Research Journal of Applied Sciences, Engineering and Technology 5(3): 1054-1058, 2013
DOI:10.19026/rjaset.5.5062
ISSN: 2040-7459; E-ISSN: 2040-7467

Submitted: June 29, 2012 Accepted: July 28, 2012 Published: January 21, 2013

Research Article

"Untraceability" Analysis of Two ID-Based Proxy Blind Signature from Bilinear Pairings

[1]Hua Chen, [2]Jianhua Chen, [1]Guangxing Cai and [3]Aihua Luo
[1]School of Science, Hubei University of Technology, Hubei Wuhan 430068, China
[2]School of Mathematics and Statistics, Wuhan University, Hubei Wuhan 430000, China
[3]School of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430000, China

Abstract: "Untraceability" is an important property of Proxy blind signature. Zhang proposed some new untraceable blind signatures in order to enhance the security of Cai *et al.* (2007) and Hu *et al.* (2007)'s schemes. However, this study shows there are three important conclusions: 1. By reduction, we prove that the cryptanalysis method proposed by Zhang is improper and Cai *et al.* (2007)'s schemes does satisfy the property of untraceability; 2. On that basis, we pinpoints a new analysis method of untraceability which has effectively proved that Hu *et al.* (2007)'s scheme doesn't satisfy the property of untraceability. Furthermore, the method can be used as a standard method which could analyze other schemes related with blind signature; 3. Zhang's scheme is unpractical since the cost of the scheme is higher compared with Cai *et al.* (2007)'s scheme.

Keywords: Cryptanalysis, ID-based cryptograph, proxy blind signature, untraceability

INTRODUCTION

In Chaum (1982) first proposed the concept of blind signature. It is a particular digital signature which needs to satisfy two additional properties:

- **Blindness:** The signer does not see the content of the message.
- **Untraceability:** The signer is unable to link the message-signature pair with the corresponding view after the blind signature has been revealed to the public by the requester.

Proxy signature scheme was first presented by Mambo *et al.* (1996) which enables a proxy signer to sign message on behalf of an original signer. Recently, many proxy blind signatures have been proposed. A proxy blind signature is a digital signature scheme which combines the properties of proxy signature and blind signature schemes. Furthermore, it produces some new properties. So it is very useful in some special applications.

In Cai *et al.* (2007), pointed out Li's *et al.*, proxy blind signature was insecure and proposed an improved scheme which had been proved secure (Cai *et al.*, 2007). Hu *et al.* (2007) presented a new ID-based strong proxy blind signature scheme from bilinear pairings (Hu *et al.*, 2007). However, the author just simply claimed that the scheme met the property of untraceability and didn't give a proof. Recently, Zhang (2009) showed Cai *et al.* (2007)'s scheme and Hu *et al.* (2007)'s scheme couldn't satisfy the property of untraceability and proposed 2 corresponding improved schemes (Zhang, 2009). Chen *et al.* (2010) have a research of the cryptanalysis of a new blind signature based on the DLP. Unfortunately, in this manuscript, we point out that Zhang's analysis method is improper and acquire three important conclusions.

CAI ET AL.'S SCHEME AND SECURITY ANALYSIS

Cai *et al.*'s scheme: Here, we will briefly recall (Cai *et al.*, 2007)'s scheme.

Setup: Let G_1, G_2, be additive cyclic group and multiplicative cyclic group respectively with prime order q. A bilinear pairing $e: G_1 \times G_1 \to G_{2.}$ Pick $s \in_R Z_q^*$ as system master key, Set $Q_p = sp$ as system public key, where, P is the generator of G_1. Let, H_1, H_2, be two hash functions, where, H_1: $\{0, 1\} \times G_2 \to Z^*_q$, H_2: $\{0, 1\} \to G_1$. $S_{ID_A} = sQ_{ID_A}$ is the private key of original signer A, where, $Q_{IDA} = H_2(ID_A)$ is the corresponding public key. $S_{ID_B} = sQ_{ID_B}$ is the private key of proxy signer B, where, $Q_{ID_B} = H_2(ID_B)$ is the corresponding public key. Publish the system parameter:

Corresponding Author: Aihua Luo, School of Mathematics and Statistics, South-Central University for Nationalities, Wuhan 430000, China

$$\{G_1, G_2, e, q, P, Q_P, H_1, H_2\}$$

Proxy delegation phase:

- The original signer A picks $P_1 \in_R G_1$, computes:

  $r_A = e(P_1, P)$,

  $V_A = H_1(m_w, r_A)$, $U_A = V_A S_{ID_A} + P_1$

  where, m_w is proxy delegation certification and then sends (U_A, V_A, r_A, m_w) to proxy signer B.
- B checks whether the equation:

  $$e(U_A, P) = e(Q_{ID_A}, Q_P)^{V_A} \cdot r_A$$

  holds. If it holds, B computes $S_P = U_A + S_{ID_B}$ as the private key of proxy signer B.

