International Journal of Computer and Communication Technology

Volume 3 | Issue 2 Article 13

April 2012

Improved Self-certified Partially Blind Signature Scheme

Binayak Kar
Department of Computer Science and Engineering Nalanda Institute of Technology, Bhubaneswar 754 005, India, binayakdilu@rediffmail.com

Pritam Prava Sahoo
Department of Computer Science and Engineering Nalanda Institute of Technology, Bhubaneswar 754 005, India, sahoo_pritam@rediffmail.com

Asif Uddin Khan
Department of Computer Science and Engineering Nalanda Institute of Technology, Bhubaneswar 754 005, India, asifkhan.iiit@gmail.com

Improved Self-certified Partially Blind Signature Scheme

Binayak Kar, Pritam Prava Sahoo
Department of Computer Science and Engineering
Nalanda Institute of Technology, Bhubaneswar 754 005, India
{binayakdilu, sahoo_pritam}@rediffmail.com

Asif Uddin Khan
Department of Computer Science and Engineering
Nalanda Institute of Technology, Bhubaneswar 754 005, India
asifkhan.iiit@gmail.com

***Abstract*—Blind signature allows one user to get a signature without giving the signer any information about the actual message or the resulting signature. In this paper, we aim to improve the recently proposed Lin et al.'s Self-certified Partially Blind Signature Scheme[1] in order to withstand the security flaw in their scheme. The security of the improved scheme is enhanced in the blind signing phase of the scheme. The analysis shows that the proposed scheme resolves security problem in Lin et al.'s scheme and also meets the aspects of security features needed by a partial blind signature.**

Keywords- Partial blind signature; self-certified; bilinear pairing; security.

I. INTRODUCTION

Blind signature was introduced by D.Chaum [4]. It can provide an anonymity of signed message. Since it was introduced, blind signature schemes have been used in numerous applications, most prominently in anonymous voting and anonymous e-cash. Blind signature[3,4] is a very useful cryptographic technique, which allows a user to get a signature without giving the signer any information about the actual message or the resulting signature. A typical blind signature scheme must satisfy the following two fundamental characteristics: *Blindness* and *Unforgeability*.

Blindness: A blind signature allows a user to obtain a valid signature on message m without revealing anything about the message m to the signer. In addition, the signature is not traceable in the sense that the signer cannot determine when he or she signed this message after the signature is published, although he or she knows that it is really signed by him or her.

Unforgeability: Only the original signer can generate valid signatures, while anyone else cannot.

There are many blind signature schemes[5,6] are used in a practical electronic cash system, they are subject to some common problems, such as the unlimited growth of the bank's database which keeps all the spent e-coins for preventing double spending and the bank's uninscribing the value on the blindly issued e-coins. To cope with these problems, the concept of partially blind signature was introduced. A partially blind signature is an extension of blind signature that allows a signer to produce a blind signature on a message for a user. The signature also explicitly includes commonly agreed information which remains clearly visible despite of the blinding process. Because of the partial blindness property, a partially blind signature scheme is more efficient than ordinary blind signature schemes when it is used in an electronic cash system. Therefore, in recent years, many partially blind signature schemes [7, 8] have appeared.

The remainder of this paper is organized as follows. In Section II, we provide the basic concept of bilinear pairing. In Section III, we review Lin *et.al*'s blind signature scheme. In Section IV we analyze Lin *et.al*'s scheme to show that their scheme is insecure. We then propose an improvement of Lin et al.'s scheme in Section V. We analyze the improved scheme in Section VI and we give performance comparison of our scheme with Lin et al.'s scheme. Finally, we conclude the paper in Section VII.

II. BASIC CONCEPTS ON BILINEAR PAIRINGS

Bilinear pairing is an important cryptographic primitive

and has recently been applied in many positive applications

in cryptography . Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group of the same prime order q . We assume that the discrete logarithm problems in both G_1 and G_2 are hard. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ which satisfies the following properties:

Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$ for $P, Q \in G_1$ and for all $a, b \in Z_q$.

Non-degenerate: There exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.

Computability: There exist an efficient algorithm to compute $e(P, Q)$ for any $P, Q \in G_1$

From [2], we note that such a bilinear pairing can be realized using the modified Weil pairing associated with super singular elliptic curve.

Bilinear Parameter Generator: A bilinear parameter generator Gen is a probabilistic algorithm that takes a security parameter k as input and outputs a 5-tuple

(q, G_1, G_2, e, P) as the bilinear parameters, including a prime number q with $|q| = k$, two cyclic groups G_1, G_2 of the same order q, an admissible bilinear map $e: G_1 \times G_1 \to G_2$ and a generator P of G_1.

III. Review of Lin et.al's Self-certified Partially Blind Signature Scheme

In this section, we briefly review Lin *et.al*'s self-certified partially blind signature scheme [1]. The scheme consists of the following phases.

