A NOVEL ECDLP-BASED BLIND SIGNATURE SCHEME

Debasish Jena, Saroj Kumar Panigrahy, *Bibhudendra Acharya and Sanjay Kumar Jena
Department of Computer Science & Engineering
*Department of Electronics & Communication Engineering
National Institute of Technology Rourkela, India

Abstract—*In this paper, a novel Blind Signature Scheme (BSS) based on Elliptic Curve Discrete Logarithm Problem (ECDLP) has been proposed. The signer signs the encrypted message after receiving it from the requester. Hence the signer has no scope to learn the contents of the message that he has signed. But there is a scope to verify the authenticity of the signature on the original message by the requester and any other third party. The model has been validated using a customer and bank example and the proof of correctness has been made. The applicability of the proposed scheme can be extended to e-voting and others where the requester needs a blind signature on the message.*

Keywords: Blind signature, Elliptic Curve, ElGamal, Digital Signature, RSA.

Introduction

Transaction over the Internet has become an essential feature in almost all business as well as official environment. 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 in some applications like e-voting, e-cash etc. 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 signature and sent to the signer. 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.
- *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 ECDLP. The proposed scheme is based on a variation of the ElGamal signature scheme which satisfies all the properties of BSS. In the Section 2, basic concept of Elliptic Curve is discussed. In Section 3, the proposed BSS scheme is elaborated using a communication illustration between a customer and a bank. The correctness of the proposed BSS has been made in Section 4. Finally, Section 5 describes the concluding remarks.

Elliptic Curve Groups over F_q

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

$$E: y^2 \bmod q = (x^3 + ax + b) \bmod q \quad \text{where } (4a^3 + 27b) \bmod q \neq 0 \qquad (1)$$

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.

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

$$P + Q = R \quad \text{where } R = (x_r, y_r) \quad s = (y_p - y_q)/(x_p - x_q) \bmod q \qquad (2)$$

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

$$x_r = (s^2 - x_p - x_q) \bmod q \text{ and}$$
$$y_r = (-y_p + s*(x_p - x_r)) \bmod q$$

Doubling the point P

Provided that y_p is not 0,

$$2P = R(x_r, y_r) \qquad \ldots (3)$$

$$\therefore s = ((3x_p^2 + a)/(2y_p)) \bmod q$$
$$x_r = (s^2 - 2x_p) \bmod q \text{ and}$$
$$y_r = (-y_p + s(x_p - x_r)) \bmod q$$

The elliptic curve discrete logarithm problem is defined as follows [14].

Definition 1. Let E be an elliptic curve over a finite field F_q and let $P \in E(F_q)$ be a point of order n. Given $Q \in E(F_q)$, the elliptic curve discrete logarithm problem is to find the integer $d \in [0, n-1]$, such that $Q = dP$.

Proposed Bss Scheme

The scheme is based on the variation of Elliptic Curve Digital Signature. Digital signature scheme based on discrete logarithms uses a random number *k* which is different in each signature [13, 14]. 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 customer (requester) needs a document to be signed by the bank (signer) without disclosing contents of the document. The different phases of the signature scheme are explained below.

Initially Bank should do the following:

1. Bank will select d_B randomly in the interval of [0, n-1] as secret key and compute Q as public key. Where $Q = d_B G$.

2. Select $\tilde{k}$ randomly and computes

$$\tilde{R} = \tilde{k}G, \quad R = (\tilde{x}_r, \tilde{y}_r) \quad \tilde{r} = \tilde{x}_r \bmod n \qquad (4)$$

3. It will send $\tilde{R}$ to customer.

After receiving the above value Customer should request for signature by computing the values as follows:

1. Customer select two integer a and b randomly.
2. Compute the following value

$$R = a\tilde{R} + bG, \quad R = (x_r, y_r)$$
$$r = x_r \mod n \tag{5}$$

3. Compute the blind message as

$$\tilde{m} = am\tilde{r}r^{-1} \mod n \tag{6}$$

4. Sends blind messages $\tilde{m}$ to Bank for signature

Bank should do the followings:

