On the Forgeability of Wang-Tang-Li's ID-Based Restrictive Partially Blind Signature *

Shengli Liu[1], Xiaofeng Chen[2], Fangguo Zhang[3]
[1]Department of Computer Science and Engineering,
Shanghai Jiao Tong University, Shanghai 200030, P.R.China
email: slliu@sjtu.edu.cn
[2]Department of Computer Science,
Sun Yat-sen University, Guangzhou 510275, P.R.China
email: isschxf@mail.sysu.edu.cn
[3]Department of Electronics and Communication Engineering,
Sun Yat-sen University, Guangzhou 510275, P.R.China
email: isszhfg@mail.sysu.edu.cn

Abstract

Restrictive partially blind signature (RPBS) plays an important role in designing secure electronic cash system. Very recently, Wang, Tang and Li proposed a new ID-based restrictive partially blind signature (ID-RPBS) and gave the security proof. In this paper, we present a cryptanalysis of the scheme and show that the signature scheme does not satisfy the property of **unforgeability** as claimed. More precisely, a user can forge a valid message-signature pair $(ID, msg, \mathbf{info}', \sigma')$ instead of the original one $(ID, msg, \mathbf{info}, \sigma)$, where **info** is the original common agreed information and $\mathbf{info}' \neq \mathbf{info}$. Therefore, it will be much dangerous if Wang-Tang-Li's ID-RPBS scheme is applied to the off-line electronic cash system. For example, a bank is supposed to issue an electronic coin (or bill) of \$100 to a user, while the user can change the denomination of the coin (bill) to any value, say \$100, 000, 000, at his will.

Key words: Unforgeability, restrictive partially blind signature, ID-based cryptography, electronic cash.

1 Introduction

Blind signatures, introduced by Chaum [1], allow a recipient to obtain a signature on message m without revealing anything about the message to the signer. Blind signatures play an important role in plenty of applications such as electronic voting, electronic cash schemes where anonymity is of great concern.

Restrictive blind signatures, firstly introduced by Brands [5], which allow a recipient to receive a blind signature on a message not known to the signer but the choice of the message is restricted and must conform to certain rules. Restrictive blind signature schemes have been important building blocks in designing secure electronic cash systems [4, 7, 8].

*Supported by NSFC under Grants 60303026, 60503006 and 60403007

The concept of partially blind signatures was first introduced by Abe and Fujisaki [2] and allows a signer to produce a blind signature on a message for a recipient and the signature explicitly includes common agreed information which remains clearly visible despite the blinding process. This notion overcomes some disadvantages of fully blind signatures such as the signer has no control over the attributes except for those bound by the public key. There have some constructions of partially blind signature schemes such as Huang-Chang's partially blind signature scheme [13], and Cao-Lin-Xue's partially blind signature scheme [15]. However, both of them are proved not secure [14, 16].

Maitland and Boyd [9] first incorporated these two blind signatures and proposed a provably secure restrictive partially blind signature scheme, which satisfies the partial blindness and restrictive blindness. Their scheme followed the construction proposed by Abe and Okamoto [3] and used Brand's restrictive blind signature scheme. Chen et al. [6] proposed a new provably secure restrictive partially blind signature scheme from pairings. However, these schemes were constructed under the CA-based public key systems.

Identity-based cryptography was first proposed by Shamir in 1985 [10], where the identity information of a user serves as his public key. Identity-based cryptography can simplify certificate management in traditional public key infrastructure. There are many identity-based cryptographic primitives proposed after Shamir's initial work. The first identity-based restrictive partially blind signature (ID-RPBS) scheme was proposed by Chen, Zhang and Liu in [11]. Very recently, Wang, Tang and Li proposed another ID-RPBS scheme in [12], which we call Wang-Tang-Li's ID-RPBS scheme.

In this paper, we give a cryptanalysis of Wang-Tang-Li's ID-RPBS scheme. We show that it does not satisfy the property of unforgeability, $i.e.$, a user can forge a signature with a different common information without being known by the signer. Therefore, the scheme is broken and can not be used in the electronic cash system.

The rest of the paper is organized as follows: The formal definition of the ID-RPBS is given in Section 2. The Wang-Tang-Li's ID-RPBS scheme is introduced in Section 3. In Section 4 we give a cryptanalysis of Wang-Tang-Li's scheme. Finally, conclusions will be made in Section 5.