Setup: Given a security parameter k, the trusted system authority **SA** first generates 5−tuple (q, G_1, G_2, e, P) by running the bilinear parameter generator $Gen(k)$, then choose $s \in_R Z_q$ as master key kept by himself and compute $P_{pub} = sP$. Next, **SA** also picks two cryptographic hash functions $H: \{0,1\}^* \to G_1$, $H_1: \{0,1\}^* \to Z_q$ and outputs the system parameters **params** = $(q, G_1, G_2, H, H_1, P_{pub}, e, P)$.

KGen: When a signer A with his identity ID_A wants to join the system, A first chooses a number $x_A \in_R Z_q$ as his partial private key and computes the corresponding public key $P_A = x_A P$. Then A sends (ID_A, P_A) to the trusted system authority **SA**. After receiving (ID_A, P_A), **SA** computes the partial private key $d_A = sH(ID_A \| P_A)$ with master key s and returns it to A via a secure channel.

Clearly, A can check the validity of d_A by the equation $e(d_A, P) = e(H(ID_A \| P_A), P_{pub})$.

BSign: The signer A and a user B first negotiate common information **info**= Δ. Then, to obtain a blind signature on message m, they execute the following steps:

The signer A first select a random number $r \in_R Z_q$ to compute R^1 and S^1, where $R^1 = rP$, $S^1 = rH(ID_A \| P_A)$. Then sends (R^1, S^1) to B.

After receiving (R^1, S^1), B randomly select three numbers $\alpha, \beta, \gamma \in Z_q$ to compute

$R = \alpha R^1 + \gamma(P_{pub} + P_A)$

$S = \alpha S^1 + \alpha\beta H(ID_A \| P_A) - \gamma H(\Delta)$

$h = \alpha^{-1} H_1(m, R, S) + \beta$ and send h to A.

A computes $\bar{\varsigma}$ and sends it to user B, where $\bar{\varsigma} = (h + r)(x_A H(ID_A \| P_A) + d_A) + rH(\Delta)$

The user B unblinds the received message $\bar{\varsigma}$ as ς

Where $\varsigma = \alpha\bar{\varsigma}$

The resultant blind signature of the message m is (S, R, ς)

Verify: The resultant signature is valid if it satisfies the following equation.

$$e(\varsigma, P) = e(S + H_1(m, R, S)H(ID_A \| P_A), P_{pub} + P_A)e(H(\Delta), R)$$

IV. Attack on Lin et.al's Self-certified Partially Blind Signature

Lin *et.al* claimed that their self-certified partially blind signature scheme [1] was secure against chosen message attack. In a self-certified signature, a user is able to freely choose his public key and his public key can be verified implicitly. In the followings, we show that the scheme is insecure, namely, anyone can produce a forged signature on arbitrary message m in the name of other user by analyzing Lin *et.al*'s self-certified partially blind signature.

Let an adversary produces a forged signature on message m in the name of identity ID_i, the attack is as follows:

Step 1. Select randomly $r \in Z_q$ and set the public key of identity ID is $P_i = rP - P_{pub}$

Step 2. Select $k \in Z_q$ randomly.

Compute : $R = kP$

Step 3. Choose $S \in \mathbb{G}_1$ randomly and compute

$\varsigma = r(S + H_1(m, R, S)H(ID_i \| P_i)) + kH(\Delta)$

Step 4. Finally the forged signature of the message m is (R, S, ς)

Step 5. In the following we are showing the validity of the forged message.

$$e(\varsigma, P) = e(r(S + H_1(m, R, S)H(ID_i \| P_i)) + kH(\Delta), P)$$

$$= e(S + H_1(m, R, S)H(ID_i \| P_i), rP)e(H(\Delta), kP)$$

$$e(H(\Delta), R) = e(S + H_1(m, R, S)H(ID_i \| P_i), P_{pub} + P_i)e(H(\Delta), R)$$

According to the verification equation of Section-III, our attack is valid. Hence Lin et.al's scheme is not secure against unforgeability attack.

V. THE IMPROVED SCHEME

In this section, we describe our improved self-certified partially blind signature scheme in order to withstand the security flaws of Lin *et. al*'s blind signature scheme discussed in Section IV. We use the same set of system parameters as used in Lin *et. al*'s blind signature scheme, which are listed in Section III.

