International Journal of Cryptology Research 5(1): 21-27 (2015)

Linkability Attack of an ID-based Blind Signature Scheme

[1]Syh-Yuan Tan, [2]Wun-She Yap and [2]Bok-Min Goi
[1]Faculty of Information Science and Technology, Multimedia University
[2]Lee Kong Chian Faculty of Engineering and Science, Universiti Tunku Abdul Rahman
Email: [1]sytan@mmu.edu.my, [2]{yapws,goibm}@utar.edu.my

ABSTRACT

In 2010, Rao et al. proposed an identity-based blind signature (IBBS) scheme based on Hess IBS scheme. The proposed scheme is claimed to have achieved blindness and also secure against unforgeability in the generic proofs. In this paper, we mount a linkability attack on the blindness property of Rao et al.'s IBBS to show that it is only an IBS scheme. However, we note that the IBBS scheme remains unforgeable and one can view it as an inefficient variant of Hess IBS scheme.

1. INTRODUCTION

Public key cryptography (PKC) was introduced to overcome the key distribution problem of symmetric key cryptography. However, PKC suffers from the man-in-the-middle attack where an adversary C can replace the public key of a user A, to impersonate A in communicating with another user B. As B cannot verify the authenticity of A's public key, B will fall prey to C. In order to solve this problem, public key certification using digital signature scheme is needed where A and B obtain a signature generated by a trusted third party (TTP) on their public keys respectively.

However, when the number of user grows, TTP faces the certificate and public key management issues. In view of this, Shamir (1984) proposed the notion of identity-based cryptography (IBC) which achieves implicit certification through the unique private key generation. The user's identity which is verifiable publicly such as phone number, IC number, email, office room number and so on can be used as the public key. IBC was not realised until the work of Boneh and Franklin (2001). Since then, many identity-based cryptographic primitives were formalised, including identity-based blind signature (IBBS) scheme. Informally, IBBS is an identity-based signature scheme that allows a signer to sign a document sent by a user blindly without knowing any information about the signed document. Thus, IBBS provides anonymity of users.

In 2010, using Hess IBS (Hess, 2002) scheme as building block, Rao et al. proposed an IBBS (Rao et al., 2010) scheme and provided a brief security proof, indicated that their IBBS scheme fulfilled the blindness

property besides being unforgeable. In other words, the IBBS assures that the signer cannot identify which message does a signature belongs to while none can generate a valid signature on the unknown message except the signer himself. We falsify the security claim of Rao et al.'s IBBS scheme by showing that the signer can link a message to the corresponding signature. Anyway, we note that the unforgeability remains valid, as the underlying building block, namely, Hess identity-based signature (IBS) scheme is proven secure.

The rest of the paper is organized as follows. In Section 2, we briefly describe the mathematical notations involved and review the definition of IBBS scheme. In Section 3, we present the cryptanalysis result by mounting a linkability attack on the IBBS scheme. We conclude the paper in Section 4.

2. PRELIMINARIES

In this section, we briefly review the definition for bilinear pairing as well as the scheme model and security notion of IBBS scheme.

2.1 Bilinear Pairing

A bilinear pairing is a pairing function e which pairs two elements $P, Q \in G_1$ to an element $Z \in G_2$ such that $e: P \times Q \rightarrow Z$. To be precise, the pairing function also fulfills the following properties:

1. Bilinearlity: $e(aP, Q) = e(P, aQ) = e(P, Q)^a = e(Q, P)^a$.
2. Non-degeneracy: $e(P, P) \neq 1 \neq e(Q, Q)$.
3. Easily computable.

2.2 Identity-Based Blind Signature Scheme

An IBBS scheme consists of four algorithms: Setup, Extract, Blind Issue and Verification.

Setup (1^k): Take as input a security parameter *k* and return the master public key *mpk* and a master secret key *msk*. *mpk* is published while *msk* is kept securely.

Extract (*mpk*, *msk*, *ID*): Take as inputs *mpk*, *msk* and a public identity *ID*. Return the user private key *upk*.