2 ID-Based Restrictive Partially Blind Signature

The formal definition of ID-based restrictive partially blind signature was proposed by Chen et al. [11] as follows:

Definition 1 *An ID-based Restrictive Partially Blind Signature is a four-tuple* $(\mathcal{PG}, \mathcal{KG}, \mathcal{SG}, \mathcal{SV})$.

- **System Parameters Generation** $\mathcal{PG}$**:** *On input a security parameter* 1^{κ}*, outputs the common system parameters* $Params$ *and a master key* s*.*
- **Key Generation** $\mathcal{KG}$**:** *On input* $Params$ *and an identity information* ID*, outputs the private key* $sk = S_{ID}$*.*
- **Signature Generation** $\mathcal{SG}$**:** *Let* U *and* S *be two probabilistic interactive Turing machines and each of them has a public input tape, a private random tape, a private work tape, a private output tape, a public output tape, and input and output communication tapes. The random tape and the*

input tapes are read-only, and the output tapes are write-only. The private work tape is read-write. Suppose **info** *is agreed common information between U and S. The public input tape of U contains ID and* **info***, where ID is the signer's identity. The public input tape of S contains* **info***. The private input tape of S contains sk, and that for U contains a message m which he knows a representation with respect to some bases in $Params$. The lengths of* **info** *and m are polynomial to κ. U and S engage in the signature issuing protocol and stop in polynomial-time. When they stop, the public output of S contains either completed or not-completed. If it is completed, the private output tape of U contains either $\perp$ or $(ID, \mathbf{info}, m, \sigma)$.*

- **Signature Verification $\mathcal{SV}$:** *On input $(ID, \mathbf{info}, m, \sigma)$ and outputs either accept or reject.*

There are also formal definition for "completeness", "Restrictiveness", " Partial Blindness" and "Unforgeability". Here we only review the definition of "Unforgeability" for an ID-RPBS scheme, referring to [9].

Definition 2 *(Unforgeability) Let $\mathcal{S}$ be an honest signer that follows the signature issuing protocol. Let $\mathcal{A}$ play the following game in the presence of an independent umpire.*

1. $(Params, s) \leftarrow \mathcal{PG}(1^\kappa)$.

2. *$\mathcal{A}$ engages in the signature issuing protocol with $\mathcal{S}$ in a concurrent and interleaving way. Each time, the umpire computes $S_{ID} \leftarrow \mathcal{KG}(Params, s, ID)$ with ID the signer's identity. The umpire places S_{ID} and a common* **info***, agreed between $\mathcal{S}$ and $\mathcal{A}$, on the proper input tapes of $\mathcal{S}$.*

For each **info***, let $l_{\mathbf{info}}$ be the number of executions of the signature issuing protocol where $\mathcal{S}$ outputs completed and* **info** *is on its output tapes. (For* **info** *that has never appeared on the private output tape of $\mathcal{S}$, define $l_{\mathbf{info}} = 0$.)*

$\mathcal{A}$ outputs a single piece of common information, **info***, and $l_{\mathbf{info}} + 1$ signatures $(ID, \mathbf{info}, msg_1; \sigma_1)$, $\cdots$, $(ID, \mathbf{info}, msg_{l_{\mathbf{info}}+1}; \sigma_{l_{\mathbf{info}}+1})$.*

A partially blind signature scheme is unforgeable if, for any probabilistic polynomial-time algorithm $\mathcal{A}$ that plays the above game, the probability that the output of $\mathcal{A}$ satisfies $\mathcal{SV}(ID, \mathbf{info}, msg_j, \sigma_j) =$ accept for $j = 1, 2, \cdots, l_{\mathbf{info}} + 1$ is at most $1/k^c$ where $k > k_0$, for some bound k_0 and some constant $c > 0$. The probability is taken over the coin flips of $\mathcal{PG}$, $\mathcal{A}$ and $\mathcal{S}$.

3 Wang-Tang-Li's ID-RPBS Scheme

Let G_1 and G_2 be two groups with prime order p of size κ and let e be a bilinear map such that $e : G_1 \times G_1 \rightarrow G_2$.

