Linkability of Several Blind Signature Schemes

Xuesheng Zhong

Institute of System Sciences, AMSS, CAS, Beijing, China. zhongxsh@163.com

Abstract The unlinkability is an important security property that blind signature schemes should satisfy. But we find that the several blind signature schemes [1,2,3] are linkable. The Signer can derive a link between a protocol view and a valid blind signature. They are not secure.

Keywords blind signature, anonymity, protocol view, linkability.

1 Introduction

The blind signature was introduced by D.Chaum [4], which can provide anonymity of users in applications such as electronic voting and electronic payment systems. In contrast to general signature schemes, a blind signature scheme allows the user to obtain a signature of a message in a way that the signer learns neither the message nor the resulting signature.

We know that every digital signature scheme should satisfy the unforgeability property. The unforgeability property means that only the signer should be able to generate the valid signatures. The unlinkability is the additional security property that the blind signature scheme should satisfy. A protocol view for a signature scheme is defined to be the set of all messages that the signer has received and generated in issuing the signature. Then, the unlinkability property means that no one can derive a link between a protocol view and a valid blind signature except the signature requester.

In this paper, we show that the several blind signature schemes are linkable. The Signer can link a protocol view to a valid blind signature. Therefore, those schemes are not secure.

2 Zhang-Kim ID-based blind signature scheme

In 2002, Zhang and Kim[1] proposed an ID-based blind signature scheme. It can be described as follows.

Let G be a cyclic group generated by P, whose order is a prime q, and V be a cyclic multiplicative group of the same order q. The discrete logarithm problems in both G and V are hard. Let $e : G \times G \longrightarrow V$ be a pairing which satisfies the following conditions:

(1) Bilinear: $e(P_1+P_2, Q) = e(P_1, Q)e(P_2, Q)$ and $e(P, Q_1+Q_2) = e(P, Q)e(P, Q_2)$, or $e(aP, bQ) = e(P, Q)^{ab}$;

(2) Non-degenerate: There exists $P \in G$ and $Q \in G$ such that $e(P, Q) \neq 1$;

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

An ID-based blind signature scheme is considered be the combination of a general blind signature scheme and an Id-based one, i.e., it is a blind signature, but its public key for verification is just the signer's identity.

2.1 Review

Setup Let P be a generator of G. Choose a random number $s \in Z_q^*$ and set $P_{pub} = sP$. Define two cryptographic hash functions $H : \{0,1\}^* \longrightarrow Z/q$ and $H_1 : \{0,1\}^* \longrightarrow G$. The system parameters are $PARAMS = \{G, q, P, P_{pub}, H, H_1\}$, and s be the MASTER-KEY of TA.

Extract Given an identity ID, which implies the public key $Q_{ID} = H_1(ID)$, the algorithm returns the private key $S_{ID} = sQ_{ID}$.

The above two operations are carried out by TA. Note that TA can access to the sensitive private key S_{ID}. To avoid power abuse by TA, n trust authorities with $(n, n)-$threshold secret sharing scheme can be used to escrow the MASTER-KEY.

Blind signature issuing protocol

User	$\overset{request}{-- \longrightarrow}$	Signer
		choose $r \in_R Z_q^*$, compute $R = rP$
choose $a, b \in_R Z_q^*$, compute	$\overset{R}{\longleftarrow --}$	
$t = e(bQ_{ID} + R + aP, P_{pub})$,		
$c = H(m, t) + b(mod\ q)$	$\overset{c}{-- \longrightarrow}$	compute $S = cS_{ID} + rP_{pub}$
compute $S' = S + aP_{pub}$,	$\overset{S}{\longleftarrow --}$	
$c' = c - b$		
(S', c') is the blind signature of the message m.		

Verification Accept the signature if and only if

$$c' = H(m, e(S', P) \cdot e(Q_{ID}, P_{pub})^{-c'})$$

2.2 Linkability

After receiving a user's request, say Alice, the signer can record the protocol view as (R, c, S) and link it to Alice. Given a valid blind signature (m, S', c'), the signer can determine whether it does correspond to (R, c, S) by checking the following equation:

$$H(m, e((c - c')Q_{ID} + R, P_{pub}) \cdot e(P, S' - S)) \overset{?}{=} c' \tag{1}$$

If it holds, the signer can claim that the blind signature (m, S', c') is sent to Alice.

