Forgery Attacks on an ID-Based Partially Blind Signature Scheme

Yuh-Min Tseng, Tsu-Yang Wu and Jui-Di Wu

***Abstract*—A partially blind signature is a variant of the blind signature. The partially blind signature scheme allows a signer to sign a partially blind message that explicitly includes the pre-agreed information. In 2005, Chow et al. first proposed an ID-based partially blind signature scheme with bilinear pairings. ID-based public key systems with bilinear pairings defined on elliptic curves offer a flexible approach to achieve both simplifying the certificate management and reducing the computational cost. However, their scheme is time-consuming for requesters (or clients) with mobile devices. In 2007, Hu and Huang proposed an efficient ID-based partially blind signature scheme based on bilinear pairings. They claimed that the proposed scheme is provably secure under the random oracle model. However, this paper shows that the Hu-Huang scheme suffers from forgery attacks.**

***Index Terms*—Security, Partially blind signature, Bilinear pairings, Identity-based.**

I. Introduction

The concept of the blind signature is introduced by Chaum in [1, 2]. A blind signature scheme is a mechanism, and it allows that a client requests the signer to sign a blinded-message. Then, the requester may obtain a signature on the plain-message from the signed blind message. The signer can neither learn the message he signs nor recognize the signature the requester obtains afterwards. In the past, many improved blind signature schemes have been proposed [3, 4]. By blindness (or un-traceability) property, the blind signature is widely used in many e-commerce applications [5, 6, 7, 8, 9].

However, the blindness property of the blind signature is undesirable in some situations. For example, in an e-cash system, the expiration date and the value of an e-cash should be imposed on the blind signature. Therefore, a partially blind signature scheme was proposed by Abe and Fujisaki [10] in 1996. A partially blind signature scheme allows the signer to embed the non-removable common information into the blind signature. The common information is known and pre-agreed by both the signer and the requester before the signing process. In their scheme, the bank is clearly notified the common information (i.e., the expiration date of an e-cash). With the common information, the bank needs only to keep the still-alive e-cashes in the database to prevent double spending. The partial blindness property preserves the un-traceability of the blind signature, and embeds the pre-agreed common information on the blind signature. In the past, many partially blind signature schemes [11, 12, 13, 14, 15] were also proposed to improve the performance on the requester side or enhance the security. In the following, we briefly present the security requirements and the details refer to [10, 11, 12, 13].

- Unforgeability: Any attackers (or requesters) can not forge a signature that passes the verification in a partially blind signature scheme. Certainly, the requester is also unable to change the pre-agreed common information.
- Partially Blindness: Except for the agreed common information, the signer can neither learn the message he signs nor recognize the signature the requester obtains afterwards.
- Verifiability: If the partially blind signature is generated, any verifiers can check its validity.

An identity (ID)-based public-key system is first introduced by Shamir [16] in 1984. Shamir's cryptosystem may simplify the certificate management as compared with traditional public-key system, but it still suffers from many implementing problems, especially the computational complexity. Recently, Boneh and Franklin [17, 18] proposed a practical ID-based encryption system based on bilinear pairings. Bilinear pairings defined on elliptic curves offer an effective approach to reduce the computational cost of ID-based cryptographic schemes. Afterwards, there are many ID-based signature schemes based on bilinear pairings have been proposed [19, 20, 21, 22].

In 2005, Chow et al. [23] first proposed an ID-based partially blind signature scheme with bilinear pairings. Their scheme possesses the property of simplifying the certificate management as compared with the previously proposed partially blind signature schemes. However, their scheme requires some expensive computations for the requester side.

In 2007, Hu and Huang [24] proposed an efficient ID-based partially blind signature scheme based on bilinear pairings. Their scheme is more efficient and requires less computational cost than Chow et al.'s scheme [23]. They claimed that their scheme is provably secure under the random oracle model. In this paper, we will show that their scheme suffers from forgery attacks. In the forgery attacks, a requester can change the pre-agreed common information.

Manuscript received June 18, 2008. This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC95-2221-E-018-010.

Yuh-Min Tseng is with the Department of Mathematics, National Changhua University of Education, Chang-Hua City 500, Taiwan, R.O.C. (corresponding author to provide e-mail: ymtseng@cc.ncue.edu.tw).

Tsu-Yang Wu is with the the Department of Mathematics, National Changhua University of Education, Chang-Hua City 500, Taiwan, R.O.C..

Jui-Di Wu is with the the Department of Mathematics, National Changhua University of Education, Chang-Hua City 500, Taiwan, R.O.C..