System Parameter Generation $\mathcal{PG}$: PKG chooses $s \in_R \mathbb{Z}_q^*$, $P \in G_1$, and compute $P_{pub} = sP$. Let $H_0 : \{0,1\}^* \rightarrow G_1$, $H_1 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0,1\}^* \times G_1 \times \mathbb{Z}_q^{*3} \rightarrow \mathbb{Z}_q^*$ be cryptographic hash functions. Then the master key is s and the public parameters are $para = \{\kappa, G_1, G_2, e, q, P, P_{pub}, H_0, H_1, H_2\}$.

Key Generation$\mathcal{KG}$: The signer submits his identity information ID to PKG, and PKG computes $Q_{ID} = H_0(ID)$ and return $S_{ID} = sQ_{ID}$ as the signer's private key.

Signature Generation$\mathcal{SG}$: Let $A_1 \in G_1$ be the message to be blindly signed. Let $g = e(P, Q_{ID})$, and $h = e(P_{pub}, Q_{ID})$. Let **info** denote the common agreed information between the signer and the requestor.

(1) The signer chooses $W \in_R G_1$ and computes $a' = e(P, W), b' = e(A_1, W)$ and $z' = e(A_1, S_{ID})$. The signer sends (a', b', z') to the requestor.

(2) The requestor chooses $(u, v, \alpha, \beta) \in_R \mathbb{Z}_q^{*4}$ and computes $A = \alpha A_1 + \beta P$, $A' = e(A, Q_{ID})$, $z = z'^{\alpha} h^{\beta}$, $a = a'^{u} g^{v}$, $b = a'^{u\beta} b'^{u\alpha} A'^{v}$ and $c = H_2(\mathbf{info}, A, z, a, b)$. The requestor sends $c' \equiv c/u \mod q$ to the signer.

(3) The signer responds with $S' = W + c' S_{ID} H_1(\mathbf{info})$.

(4) The requestor checks whether $e(P, S') = a' h^{c' H_1(\mathbf{info})}$ and $e(A_1, S') = b' z'^{c' H_1(\mathbf{info})}$. If yes, he computes $S = uS' + vQ_{ID}$.

The signer with identity ID outputs $\sigma = (z, a, b, S)$ as a signature of $(A, \mathbf{info})$.

Signature Verification$\mathcal{SV}$: Given $(ID, A, \mathbf{info}, \sigma)$ with $\sigma = (z, a, b, S)$, the verifier computes $c = H_2(\mathbf{info}, A, z, a, b)$. If $e(P, S) = a h^{c H_1(\mathbf{info})}$ and $e(A, S) = b z^{c H_1(\mathbf{info})}$, the verifier accepts $\sigma = (A, \mathbf{info}, \sigma)$ as a valid signature from signer ID.

4 Cryptanalysis of Wang-Tang-Li's ID-RPBS Scheme

In this section, we present an attack to show that Wang-Tang-Li's ID-based restrictive partially blind signature scheme does not satisfy the property of "unforeability". In this attack, the adversary will substitute a new $\widetilde{\mathbf{info}}$ for the original common agreed **info**, hence resulting in a valid signature $(ID, msg, \widetilde{\mathbf{info}}, \sigma')$ which is supposed to be $(ID, msg, \mathbf{info}, \sigma)$.

Theorem 1 *Wang-Tang-Li's ID-based restrictive partially blind signature scheme is* **NOT** *secure against the existential adaptive chosen-message-and identity-attacks under the CDHP assumption.*

Proof. To prove that Wang-Tang-Li's ID-RPBS Scheme does not satisfies "unforeability" property, we will show there exists an adversary $\mathcal{A}$ who is able to win the game in Definition 2 with probability 1.

Now let us review the game between $\mathcal{A}$ and the signer $\mathcal{S}$ and an umpire, and see how $\mathcal{A}$ wins the game.

- The umpire setups the system with master key s and public parameters $Params$.
- The adversary $\mathcal{A}$ queries $\mathcal{S}$ for a signature for $(ID, \mathbf{info}, M_1)$, where ID is the identity information of the signer, **info** the common agreed information, and $M_1 \in G_1$ is the message to be blindly signed.