Correctness:

$$\begin{aligned} & H(m, e((c - c')Q_{ID} + R, P_{pub}) \cdot e(P, S' - S)) \\ = \; & H(m, e(bQ_{ID} + R, P_{pub}) \cdot e(P, aP_{pub})) \\ = \; & H(m, e(bQ_{ID} + R, P_{pub}) \cdot e(aP, P_{pub})) \\ = \; & H(m, e(bQ_{ID} + R + aP, P_{pub})) \\ = \; & H(m, t) = c' \end{aligned}$$

Clearly, if a view $(\bar{R}, \bar{c}, \bar{S})$ does not match the blind signature (m, S', c'), the above equation (1) cannot hold. Otherwise, set $\bar{b} = \bar{c} - c', \bar{a}P_{pub} = S' - \bar{S}$, we have

$$H(m, e(bQ_{ID} + R + aP, P_{pub})) = H(m, e(\bar{b}Q_{ID} + R + \bar{a}P, P_{pub}))$$

But the probability of the event is negligible.

3 Maitland-Boyd blind signature scheme

To seek a blind variant of the Schnorr [5] protocol which uses nultiplicative (rather than the standard additive operation) to blind the challenge, Maitland and Boyd proposed the following blind signature scheme [2].

3.1 Review

Let two primes p and q be given such that q divides $p - 1$ and let $g \in Z_p^*$ be an element of order q, $H(\cdot)$ be a cryptographic hash function. Let $y = g^x (mod\ p)$ be the public key of the signer, x be the corresponding secret key, and m be a message from the receiver.

–The signer generates a random number $r \in_R Z_q$, and sends $a = g^r\ mod\ p$ to the receiver.

–The receiver chooses blinding factors $u, v \in_R Z_q$ and computes $a' = a^u g^v\ mod\ p$. The receiver then computes $c' = H(m||a')$ and sends $c = c'/u\ mod\ q$ to the signer.

–The signer responds with $s = r + cx \ mod \ q$.

–The receiver accepts if and only if $a = g^s y^{-c} \ mod \ p$.

–If the receiver accepts, computes $s' = us + v \ mod \ q$.

(c', s') is a valid signature on m satisfying

$$c' = H(m||g^{s'} y^{-c'})$$

3.2 Linkability

After receiving a user's request, say Alice, the signer can record the protocol view as (r, a, c, s) and link it to Alice. Given a valid blind signature (m, c', s'), the signer can determine whether it does correspond to (r, a, c, s) by checking the following equation:

$$c' \overset{?}{=} H(m\|a^{c'c^{-1}} g^{s'-c'c^{-1}s}) \tag{2}$$

where c^{-1} is the reverse of c in group Z_q^*. If it holds, the signer can claim that the blind signature (m, c', s') is sent to Alice.

Correctness

$$a^{c'c^{-1}} g^{s'-c'c^{-1}s} = a^u g^{s'-us} = a^u g^v = a'$$

Clearly, if a protocol view $(\bar{r}, \bar{a}, \bar{c}, \bar{s})$ does not match the blind signature (m, c', s'), the above equation (2) cannot hold. Otherwise, set

$$\bar{u} = c'(\bar{c})^{-1} \ (mod \ q), \quad \bar{v} = s' - c'(\bar{c})^{-1}(\bar{s}) \ (mod \ q),$$

we have

$$\bar{a}^{c'(\bar{c})^{-1}} g^{s'-c'(\bar{c})^{-1}(\bar{s})} = \bar{a}^{\bar{u}} g^{\bar{v}} = a' = a^u g^v \quad (mod \ p)$$

Combining the generation of the protocol view, we know there exists a number $\bar{r} \in Z_q^*$ such that $\bar{a} = g^{\bar{r}} \ (mod \ p)$. Hence,

$$\bar{r}\bar{u} + \bar{v} = ru + v \quad (mod \ q)$$

But the probability of the event is negligible because $\bar{r}, r, u, v$ are randomly picked in signing.

4 Maitland-Boyd restrictive partially blind signature scheme

In the same paper [2], Maitland and Boyd proposed a restrictive partially blind signature scheme. We now review it as follows:

4.1 Review

Let two primes p and q be given such that q divides $p-1$ and let $g \in Z_p^*$ be an element of order q, $H(\cdot)$ be a cryptographic hash function. Let $y_1 = g^{x_1}(mod\ p)$ be the public key of the signer, x_1 be the corresponding secret key, and m be a message from the receiver. The common information, $info$, is placed in the Schnorr public key y_2 by setting $y_2 = F(info)$, where $F : \{0,1\}^* \rightarrow G_q$ is a public hash function which maps arbitrary strings into elements in G_q.