Signer		Requester
$r \in Z_q^*$ $R = rP$		
	===== R ====>	$a,b \in Z_q^*$ $Y' = bQ_{ID} + R + aP$ $h = H_3(m,Y') + bH_1(c)$
$S = hD_{ID} + r H_1(c) P_{pub}$	<==== h =====	
	===== S ====>	$S' = S + a H_1(c) P_{pub}$ Output (m, c, Y', S')
Verification: $e(S',P) =? = e(H_1(c)\, Y' + H_b(m,Y')Q_{ID}, P_{pub})$		

Fig. 1 Hu and Huang's ID-based partially blind signature scheme

II. Review of Hu and Huang's scheme

In this section, we first introduce the concepts of bilinear pairings, as well as the related mathematical assumptions. Then, we briefly review Hu and Huang's ID-based partially blind signature scheme [24]. In this section, we first introduce the concepts of bilinear pairings, as well as the related mathematical assumptions. Then, we briefly review Hu and Huang's ID-based partially blind signature scheme [24].

Let G_1 be an additive cyclic group with a prime order q and G_2 be a multiplicative cyclic group with the same order q. G_1 is a subgroup of the group of points on an elliptic curve over a finite field $E(F_p)$ and G_2 is a subgroup of the multiplicative group over a finite field. Let P be a generator of G_1. We refer to [17, 18] for a fuller description of how these groups, maps and other parameters should be selected in practice for efficiency and security. A bilinear pairing is a map e: $G_1 \times G_1 \rightarrow G_2$ and it satisfies the following properties:

(1) Bilinear: $e(xP,yQ)=e(P,Q)^{xy}$ for all $P, Q \in G_1$ and $x, y \in Z_q^*$.

(2) Non-degenerate: there exists $P, Q \in G_1$ such that $e(P,Q) \neq 1$.

(3) Computability: there is an efficient algorithm to compute $e(P,Q)$ for all $P, Q \in G_1$.

The security of Hu and Huang's ID-based partially blind signature scheme is based on the intractability of the Computational Diffie-Hellman Problem. Here, we present the related mathematical problem and assumption.

For proving the security of the proposed scheme, some important mathematical assumptions for bilinear pairings on elliptic curves are introduced. We refer to [4,5,7,8] for the following assumptions in details.

• *Computational Diffie-Hellman* (*CDH*) *problem*: Given P, xP, $yP \in G_1$, finding xyP.

• *Computational Diffie-Hellman* (*CDH*) *assumption*: No probabilistic algorithm can solve the CDH problem with non-negligible advantage within polynomial time.

In the following, we briefly review Hu and Huang's ID-based partially blind signature scheme [24]. The Hu-Huang scheme consists of four phases: the *Setup* phase, the *Extract* phase, the *Issue* and the *Verify* phases.

A. Setup:

A key generation center (KGC) randomly chooses a system secret key $s \in Z_q^*$, and computes the system public key $P_{pub} = sP$. The KGC selects three cryptographic hash functions $H_1:\{0,1\}^* \rightarrow Z_q^*$, $H_2:\{0,1\}^* \rightarrow G_1$, and $H_3:\{0,1\}^* \times G_1 \rightarrow Z_q^*$. Then, the KGC publishes *Parameters* = $\{G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3\}$.

B. Extract:

The user submits his identity ID to the KGC. After receiving the user's identity, the KGC computes $Q_{ID}=H_2(ID)$ and $D_{ID}= sQ_{ID}$, where D_{ID} is the user's private key. The KGC then sends D_{ID} to the user via a secure channel.

C. Issue:

Suppose that a requester would like to get the signature of a message m. Let c is the pre-agreed common information to be attached with the message m. Note that both the requester and signer have agreed on the common information c. The Issue phase is depicted in Fig.1. The interaction steps between the requester and the signer are presented as follows:

- (Commitment step): The signer with the identity ID chooses a random number $r \in Z_q^*$ and computes $R=rP$. Then, the signer sends R to the requester.
- (Blinding step): The requester randomly selects two numbers $a, b \in Z_q^*$, and computes $Y'=bQ_{ID}+R+aP$ and $h=H_3(m,Y')+bH_1(c)$. The requester sends h to the signer.
- (Signing step): The signer computes $S=hD_{ID}+ rH_1(c)P_{pub}$ and sends S to the requester.
- (Un-blinding step): The requester computes $S'=S +aH_1(c)P_{pub}$.

Finally, (m, c, Y', S') is the partially blind signature of the message m with the pre-agreed common information c.

D. Verify:

Any verifiers can verify the validity of (m, c, Y', S') by checking whether the equation $e(S', P)= e(H_1(c)Y' +H_3(m,Y')Q_{ID}, P_{pub})$ holds or not. If it holds, the verifier accepts the partially blind signature (m, c, Y', S').