  1. The umpire computes $S_{ID} \leftarrow \mathcal{KG}(Params, s, ID)$. He places S_{ID} and **info** on the proper input tapes of $\mathcal{S}$.

2. $\mathcal{S}$ chooses $W \in_R G_1$ and computes $a' = e(P, W), b' = e(M_1, W)$ and $z' = e(M_1, S_{ID})$. $\mathcal{S}$ sends (a', b', z') to $\mathcal{A}$.
3. $\mathcal{A}$ chooses $(u, v, \alpha, \beta) \in_R \mathbb{Z}_q^{*4}$ and $\widetilde{\mathbf{info}} \in \{0,1\}^*$ with $\widetilde{\mathbf{info}} \neq \mathbf{info}$. $\mathcal{A}$ computes
   - $M = \alpha M_1 + \beta P$,
   - $M' = e(M, Q_{ID})$,
   - $z = z'^{\alpha} h^{\beta}$,
   - $a = a'^{u} g^{v}$,
   - $b = a'^{u\beta} b'^{u\alpha} A'^{v}$,
   - $c = H_2(\widetilde{\mathbf{info}}, M, z, a, b)$ instead of $H_2(\mathbf{info}, M, z, a, b)$.

   $\mathcal{A}$ sends $c' \equiv c \cdot H_1(\widetilde{\mathbf{info}}) \cdot (u \cdot H_1(\mathbf{info}))^{-1} \mod q$ to the signer.
4. $\mathcal{S}$ responds with $S' = W + c' S_{ID} H_1(\mathbf{info})$.
5. $\mathcal{A}$ checks whether $e(P, S') = a' h^{c' H_1(\widetilde{\mathbf{info}})}$ and $e(M_1, S') = b' z'^{c' H_1(\widetilde{\mathbf{info}})}$. If yes, $\mathcal{A}$ computes $S = uS' + vQ_{ID}$.

- $\mathcal{A}$ outputs a tuple $(ID, \widetilde{\mathbf{info}}, M, \sigma)$ with $\sigma = (z, a, b, S)$.

In the following we show that $\sigma = (z, a, b, S)$ is a valid signature for $(\widetilde{\mathbf{info}}, M)$ with $l_{\widetilde{\mathbf{info}}} = 0$. In the game, note that $c' \equiv c \cdot H_1(\widetilde{\mathbf{info}}) \cdot (u \cdot H_1(\mathbf{info}))^{-1} \mod q$, so we have

$$S' = W + c' S_{ID} H_1(\mathbf{info}) = W + c \cdot u^{-1} S_{ID} H_1(\widetilde{\mathbf{info}}).$$

Consequently, $e(P, S) = a h^{c H_1(\widetilde{\mathbf{info}})}$ and $e(A, S) = b z^{c H_1(\widetilde{\mathbf{info}})}$ always hold. On the other hand, since $(ID, m, \widetilde{\mathbf{info}})$ is never queried before, *i.e.*, $l_{\widetilde{\mathbf{info}}} = 0$, the adversary $\mathcal{A}$ wins the game with probability 1.

□

In [12], Wang-Tang-Li's ID-RPBS scheme is applied to an electronic cash system, where banks issue electronic coins (bills) with help of Wang-Tang-Li's ID-RPBS scheme. Now we show how dangerous it is for Wang-Tang-Li's ID-RPBS scheme without unforgeability to be used in an electronic cash system.

Suppose a user and a bank agrees with a common information for an electronic coin (bill), and the common information **info** consists of expiry date and denomination of the coin (bill). More precisely, let $\mathbf{info} = \{\texttt{2008.01.01}, \quad \$100\}$. During the signing process the user can change the common information into a different one, for instance, $\widetilde{\mathbf{info}} = \{\texttt{2010.12.31}, \quad \$100,000,000\}$. The only thing the user needs to do in the signing process is to compute

- $c = H_2(\widetilde{\mathbf{info}}, M, z, a, b)$ instead of $H_2(\mathbf{info}, M, z, a, b)$.
- $c' \equiv c \cdot H_1(\widetilde{\mathbf{info}}) \cdot (u \cdot H_1(\mathbf{info}))^{-1} \mod q$ instead of $c' \equiv c/u \mod q$.