–The signer generates a random number $r \in_R Z_q$, computes

$$z_1 = m^{x_1}, \quad a_1 = g^{r_1}, \quad b_1 = m^{r_1}$$

simulates Schnorr transcript

$$c_2, s_2 \in_r Z_q^*, \quad a_2 = g^{s_2} y_2^{-c_2}$$

where $y_2 = F(info)$. Then he sends

$$z_1, a_1, b_1, a_2$$

to the receiver.

– The receiver chooses $\alpha_1, \beta_1, u_1, v_1, u_2, v_2 \in_R Z_q$, computes

$$m_1' = m^{\alpha_1} g^{\beta_1}, \ \ z_1' = z_1^{\alpha_1} y_1^{\beta_1}, \ \ a_1' = a_1^{u_1} g^{v_1},$$

$$b_1' = a_1^{u_1 \beta_1} b_1^{u_1 \alpha_1} (m_1')^{v_1}, a_2' = a_2^{u_2} g^{v_2}$$

generates the challenge

$$c' = H(g||y_1||y_2||m_1'||z_1'||a_1'||b_1'||a_2')$$

and blinds the challenge as $c = c'/(u_1 u_2)\ mod\ q$.

–The signer computes $c_1 = c/c_2$ and responds with $s_1 = r_1 + c_1 x_1\ mod\ q$.

–The receiver checks

$$c \overset{?}{=} c_1 c_2, \ \ a_1 \overset{?}{=} g^{s_1} y_1^{-c_1}, \ \ b_1 \overset{?}{=} m^{s_1} z_1^{-c_1}, \ \ a_2 \overset{?}{=} g^{s_2} y^{-c_2}$$

then computes

$$c_1' = c_1 u_1, \ \ s_1' = u_1 s_1 + v_1\ mod\ q, \ \ c_2' = c_2 u_2, \ \ s_2' = u_2 s_2 + v_2\ mod\ q$$

The resulting signature on a message m_1' derived from the base message m and with common information $info$ is a tuple

$$z_1', c_1', s_1', c_2', s_2')$$

The signature is valid if it satisfies

$$c_1'c_2' = H(g||y_1||y_2||m_1'||z_1'||g^{s_1'}y^{-c_1'}||(m_1')^{s_1'}(z_1')^{-c_1'}||g^{s_2'}y_2^{-c_2'}) \mod q$$

4.2 Linkability

After receiving a user's request, say Alice, the signer can record the protocol view as

$$(m, r, z_1, a_1, b_1, c_2, s_2, a_2, c, c_1, s_1, c_2, s_2)$$

and link it to Alice. Given a valid blind signature $(m_1', z_1', c_1', s_1', c_2', s_2')$, the signer can determine whether it does correspond to $(m, r, z_1, a_1, b_1, c_2, s_2, a_2, c, c_1, s_1, c_2, s_2)$ by checking the following equation:

$$c_1'c_2' = H(g||y_1||y_2||m_1'||z_1'||a_1^{c_1'c_1^{-1}} g^{s_1'-c_1'c_1^{-1}s_1}||(m_1')^{s_1'}(z_1')^{-c_1'}||g^{s_2'}y_2^{-c_2'}) \mod q \qquad (3)$$

where c_1^{-1} is the reverse of c_1 in group Z_q^*. If it holds, the signer can claim that the blind signature $(m_1', z_1', c_1', s_1', c_2', s_2')$ is sent to Alice.

Correctness

$$a_1^{c_1'c_1^{-1}} g^{s_1'-c_1'c_1^{-1}s} = a_1^{u_1} g^{s_1'-u_1s_1} = a^{u_1}g^{v_1} = a_1'$$

Clearly, if a protocol view $(m, r, z_1, a_1, b_1, c_2, s_2, a_2, c, c_1, s_1, c_2, s_2)$ does not match the blind signature $(m_1', z_1', c_1', s_1', c_2', s_2')$, the above equation (3) cannot hold. Otherwise, set

$$\bar{u_1} = c_1'(\bar{c_1})^{-1} \ (mod\ q), \quad \bar{v_1} = s_1' - c_1'(\bar{c_1})^{-1}(\bar{s_1}) \ (mod\ q),$$

we have

$$\bar{a_1}^{c_1'(\bar{c_1})^{-1}} g^{s_1'-c_1'(\bar{c_1})^{-1}(\bar{s_1})} = \bar{a_1}^{\bar{u_1}} g^{\bar{v_1}} = a_1' = a_1^{u_1}g^{v_1} \quad (mod\ p)$$