1. The Bank receives blind message from Customer and treats it as any ordinary message since the Bank does not recognize the blinding. The Bank computes $\tilde{s}$ as

$$\tilde{s} = (d_B\tilde{r} + \tilde{k}\tilde{m}) \mod n \tag{7}$$

2. After computing the blind messages $\tilde{s}$, Bank sends it to Customer as signature

Customer should do the followings to recover the real signature s after receiving the blinded signature $\tilde{s}$ from the Bank:

1. Compute the s as follows

$$s = \tilde{s}\tilde{r}^{-1}r + bm \mod n \tag{8}$$

2. Now the complete signature pair of the message *m* is: (*r, s*) *and R* which are known to Customer but not to the Bank.
3. Verification by the customer or anyone can be done by the following equation

$$G = u_1Q + u_2R \tag{9}$$

where

$$u_1 = rw \mod n$$
$$u_2 = mw \mod n$$
$$w = s^{-1} \mod n$$

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

$$\begin{aligned} s &= \tilde{s}\tilde{r}^{-1}r + bm \mod n \\ &= (d_B\tilde{r} + \tilde{k}\tilde{m})\tilde{r}^{-1}r + bm \mod n \\ &= (d_B\tilde{r} + \tilde{k}(am\,\tilde{r}r^{-1}))\tilde{r}^{-1}r + bm \mod n \\ &= d_Br + \tilde{k}am + bm \mod n \end{aligned}$$

Finally,

$$s = d_Br + \tilde{k}am + bm \tag{10}$$

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

$$\begin{aligned} sG &= d_BrG + m(\tilde{k}aG + bG) \\ \Rightarrow sG &= rQ + m(a\tilde{R} + bG) \\ \Rightarrow sG &= rQ + mR \\ \Rightarrow G &= rs^{-1}Q + ms^{-1}R \end{aligned}$$

The proposed Blind Signature Scheme is depicted in Fig. 1.

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 a bank example. To validate the scheme the correctness of the scheme has also been proved.

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

[11] 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.

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

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

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

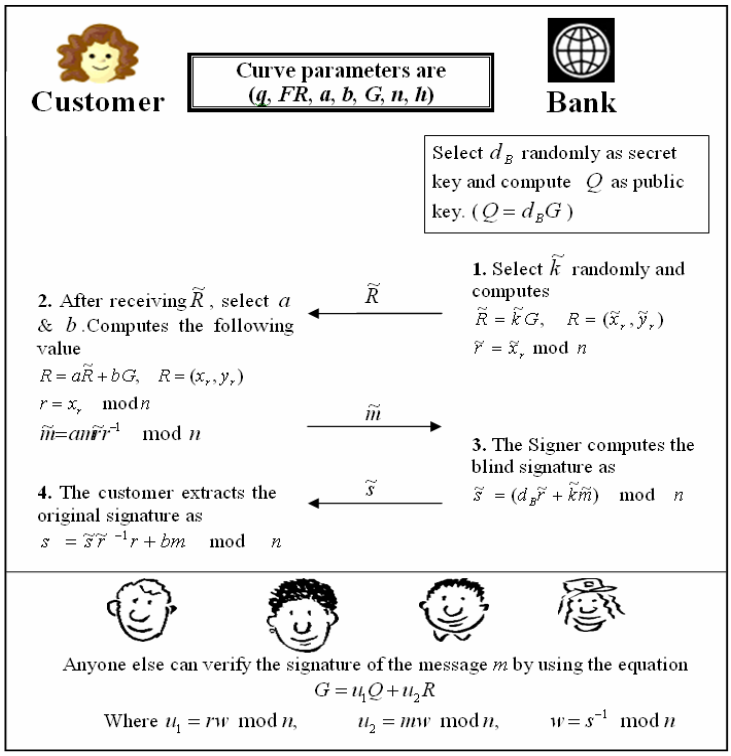

Figure 1. Proposed Blind Signature Scheme