The bank will never realize that the denomination of the coin (bill) has been changed into $ 100,000,000 and the expiry date has been prolonged by the user!

5 Conclusion

In this paper, we give a cryptanalysis of Wang-Tang-Li's ID-based restrictive partially blind signature scheme [12]. We show that the scheme does not satisfy the property of unforgeability. Therefore, it will suffer from the serious problems if the scheme is used in the electronic cash system .

References

[1] Chaum D. Blind signatures for untraceable payments. In *Proc. Crypto'82*, Plenum Press, 1983, pp.199∼203.

[2] Abe M, Fujisaki E. How to date blind signatures. In *Proc. Advances in Cryptology — ASIACRYPT'96*, Kyongju, South Korea, LNCS 1163, 1996, pp.244∼251.

[3] Abe M, Okamoto T. Provably secure partially blind signatures. In *Proc. Advances in Cryptology — Crypto'2000*, Santa Barbara, CA, USA, LNCS 1880, Springer-Verlag, 2000, pp.271∼286.

[4] A. Chan, Y. Frankel, and Y. Tsiounis. Easy come — easy go divisible cash. In Kaisa Nyberg, editor, *Advances in Cryptology—EUROCRYPT 98*, volume 1403 of Lecture Notes in Computer Science, Springer-Verlag, 1998, pp. 561∼576.

[5] Brands, S.: Untraceable Off-line Cash in Wallet with Observers. In: Stinson, D.R. (ed.): *Advances in Cryptology-Crypto93*. Lecture Notes in Computer Science, Vol. 773. Springer-Verlag, Berlin Heidelberg New York, 1993, pp. 302-318.

[6] Chen X, Zhang F, Mu Y , and Susilo W. Efficient Provably Secure Restrictive Partially Blind Signatures from Bilinear Pairings, *Financial Cryptography and Date Security 06*, LNCS 4107, 251-265, Springer-Verlag, 2006.

[7] Boyd C, Foo E, Pavlovski C. Efficient electronic cash using batch signatures. In J. Pieprzyk, R. Safavi-Naini, and J. Seberry, editors, *Australasian Conference on Information Security and Privacy (ACISP'99)*, volume 1587 of Lecture Notes in Computer Science, Springer-Verlag, 1999, pp. 244∼257.

[8] Nyang D, Song J. Preventing double-spent coins from revealing user's whole secret. In J.S. Song, editor, *Second International Conference on In- formation Security and Cryptology (ICISC'99)*, volume 1787 of Lecture Notes in Computer Science, Springer-Verlag, 1999, pp. 13∼20.

[9] Maitland G, Boyd C. A provably secure restrictive partially blind signature. In *Proc. the 5th Int. Workshop on Practice and Theory in Public Key Cryptosystems*, Paris, France, LNCS 2274, Springer-Verlag, 2002, pp.99∼114.

[10] Shamir A. Identity-based cryptosystems and signature schemes. In *Proc. Advances in Cryptology — CRYPTO'84*, Santa Barbara, CA, USA, LNCS 196, Springer-Verlag, 1985, pp.47∼53.

[11] Chen X, Zhang F, Liu S. ID-based restrictive partially blind signatures and applications. *Journal of System and Software*, 2007, 80(2): 164∼171.

[12] Wang C, Tang Y, Li Q, ID-Based Fair Off-Line Electronic Cash System with Multiple Banks. *Journal of Computer Science and Technology*, 2007, 22(3): 487∼493.

[13] Huang H, Chang C. A new design of efficient partially blind signature scheme. *The jounal of Systems and Software*, 2003, 73, pp. 397-403.

[14] Zhang F, and Chen X. Cryptanalysis of Huang-Chang Partially Blind Signature Scheme, *The Journal of Systems & Software*, Vol 76, No.3, 2005, pp 323∼325.

[15] Cao T, Lin D, Xue R. A randomized RSA-based partially blind signature scheme for electronic cash. *Computers and Security*, vol. 24, no.1, 2005, pp.44∼ 49.

[16] Martinet. G, Poupard. G, Sola.P. Cryptanalysis of a Partially Blind Signature Scheme or How to Make $100 Bills with $1 and $2 Ones. *Financial Cryptography 2006*, 2006, pp. 171∼176.