III. Our forgery attacks

According to the security requirements of a partially blind signature scheme [10, 11, 12, 13], we know that the

pre-agreed common information c should be involved in the signature verification because both the requester and signer have agreed on the common information c before the signing process. That is, the requester cannot change the pre-agreed common information c to another information c_1 because c_1 is not the pre-agreed common information. In this section, we show that a requester can change the pre-agreed common information in Hu and Huang's ID-based partially blind signature scheme [24]. In the following, we present two forgery attacks on their scheme.

[Forgery attack 1]

Assume that c is the pre-agreed common information to be attached with the message m. The requester wants to obtain another valid signature on a non-pre-agreed common information c_1. Following their proposed scheme, the signer makes the same steps on the pre-agreed common information c. The requester can use another forged common information c_1 to obtain a valid signature as follows:

(1) In the blinding step, the requester computes $Y'=bQ_{ID}+H_1(c)R+aP$ and $h=H_1(c_1)^{-1}H_3(m,Y')+b$.

(2) In the un-blinding step, the requester computes $S'=(S+aP_{pub})H_1(c_1)$ after receiving S. Finally, the requester publishes a partially blind signature (m, c_1, Y', S').

The validation of (m, c_1, Y', S') is presented as follows:

$$
\begin{aligned}
&e(S', P)\\
&= e((S+aP_{pub})H_1(c_1), P)\\
&= e((hD_{ID}+rH_1(c)P_{pub}+aP_{pub})H_1(c_1), P)\\
&= e(H_3(m,Y')D_{ID}+(bD_{ID}+rH_1(c)P_{pub}+aP_{pub})H_1(c_1),P)\\
&= e(H_3(m,Y')sQ_{ID}+(bsQ_{ID}+rH_1(c)sP+asP)H_1(c_1), P)\\
&= e(H_3(m,Y')Q_{ID}+(bQ_{ID}+rH_1(c)P+aP)H_1(c_1), sP)\\
&= e(H_3(m,Y')Q_{ID}+H_1(c_1)Y', P_{pub})
\end{aligned}
$$

In this case, (m, c_1, Y', S') is a valid partially blind signature, even though the signer agrees only the common information c. That is, the requester can forge any c. Since the common information c can be changed and the message m is determined only by the requester, the requester can also obtain a valid signature of another pair (m_1, c_1). Thus, their partially blind signature scheme is not secure against forgery attacks. Their scheme violates the security requirements of a partially blind signature scheme [10, 11, 12, 13].

[Forgery attack 2]

Furthermore, in Hu and Huang's ID-based partially blind signature scheme [24], we know that their verification equation $e(S', P)=e(H_1(c)Y'+H_3(m,Y')Q_{ID}, P_{pub})$, and Y' is computed by the requester. Therefore, we observe another simple forged method. The requester only changes $Y'=H_1(c_1)H_1(c)^{-1}(bQ_{ID}+R+aP)$ in the *Issue* phase and other steps keep unchanged, the verification equation still holds as follows:

$$
\begin{aligned}
&e(S', P)\\
&= e(S+aH_1(c)P_{pub}, P)\\
&= e(hD_{ID}+rH_1(c)P_{pub}+aH_1(c)P_{pub}, P)\\
&= e((H_3(m,Y')+bH_1(c))D_{ID}+rH_1(c)P_{pub}+aH_1(c)P_{pub}, P)\\
&= e(H_3(m,Y')sQ_{ID}+H_1(c)(bsQ_{ID}+rsP+asP), P)\\
&= e(H_3(m,Y')Q_{ID}+H_1(c)(bQ_{ID}+R+aP), sP)\\
&= e(H_3(m,Y')Q_{ID}+H_1(c_1)Y', P_{pub})
\end{aligned}
$$

In this case, (m, c_1, Y', S') is also a valid partially blind signature, even though the signer agrees only the common information c in the *Issue* phase. Thus, our forgery attack is successful.

IV. Conclusions and Future Work

In this paper, we have shown that Hu and Huang's ID-based partially blind signature scheme is vulnerable to forgery attacks. Even though the signer agrees only a common information c, the requester can still forge any common information. Their scheme cannot satisfy the security requirements of a partially blind signature scheme. Due to the rapid growth in popularity of both wireless communications and mobile devices, the security scheme design suited for mobile devices with low-power computing capability is one of many important research issues recently. It is an important future work to propose an efficient ID-based partially blind signature scheme for mobile e-commerce applications.

Acknowledgment

This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no. NSC95-2221-E-018-010.

References

[1] D. Chaum, "Blind signatures for untraceable payments," *Advances in Cryptology - Crypto'82*, Plenum Press, 1983, pp. 199-203.