A. *Key generation algorithm KGen:*

This phase consists of the following steps.

a) When a signer A with his identity ID_A wants to join the system, A first chooses a number $x_A \in_R Z_q$ as his partial private key and computes the corresponding public key $P_A = x_A P$.

b) Then the user A *sends* (ID_A, P_A) *to the trusted system authority* ***SA***.

c) After receiving (ID_A, P_A) from the user A, **SA** computes the partial private key $d_A = sH(ID_A \| P_A)$ with master key s and returns it to user A via a secure channel.

d) The user A *can check the validity of* d_A *by the equation*.

$$e(d_A, P) = e(H(ID_A \| P_A), P_{pub}).$$

B. *Blind signing algorithm BSign:*

The signer A and a user B first negotiate common information **info**= Δ. Then, to obtain a blind signature on message m, they execute the following steps:

Step1. The signer A first select a random number $r \in_R Z_q$.

And it computes:

$R^1 = (r + x_A)P$,

$S^1 = rH(ID_A \| P_A)$.

Finally the signer A sends (R^1, S^1) to the user B.

Step2. After receiving (R^1, S^1) from the signer A, the user B randomly select three numbers $\alpha, \beta, \gamma \in Z_q$.

Then the user B computes the followings.

$R = \alpha R^1 + \gamma(P_{pub} + P_A)$

$S = \alpha S^1 + \alpha\beta H(ID_A \| P_A) - \gamma H(\Delta)$

$h = \alpha^{-1} H_1(m, R, S) + \beta$

and sends h to the signer A.

Step3. The signer A computes $\bar{\varsigma}$ after receiving h from the user B.

$\bar{\varsigma} = (h + r)(x_A H(ID_A \| P_A) + d_A) + (r + x_A)H(\Delta)$

And send $\bar{\varsigma}$ to the user B.

Step4. Finally, the user B unblinds the received message $\bar{\varsigma}$ as ς. Where

$\varsigma = \alpha\bar{\varsigma}$

$= \alpha(h + r)(x_A H(ID_A \| P_A) + d_A) + (r + x_A)\alpha H(\Delta)$

Step5. In the end , the resulting signature for message m and agreed information Δ is $\sigma = (R, S, \varsigma)$.

C. *Signature verifying algorithm Verify:*

The validity of the signature $\sigma = (R, S, \varsigma)$ can be checked by the following equality.

$e(\varsigma, P)$

$= e(S + H_1(m, R, S)H(ID_A \| P_A), P_{pub} + P_A)e(H(\Delta), R)$

If it holds, the signature $\sigma = (R, S, \varsigma)$ is accepted as valid, otherwiseit is rejected.

VI. ANALYSIS OF THE IMPROVED SCHEME

A. *Correctness of signature verification:*

The consistency of the signature verification phase can be verified as follows.

$$e(S + H_1(m, R, S)H(ID_A \| P_A), P_{pub} + P_A)e(H(\Delta), R)$$

$$= e(\alpha S^1 + \alpha\beta H(ID_A \| P_A) - \gamma H(\Delta) + H_1(m, R, S)$$

$$H(ID_A \| P_A), P_{pub} + P_A)e(H(\Delta), \alpha R^1 + \gamma(P_{pub} + P_A))$$

$$= e(\alpha r H(ID_A \| P_A) + \alpha\beta H(ID_A \| P_A) - \gamma H(\Delta) + H_1(m, R, S)$$

$$H(ID_A \| P_A), P_{pub} + P_A)e(H(\Delta), \alpha(r + x_A)P + \gamma(P_{pub} + P_A))$$

$$= e((\alpha r + \alpha\beta + H_1(m, R, S))H(ID_A \| P_A) - \gamma H(\Delta), P_{pub} + P_A)$$

$$e(H(\Delta), \alpha(r + x_A)P)e(H(\Delta), \gamma(P_{pub} + P_A))$$

$$= e((\alpha r + \alpha h)H(ID_A \| P_A), (s + x_A)P)e(H(\Delta), \alpha(r + x_A)P)$$

$$= e(\alpha(r + h)H(ID_A \| P_A)(s + x_A), P)e(\alpha(r + x_A)H(\Delta), P)$$

$$= e(\alpha(r + h)(x_A H(ID_A \| P_A) + sH(ID_A \| P_A)), P)$$

$$e(\alpha(r + x_A)H(\Delta), P)$$

$$= e(\alpha(r + h)(x_A H(ID_A \| P_A) + d_A)$$

$$+ \alpha(r + x_A)H(\Delta), P)$$

$$= e(\alpha((r + h)(x_A H(ID_A \| P_A) + d_A)$$

$$+ (r + x_A)H(\Delta)), P)$$

$$= e(\alpha\bar{\varsigma}, P) = e(\varsigma, P)$$

B. Security analysis of the Improved Scheme:

For digital signatures, the well-known strong security notion is *existential forgery against adaptive chosen message attack* (EF-CMA) introduce in[9]. Therefore, with respect to the *unforgeability* of improved scheme, we will define it as follows. In the random oracle model, we consider an EF-CMA adversary E .The adversary E is fed with the system parameters params and the signer A 's identity ID_A and public key pk ; also allowed to access to the signing oracle O_S and the random oracle O_H . In the end, the adversary E returns a new valid signature-message pair (σ^*, m^*) .There is a natural restriction that the signature σ^* has not been obtained from the signing oracle O_S before.