Signing phase:

- B picks $P_2 \in_R G_1$, computes $r_B = e(P_2, P)$ and then sends (r_B, r_A) to the receiver C
- C picks $P_3 \in R\ G_{1,}$, $k \in_R Z_q^*$, computes:

  $$r = {r_B}^k e(P_3, P)$$

  $$V = H_1(m, r), V' = Vk^{-1}$$

  and then sends V' to B
- B computes $U_B = V'S_P + P_2$ and then sends U_B to C
- C computes $U = kU_B + P_3$

  The blind signature of the message m is (U, r, V)

Verification phase: Anyone can verify the validness of the proxy blind signature (U, r, V) by checking whether:

$$e(U, P) = e(Q_{ID_A}, Q_P)^{VV_A} {r_A}^V e(Q_{ID_B}, Q_P)^V r$$

holds.

Zhang's cryptanalysis: In Zhang's cryptanalysis (Zhang, 2009), he claimed that Cai *et al.* (2007)'s blind signature could be traced by the proxy signer. The proxy signer will keep a set of record (U_B, r_B, V') as a view for all blinding signed messages. After revealing the message-signature pair (U, r, V) to the public by the requester, the proxy signer can compute factors $\{k, P_3\}$, where, $k = VV'^{-1}$, $P_3 = U - kU_B$

Then the proxy signer can trace the blind signature by checking $r = {r_B}^k e(P_3, P)$. If the checking equation holds, the scheme will satisfy the property of untraceability. Otherwise, it will not meet the property.

DISCUSSION

In this section, we will prove Zhang's cryptanalysis is unfortunately incorrect. Let:

$$(U_i, r_i, V_i),\quad (U_j, r_j, V_j)$$

be the two arbitrary message-signatures of the scheme and their corresponding views are (U_{Bi}, r_{Bi}, V_i'), (U_{Bj}, r_{Bj}, V_j') respectively, so the following equations hold:

$$\begin{cases} r_{Bi} = e(P_{2i}, P), r_i = {r_{Bi}}^{k_i} e(P_{3i}, P) \\ V_i' = V_i {k_i}^{-1}, U_{Bi} = V_i' S_P + P_{2i} \\ U_i = k_i U_{Bi} + P_{3i} \end{cases} \tag{1}$$

$$\begin{cases} r_{Bj} = e(P_{2j}, P), r_j = {r_{Bj}}^{k_j} e(P_{3j}, P) \\ V_j' = V_j {k_j}^{-1}, U_{Bj} = V_j' S_P + P_{2j} \\ U_j = k_j U_{Bj} + P_{3j} \end{cases} \tag{2}$$

when the message-signature pair (U_j, r_j, V_j) is revealed to the public, the proxy signer searches all the views stored. Obviously, from its corresponding view stored, (U_{Bj}, r_{Bj}, V_j'), there exist one pair factors $\{k_j, P_{3j}\}$ which make the Zhang's checking equation hold. However, from any other view (U_{Bi}, r_{Bi}, V_i') we can prove that there still exists one pair factors $\{k, P_3\}$ which make the Zhang's checking equation always hold. The proof is listed as follows:

For the revealed message-signature pair (U_j, r_j, v_j) and any view (U_{Bi}, r_{Bi}, V_i') stored, let their corresponding "blindness" equations as follows:

$$r_j = {r_{B_i}}^k e(P_3, P) \tag{3}$$

$$V_i' = V_j k^{-1} \tag{4}$$

$$U_j = kU_{Bi} + P_3 \qquad (5)$$

The proxy signer computes factors {k, p$_3$} from Eq. (4) and (5):

where,

$$k = V_j V_i'^{-1}, \quad P_3 = U_j - kU_{Bi}$$

Then, by use of Eq. (1) and （2), we can see that the Eq. (3) always holds:

$$r_{Bi}{}^{k} e(P_3, P)$$

$$= r_{Bi}{}^{k} e(U_j - kU_{Bi}, P)$$

$$= r_{Bi}{}^{k} e(U_j, P) e(U_{Bi}, P)^{-k}$$

$$= r_{Bi}{}^{k} e(k_j U_{Bj} + P_{3j}, P) e(V_i' S_P + P_{2i}, P)^{-k}$$

$$= r_{Bi}{}^{k} e(k_j U_{Bj} + P_{3j}, P) e(V_i' S_P, P)^{-k} \, e(P_{2i}, P)^{-k}$$

$$= r_{Bi}{}^{k} e(k_j U_{Bj} + P_{3j}, P) e(V_i' S_P, P)^{-V_j V_i'^{-1}} \, r_{Bi}{}^{-k}$$

$$= e(k_j U_{Bj} - V_j S_P, P) e(P_{3j}, P)$$

$$= e(k_j U_{Bj} - k_j V_j' S_P, P) e(P_{3j}, P)$$

$$= e(U_{Bj} - V_j' S_P, P)^{k_j} e(P_{3j}, P)$$

$$= e(P_{2j}, P)^{k_j} e(P_{3j}, P) = r_{Bj}{}^{k_j} e(P_{3j}, P) = r_j$$

In other words, whenever the view（U_{Bi}, r_{Bi}, V_i') and the message-signature pair (U_j, r_j, V_j) are corresponding or not, the checking equation $r_j = r_{B_i}{}^{k} e(P_3, P)$ always holds. Therefore, the signer is still unable to link the message-signature pair with the corresponding view by using Zhang's method.

IMPORTANT RESULTS

Result I: The cryptanalysis method proposed by Zhang is improper and Cai *et al.* (2007)'s scheme does meet the property of untraceablity which has been proved in Cai *et al.* (2007).

Result II: The analysis and proof process in above can be used as a new method which can analyze the property of "untraceability" of other schemes related with blind signature.

Result III: The equations:

$$r = r_B{}^{k} e(P_3, P), V' = Vk^{-1}$$

in Cai *et al.* (2007)'s scheme are replaced respectively by the equations:

$$r = r_B{}^{k} e(P_3, P)(e(Q_{ID_A}, Q_P)^{V_A} r_A e(Q_{ID_B}, Q_P))^{kt}$$

$$V' = Vk^{-1} + t$$

in Zhang's scheme. Obviously, Zhang's scheme is unpractical since the cost of the scheme is higher compared with Cai *et al.* (2007)'s scheme.

Our new proof method of "untraceability" analysis: From the discussion in above section, we propose a new method of "untraceability" analysis of blind signature. The new method can be described briefly as follows:

Theorem: During the execution of the blind signature issuing protocol ∑, for the revealed message-signature pair S and any view V stored by signature (whenever they are corresponding or not), Suppose they have n corresponding "blindness" equations, the signer can compute n-1 factors from the n-1 "blindness" equations of all and then check the nth "blindness" equation by use of the given equations in the blind signature issuing protocol ∑. If the nth "blindness" equation holds, the protocol ∑ satisfies the property of "untraceability". Otherwise, it doesn't meet the property.

HU ET AL.'S SCHEME AND SECURITY ANALYSIS

Hu *et al.*'s scheme: Here, we will briefly recall Hu *et al.* (2007)'s scheme (Zhang, 2009).

Setup: Let G$_1$, G$_2$ be additive cyclic group and multiplicative cyclic group respectively with prime order q. A bilinear pairing $e: G_1 \times G_1 \rightarrow G_2$. Pick $k \in_R Z_q^*$, as system master key, Set pk = xP, as system public key, where, P is the generator of G_1.

Let h, H be two hash functions where,

$$H: \{0,1\}^* \rightarrow G_1, h: \{0,1\}^* \rightarrow Z_q^*$$

S$_{\text{IDO}}$ = xH(ID$_\text{O}$) is the private key of original signer O, where $H(ID_O)$ is the corresponding public key.

$S_{IDP} = xH(ID_P)$ is the private key of proxy signer P, where $H(ID_p)$ is the corresponding public key.

Proxy delegation phase:

- The original signer O picks $t \in_R Z_q^*$, computes $S = tH(m_w) + S_{ID_O}$ sends S to proxy signer P and then publishes the parameters tP, m_w to the public.
- P checks whether the equation:

  $e(S,P) = e(H(m_w), tP)\, e(H(ID_O),xP)$

  holds. If it holds, P computes $S' = S + S_{ID_P}$ as the private key of proxy signer and the corresponding public key is $Q' = H(ID_O) + H(ID_P)$.