Issue (*mpk*, *upk*, *ID*): It is an interactive protocol between a signer and a user. The user is given (*m*, *mpk*, *ID*), where *m* is the message he wants to be

signed on the identity *ID*. Except the blind message *V′,* the signer is given *mpk, upk* and its own identity *ID*. The signer and the user run the blind signature issuing protocol. When they stop, the user outputs a blind signature σ on the identity *ID* and message *m*.

Verification (*mpk, ID, m, σ*): It is a deterministic algorithm that takes as input *mpk*, an identity *ID*, a message *m* and a blind signature *σ*. It outputs either accept or reject.

2.2 Security Requirements of IBBS Scheme

A secure IBBS scheme should achieve the property of blindness and unforgeability against adaptive chosen message attacks. We describe the security definition for the former property only (Heng et al., 2007) since we are particularly dealing with this notion in this paper.

Definition 1. Blindness. Let A be the signer and A is involved in the following game with two honest users, namely U_0 and U_1.
1. (*ID, upk*) ← Extract(*mpk, msk, ID*).
2. (m_0, m_1)←A(*mpk, upk, ID*).
3. Select $i \in \{0,1\}$. Put m_i and m_{1-i} to the read-only input tape of U_0 and U_1 respectively.
4. A engages in the signature issuing protocol with U_0 and U_1 in an arbitrary order.
5. If U_0 and U_1 output $\sigma(m_i)$ and $\sigma(m_{1-i})$ respectively using their private tapes, then return those outputs to A. Otherwise, return ⊥ to A.
6. A outputs a bit $i' \in \{0,1\}$.
We say that A wins the game if $i' = i$. An IBBS is blind if there is no PPT algorithm A that wins the game with probability at least $1/2 + 1/k^c$ for any constant $c > 0$. The probability is taken over the coin flips of Extract, U_0, U_1 and A.

3. CRYPTANALYSIS RESULT

In this section, we describe the Rao et al.'s IBBS scheme before mounting the linkability attack on it.

3.1 Rao et al.'sIBBS Scheme

Table 1 reviews Rao et al.'s IBBS scheme.

Setup(1^k)

1. On input1^k, PKG generates groups G_1, G_2 of prime order q and randomly choose a generator $P \in G_1$. The PKG chooses $s \in Z_q^*$ as his master secret key *msk* and compute P_{pub} as sP. The published *mpk* is $\{G_1, G_2, e, P, P_{pub}, H_1, H_2\}$ where $H_1: G_1 \to \{0,1\}^*$ and $H_2: \{0,1\}^* \times G_2 \to \{0,1\}^*$.

Extract($\boldsymbol{mpk}, \boldsymbol{msk}, \boldsymbol{ID}$)

1. Given a singer's public identity$ID \in \{0,1\}^*$, compute the public key $Q_{ID} = H_1(ID)$ and the corresponding user private key $usk = d_{ID} = sQ_{ID}$.

Issue

Signer($\boldsymbol{mpk}, \boldsymbol{upk}$)		**User($\boldsymbol{m}, \boldsymbol{mpk}, \boldsymbol{ID}$)**
1. **Initialisation**: Randomly select $k \in Z_q^*$ and compute$R = e(P,P)^k$. Sends R to user as commitment.	$\xrightarrow{R}$	
	$\xleftarrow{V}$	2. **Blinding**: Randomly select $a, b \in Z_q^*$ as blinding factors, compute $R' = e\big(bQ_{ID} + aP, P_{pub}\big) \cdot R, V = H_2(m, R') + b$ and sends V to signer.
3.**Signing**: Compute $S = Vd_{ID} + kP$ and sends *S* to user.	$\xrightarrow{S}$	4.**Unblinding**: Compute $S' = S + aP_{pub}$, $V' = V - b$ and outputs (m, σ) where $\sigma = (S', V')$ is the blind signature of message *m*.

Verification ($\boldsymbol{mpk}, \boldsymbol{ID}, \boldsymbol{m}, \boldsymbol{S'}, \boldsymbol{V'}$)

Accept the signature $\sigma = (S', V')$ if $V' = H_2\left(m, e(S', P)e\big(Q_{ID}, P_{pub}\big)^{-V'}\right)$, rejects otherwise.

