptology-EUROCRYPT'94*, Rump session, pp. 428-432, 1994.

[9] C. C. Lee, M. S. Hwang and W. P. Yang, "A New Blind Signature based on the Discrete Logarithm Problem for Untraceability," Applied Mathematics and Computation, vol., pp. 837-841, May 2005.

[10] K. Nyberg, R.A. Rueppel, "A New Signature Scheme Based on the DSA Giving Message Recovery", 1st ACM Conference on Computer and Communications Security, November 3-5, Fairfax, Virginia

[11] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, 48, 1987, pp. 203-209.

[12] V. Miller, "Uses of Elliptic Curve in Cryptography," *Advances in Cryptography*, Proceedings of Crypto'85, Lectures notes on Computer Sciences, 218, Springer-Verlag, 1986, pp. 417-426.

[13] N. Koblitz, "CM-Curves with Good Cryptographic Properties," Proceeding of Crypto'91, 1992.

[14] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[15] Doug Stinson, *Cryptography Theory and Practice*, Second Edition, CRC Press, Inc, 2002.