[2] D. Chaum, "Blind signature systems," *Advances in Cryptology - Crypto'83*, Plenum Press, 1984, pp. 153-156.

[3] J.L. Camenisch, J.M. Piveteau and M.A. Stadler, "Blind signatures based on the discrete logarithm problem," *Advances in Cryptology - Eurocrypto'94*, Springer-Verlag, 1995, LNCS 950, pp. 428-432.

[4] C.I. Fan, W.K. Chen and Y.S. Yeh, "Randomization enhanced Chaum's blind signature scheme," *Computer Communication*, 2000, vol. 23, no. 17, pp. 1677–1680.

[5] D. Chaum, B. Boen, E. Heyst, S. Mjolsnes and A. Steenbeek, "Efficient off-line electronic check," *Advances in Cryptology - Eurocrypt'89*, Springer-Verlag, 1990, LNCS 434, pp. 294-301.

[6] D. Chaum, A. Fiat and M. Naor, "Untraceable electronic cash," *Advances in Cryptology – Crypto'88*, Springer-Verlag, 1990, LNCS 403, pp. 319–327.

[7] W.S. Juang and C.L. Lei, "A secure and practical electrical voting scheme for real world environments," *IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences*, 1997, vol. E80-A, no. 1, pp. 64-71.

[8] W. Ogata and K. Kurosawa, "Oblivious keyword search," *Cryptology ePrint Archive*, 2002, Report 2002/182, 2002. Available at http://eprint.iacr.org.

[9] Y. Wang, S. Lu and Z. Liu, "A simple anonymous fingerprinting scheme based on blind signature," *ICICS'03,* Springer-Verlag, 2003, LNCS 2836, pp. 260–268.

[10] M. Abe and E. Fujisaki, "How to date blind signatures," *Advances in Cryptology - AisaCrypt'96*, Springer-Verlag, 1996, LNCS 1163, pp. 244-251.

[11] C.I. Fan and C.L. Lei, "Low-computation partially blind signatures for electronic cash," *IEICE Transactions on Fundamentals of Electronics Communications and Computer Sciences*, 1998, vol. 81, no. 5, pp. 818-824.

[12] M. Abe and T. Okamoto, "Provably secure partially blind signatures," *Advances in Cryptology - Crypto'00,* Springer-Verlag, 2000, LNCS 1880, pp. 271-286.

[13] H.Y. Chien, J.K. Jan and Y.M. Tseng, "RSA-based partially blind signature with low computation," *IEEE 8th International Conference on Parallel and Distributed Systems*, IEEE press, 2001, pp. 385-389.

[14] Q.H. Wu, W. Susilo and Y.Mu, "Efficient partially blind signature with provable security," *ACIS'06*, Springer-Verlag, 2006, LNCS 3982, pp.345-354.

[15] T.Okamoto, "Efficient blind and partially blind signatures without random oracles," *TCC'06*, Springer-Verlag, 2006, LNCS 3876, pp. 80-99.

[16] A. Shamir, "Identity-based cryptosystems and signature schemes," *Advances in Cryptology - Crypto '84*, Springer-Verlag, 1984, LNCS 196, pp. 47-53.

[17] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," *Advances in Cryptology - Crypto01*, Springer-Verlag, 2001, LNCS 2139, pp. 213- 229.

[18] D. Boneh and M. Franklin, "Identity based encryption from the Weil pairing," *SIAM J. of Computing*, 2003, vol. 32, no. 3, pp. 586-615.

[19] K. Paterson, "ID-based signatures from pairings on elliptic curves," *Electronics Letters*, 2002, vol. 38, no. 18, pp. 1025-1026.

[20] H.J. Yoon, J.H. Cheon and Y. Kim, "Batch verifications with ID-based signatures," *ICISC'04*, Springer-Verlag, 2005, LNCS 3506, pp. 233–248.

[21] J.C. Cha and J.H. Cheon, "An identity-based signature from gap Diffie-Hellman groups," *PKC2003*, Springer-Verlag, 2003, LNCS 2567, pp. 18-30.

[22] Z. Jia and H. Zhen, "Identity-based digital signature algorithm in key exchange on CTP curves," *ICSP'06*, IEEE press, 2006, vol. 4, pp. 16-20.

[23] S.M. Chow, C.K. Hui, S.M.Yiu and K.P. Chow, "Two improved partially blind signature schemes from bilinear pairings," *ACISP'05*, Springer-Verlag, 2005, LNCS 3574, pp. 316-328.

[24] X. Hu and S. Huang, "An efficient ID-based partially blind signature scheme," *SNPD'07*, IEEE press, 2007, pp. 291-296.