Correctness:

$$
\begin{aligned}
& H_2\left(m, e(S', P)e\big(Q_{ID}, P_{pub}\big)^{-V'}\right) \\
&= H_2\left(m, e\big(S + aP_{pub}, P\big)e\big(Q_{ID}, P_{pub}\big)^{-V'}\right) \\
&= H_2\big(m, e\big((H_2(m, R') + b)d_{ID} + kP + asP, P\big)e(Q_{ID}, sP)^{-H_2(m,R')}\big) \\
&= H_2\big(m, e(Q_{ID}, sP)^{H_2(m,R')+b}e(P,P)^k e(aP, sP)e(Q_{ID}, sP)^{-H_2(m,R')}\big) \\
&= H_2\big(m, e(Q_{ID}, sP)^b e(aP, sP)e(P,P)^k\big) \\
&= H_2\big(m, e\big(bQ_{ID} + aP, P_{pub}\big) \cdot R\big) \\
&= H_2(m, R') \\
&= V - b \\
&= V'
\end{aligned}
$$

Table 1: Rao et al.'s IBBS Scheme

3.2Linkability Attack

We now show how to mount a linkability attack on Rao et al.'s IBBS scheme. Assume the signer is Bob with public identity ID_{Bob} and the user is Alice:

1. From Step 1, 2 and 3 in the **Issue** protocol, Bob has the knowledge of (R_0, V_0, S_0) on an unknown message m_i which belongs to Alice where $i \in \{1,0\}$.
2. Alice performs **Unblinding** and publishes $\sigma_0 = (S'_0, V'_0)$ as the signature for her messagem_0 which is signed by Bob.
3. At this point, Bob will be exposed to the values of both message m_0 and the corresponding signatureσ_0. He can now check whether m_0 is signed by him by performing the following steps:
    a. Extracting the blinding factor b_0:

$$\begin{aligned} V_0 - V'_0 &= V_0 - (V_0 - b_0) \\ &= H_2(m_0, R'_0) + b_0 - (H_2(m_0, R'_0) + b_0 - b_0) \\ &= b_0 \end{aligned}$$

    b. Extracting the value $a_0 P_{pub}$:
    c.

$$\begin{aligned} S'_0 - S_0 &= S_0 + aP_{pub} - S_0 \\ &= V_0 d_{ID_{Bob}} + k_0 P + a_0 P_{pub} - \left(V_0 d_{ID_{Bob}} + k_0 P\right) \\ &= a_0 P_{pub} \end{aligned}$$

    d. Compute $R_0^* = e\left(b_0 d_{ID} + a_0 P_{pub}, P\right) \cdot R_0$.
    e. Check if the condition $H_2(m_0, R_0^*) = V'_0$ holds? If yes, the message m_0 is signed by Bob himself; else, it is signed by other. The correctness is as follows:

$$\begin{aligned} V'_0 &= H_2(m_0, R'_0) \\ &= H_2\left(m_0, e\left(b_0 Q_{ID_{Bob}} + a_0 P, P_{pub}\right) \cdot R_0\right) \\ &= H_2\left(m_0, e\left(b_0 Q_{ID_{Bob}} + a_0 P, sP\right) \cdot R_0\right) \\ &= H_2\left(m_0, e\left(s\left(b_0 Q_{ID_{Bob}} + a_0 P\right), P\right) \cdot R_0\right) \\ &= H_2\left(m_0, e\left(b_0 d_{ID_{Bob}} + a_0 P_{pub}, P\right) \cdot R_0\right) \\ &= H_2(m_0, R_0^*) \end{aligned}$$

4. For other message m_1 which is not signed by Bob, the corresponding signature will be$\sigma_1 = (S'_1, V'_1)$ and the correctness will not hold. When Bob perform the same computations, he will:
    a. Fail in extracting the blinding factor b_1:

$$\begin{aligned} V_0 - V'_1 &= V_0 - (V_1 - b_1) \\ &= H_2(m_0, R'_0) + b_0 - (H_2(m_1, R'_1) + b_1 - b_1) \\ &= b_X \neq b_1 \end{aligned}$$