In section IV, we see that the public key identity ID is free. In Lin *et.al*'s scheme[1] , when the signer A is signing sends (R^1, S^1) to user B , it contains only the public information. Therefore the Adversary can easily forged to generate forged signature. This can be avoided by using some private key, which is difficult to obtained by the attacker. In the improved scheme in the equation $R^1 = (r + x_A)P$, in the **BSign** phase by using the private key x_A of the signer A , we able to restrict the attacker to forged the signature. Hence , except the signer no one else can sign the message.

C. Performance Comparision of improved scheme with Lin et.al's scheme:

In this section, we compare the computational costs of different phases of our scheme with those for Lin et al.'s scheme [1].

From Table I, we note that our scheme requires same computational costs in different phases as compared to those for Lin et al.'s scheme. Thus, our improved scheme is also efficient as Lin et al.'s scheme. In addition, our scheme provides better security as compared to Lin et al.'s scheme by using signer's private key x_A in **BSign** phase.

Table 1: Performance comparison between our scheme and Lin et al.'s Blind Signature Scheme;T_{pmul}: the time for one point multiplication computation in G_1; T_{padd}: the time for one point addition computation in G_1; T_{pair}:the time for one pairing computation; T_{mhash}: the time for one Map2Point hash function.

Computational cost	Lin et al.'s scheme [1]	Our scheme
KGen	$2T_{pmul} + 2T_{pair} + 2T_{mhash}$	$2T_{pmul} + 2T_{pair} + 2T_{mhash}$
BSign	$11T_{pmul} + 6T_{padd} + 2T_{mhash}$	$11T_{pmul} + 6T_{padd} + 2T_{mhash}$
Verify	$T_{pmul} + 2T_{padd}$ $3T_{pair} + 2T_{mhash}$	$T_{pmul} + 2T_{padd}$ $3T_{pair} + 2T_{mhash}$
Total cost	$14T_{pmul} + 8T_{padd}$ $5T_{pair} + 6T_{mhash}$	$14T_{pmul} + 8T_{padd}$ $5T_{pair} + 6T_{mhash}$

VII. CONCLUSION

We have pointed out the security drawback of Lin et al.'s blind signature scheme and then proposed a modification of their scheme. We have shown that Lin et al.'s is insecure against unforgeability attack. Our improved scheme can remedy the weakness of Lin et al.'s scheme and also meets the security aspects needed by a blind signature scheme. Moreover, our scheme is also efficient in terms of security and its computational costs is also same as et al.'s scheme [1].

REFERENCES

[1] X.Lin, R.Lu H.Zhu, P.Ho and X.Sherman, Provably Secure Self-certified Partially Blind Signature Scheme from Bilinear Pairings,ICC2008,pp. 1530-1535, 2008.

[2] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *in Proc. Advances in Cryptology - Crypto'01*, LNCS 2139, Springer-Verlag, Santa Barbara, California, USA, pp. 213-229, 2001

[3] D. Chaum, "Security without identification: transaction systems to make big brother obsolete," *Communications of the ACM*, Vol. 28, No. 10, pp. 1030-1044, 1985.

[4] D.Chaum, Blind signature for untraceable payment, in Advances in Cryptology-Crypto'82, Santa Barbara, California, USA, pp. 199-203, Aug. 1982.

[5] F. Zhang and K. Kim, "Efficient ID-based blind signature and proxy signature from bilinear pairings," *in Proc. Australasian conference on Information Security and Pricacy - ACISP 2003*, LNCS 2727, Springer-Verlag, Wollongong, Australia, pp. 312-323, 2003.

[6] R. Lu, Z. Cao, and Y. Zhou, "Proxy blind multi-signature schemewithout a secure channel," *Applied Mathematics and Computation,* Vol. 164, No. 1, pp. 179-187, 2005.

[7] F. Zhang and X. Chen, "Cryptanalysis of Huang-Chang partially blind signature scheme," *Journal of Systems and Software*, Vol. 76, No. 3, pp. 323-325, 2005.

[8] Sherman S.M. Chow, Lucas C.K. Hui, S.M. Yiu, and K.P. Chow, "Two improved partially blind signature schemes from bilinear pairings," *in Proc. Australasian conference on Information Security and Pricacy - ACISP 2005*, LNCS 3574, Springer-Verlag, Brisbane, Australia, pp. 316-328, 2005.

[9] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptively chosen message attacks," *SIAM Journal on Computing*, Vol. 17, No. 2, pp. 281-308, 1988.