Signing phase:

- P picks $\alpha \in_R Z_q^*$, computes $r' = e(P,tP)^{\alpha}$ and then sends r' to the receiver C.
- C picks $\beta \in_R Z_q^*$, computes $r = r'e(P,tP)^{\beta}$, $V = h(M \,||\, r)$ and then sends V to P
- P computes $U' = VS' + \alpha tP$ and then sends U' to C
- C computes $U = U' + \beta tP$

Then, the blind signature of the message m is (*U*, *r*).

Verification phase: Anyone can verify the validness of the proxy blind signature (*U*, *r*) by checking whether:

$$r = e(P,U)\, e(H(m_w), tP)^{-V}\, e(Q`, xP)^{-V}$$

holds.

Untraceability analysis of Hu *et al.*'s scheme: Zhang (2009) pointed out Hu *et al.* (2007)'s scheme didn't satisfy the property of untraceability in the same way as analyzing Cai *et al.* (2007)'s scheme. However, we have proved Zhang's analysis method is inaccurate. Therefore, in this section, we will give a proper analysis about Hu *et al.* (2007)'s scheme making use of our proposed new method in theorem. The proof is listed as follows:

Proof: During the execution of Hu *et al.* (2007)'s blind signature issuing protocol, let (U_i, r_i), (U_j, r_j) be the two arbitrary message-signatures of the scheme and their corresponding view are (U_i', r_i', V_i), (U_j', r_j', V_j), respectively. From Hu *et al.* (2007)'s scheme, the following equations hold:

$$\begin{cases} r_i' = e(P,tP)^{\alpha_i}, r_i = r_i' e(P,tP)^{\beta_i} \\ V_i = h(M_i \,\|\, r_i), U_i' = V_i S' + \alpha_i tP \\ U_i = U_i' + \beta_i tP \end{cases} \quad (6)$$

$$\begin{cases} r_j' = e(P,tP)^{\alpha_j}, r_j = r_j' e(P,tP)^{\beta_j} \\ V_j = h(M_j \,\|\, r_j), U_j' = V_j S' + \alpha_j tP \\ U_j = U_j' + \beta_j tP \end{cases} \quad (7)$$

when the message-signature pair (U_j, r_j) is revealed to the public, the proxy signer searches all the views stored. For the revealed message-signature pair (U_j, r_j) and any view (U_i', r_i', V_i) stored (whenever they are corresponding or not), obviously, they have two corresponding "blindness" equations as follows:

$$r_j = r_i' e(P,tP)^{\beta} \quad (8)$$

$$U_j = U_i' + \beta tP \quad (9)$$

The proxy signer computes factor β from Eq. (9), where:

$$\beta = (U_j - U_i')(tP)^{-1}$$

and then checks the second equation $r_j = r_i' e(P,tP)^{\beta}$ by use of the Eq. (6) and (7). Unfortunately, we find that the Eq. (8) holds if and only if $i = j$. In other words, the Eq. (8) holds if and only if the view and the revealed message-signature are corresponding. From theorem, Hu *et al.* (2007)'s scheme doesn't satisfy the property of untraceability.

CONCLUSION

In this manuscript, we point out that Zhang's cryptanalysis method of untraceability is improper. Furthermore, we present a new analysis method of untraceability which can be used to analyze other schemes related with blind signature.

ACKNOWLEDGMENT

This study is supported by a grant from Science Technology Commission of Hubei Province of China (No. 2011CDB081) and the Special Fund for Basic Scientific Research of Central Colleges, South-Central University for Nationalities (No. CZQ12016).

REFERENCES

Cai, G. and H. Chen, 2007. New ID-based proxy blind signature scheme from bilinear pairings (J). Comp. En., 33(9): 145-147.

Chaum, D., 1982. Blind signatures for untraceable payments. Advances in Cryptology: Proceeding of CRYPTO' 82, pp: 199-203.

Chen, H., J. Chen and G. Cai, 2010. Cryptanalysis of a new blind signature based on the DLP. Proceeding of IEEE International Conference on Information Theory and Information Security, ICITIS, pp: 415-418.

Hu, J. and J. Zhang, 2007. New multi-level strong proxy blind signature scheme based on bilinear pairing (J). Com. Eng., 43(18): 123-125.

Mambo, M., K. Usuda and E. Okamoto, 1996. Proxy signatures for delegating signing operation (C). Proceeding of 3rd ACM Conference on Computer and Communication Security, pp: 48-57.

Zhang, X., 2009. Two improved ID-based proxy blind signatures (J). Comp. En., 35(3): 15-17.