    Fail in extracting the value$a_1 P_{pub}$:

$$\begin{aligned} S'_1 - S_0 &= S_1 + a_1 P_{pub} - S_0 \\ &= V_1 d_{ID_X} + k_1 P + a_1 P_{pub} - \left(V_0 d_{ID_{Bob}} + k_0 P\right) \\ &= a_X P_{pub} \neq a_1 P_{pub} \end{aligned}$$

    b. Fail in computing$R_1^* \neq R_X^* = e\left(b_X d_{ID_{Bob}} + a_X P_{pub}, P\right) \cdot R_0$.
    c. Obviously the condition $H_2(m_1, R_X^*) \neq V'_1$ does not hold at all now:

$$\begin{aligned} V'_1 &= H_2(m_1, R'_1) \\ &= H_2\left(m_1, e\left(b_1 Q_{ID_{Other}} + a_1 P, P_{pub}\right) \cdot R_1\right) \\ &= H_2\left(m_1, e\left(b_1 Q_{ID_{Other}} + a_1 P, sP\right) \cdot R_1\right) \\ &= H_2\left(m_1, e\left(s\left(b_1 Q_{ID_{Other}} + a_1 P\right), P\right) \cdot R_1\right) \\ &= H_2\left(m_1, e\left(b_1 d_{ID_{Other}} + a_1 P_{pub}, P\right) \cdot R_1\right) \\ &\neq H_2(m_1, R_X^*) \end{aligned}$$

Therefore, it is obvious that Rao et al.'s blindness is broken. The main reason behind the flaw is that Rao et al. did not hide well the blinding factor b. This factor is easily extractable as shown in the attack above.

There are some instances where linkability attacks were falsified (Heng et al., 2007) but the same falsification does not apply here as the blinding factors are extractable and distinguishable from other blinding factors. Furthermore, Rao et al. misinterpreted the non-degeneracy property of bilinear pairing. They showed that $a, b \in Z_q^*$ existed uniquely such that there is always a pair of a, bwhich satisfies the blinding element R' such that:

$$R' = e(bQ_{ID} + aP, P_{pub}) \cdot R \leftrightarrow e(e\left(bQ_{ID} + aP, P_{pub}\right), P_{pub})$$

However, bilinear pairing can only take in elements in G_1 as input, not elements from G_2. Hence, the description on the relation between blinding factors a, b and the blinding element R' is flawed as well.

4. CONCLUSION

We mounted a linkability attack on Rao et al. proposed IBBS scheme and show that their proposed IBBS scheme cannot provide the blindness property. The reason behind the flaw is that the blinding factors b and aP_{pub} are not well hidden within the values (S, S') and (V, V') respectively. To fix this issue, one of the possible ways is to hide the information of b by hashing b. However, a more detailed security analysis and proofs must be performed to the revised IBBS scheme before cryptographically claiming such revised scheme is secure against linkability and forgeability attacks.

REFERENCES

Boneh, D., and Franklin, M. 2001. Identity-based encryption from the Weil pairing. *In Advances in Cryptology—CRYPTO 2001* (pp. 213-229). Springer Berlin Heidelberg.

Heng, S. H., Yap, W. S., and Khoo, K. 2007. Linkability of some blind signature schemes. *In Information Security Theory and Practices. Smart Cards, Mobile and Ubiquitous Computing Systems* (pp. 80-89). Springer Berlin Heidelberg.

Hess, F. 2003. Efficient identity based signature schemes based on pairings. *In Selected Areas in Cryptography* (pp. 310-324). Springer Berlin Heidelberg.

Shamir, A. 1985. Identity-based cryptosystems and signature schemes. *In Advances in Cryptology* (pp. 47-53). Springer Berlin Heidelberg.

Rao, B. U., Ajmath, K. A., Reddy, P. V., and Gowri, T. 2010. An ID-based Blind Signature Scheme from Bilinear Pairings. *International Journal of Computer Science and Security (IJCSS)*, 4(1), 98.