Combining the generation of the protocol view, we know there exists a number $\bar{r_1} \in Z_q^*$ such that $\bar{a_1} = g^{\bar{r_1}}$ $(mod\ p)$. Hence,

$$\bar{r_1}\bar{u_1} + \bar{v_1} = r_1u_1 + v_1 \quad (mod\ q)$$

But the probability of the event is negligible because $\bar{r_1}, r_1, u_1, v_1$ are randomly picked in signing.

5 Brands' restrictive blind signature scheme

The blind signature scheme can be described as follows [3].

5.1 Review

Let two primes p and q be given such that q divides $p-1$ and let $g \in Z_p^*$ be an element of order q, $H(\cdot)$ be a cryptographic hash function. Let $y = g^x (mod\ p)$ be the public key of the signer, x be the corresponding secret key, and m be a message from the receiver. The signer is supposed to sign m by forming $z = m^x$ and providing a signed proof that $log_g\ y = log_m\ z$.

- The signer generates a random number $r \in Z_q^*$, and sends $z = m^x, a = g^r$ and $b = m^r$ to the receiver.
- The receiver generates at random numbers $\alpha, \beta \in Z_q^*$ and computes
$$m' = m^\alpha g^\beta, \qquad z' = z^\alpha y^\beta$$
The receiver also chooses $u, v \in Z_q^*$ and computes a' and b' as follows:
$$a' = a^u g^v, \qquad b' = a^{u\beta} b^{u\alpha} (m')^v$$
The receiver then computes $c' = H(m' \| z' \| a' \| b')$ and sends $c = c'/u\ (mod\ q)$ to the signer.
- The signer responds with $s = r + cx\ (mod\ q)$.
- The receiver accepts if and only if $a = g^s y^{-c}$ and $b = m^s z^{-c}$.
- If the receiver accepts, compute $s' = us + v\ (mod\ q)$.

(z', c', s') is a valid signature on m' satisfying

$$c' = H(m' \| z' \| g^{s'} y^{-c'} \| (m')^{s'} (z')^{-c'})$$

Thus, the receiver has a signature on a message m' where $m' = m^\alpha g^\beta$ and (α, β) are values chosen by the receiver.

5.2 Linkability

After receiving a user's request, say Alice, the signer can record the protocol view as (m, r, z, a, b, c, s) and link it to Alice. Given a valid blind signature (m', z', c', s'), the signer can determine whether it does correspond to (m, r, z, a, b, c, s) by checking the following equation:

$$c' \stackrel{?}{=} H(m' \| z' \| a^{c'c^{-1}} g^{s' - c'c^{-1}s} \| (m')^{s'} (z')^{-c'}) \tag{4}$$

where c^{-1} is the reverse of c in group Z_q^*. If it holds, the signer can claim that the blind signature (m', z', c', s') is sent to Alice.

Correctness

$$a^{c'c^{-1}} g^{s' - c'c^{-1}s} = a^u g^{s' - us} = a^u g^v = a'$$

Clearly, if a protocol view $(\bar{m}, \bar{r}, \bar{z}, \bar{a}, \bar{b}, \bar{c}, \bar{s})$ does not match the blind signature (m', z', c', s'), the above equation (4) cannot hold. Otherwise, set

$$\bar{u} = c'(\bar{c})^{-1} \ (mod\ q), \quad \bar{v} = s' - c'(\bar{c})^{-1}(\bar{s}) \ (mod\ q),$$

we have

$$\bar{a}^{c'(\bar{c})^{-1}} g^{s'-c'(\bar{c})^{-1}(\bar{s})} = \bar{a}^{\bar{u}} g^{\bar{v}} = a' = a^u g^v \quad (mod\ p)$$

Combining the generation of the protocol view, we know there exists a number $\bar{r} \in Z_q^*$ such that $\bar{a} = g^{\bar{r}}\ (mod\ p)$. Hence,

$$\bar{r}\bar{u} + \bar{v} = ru + v \quad (mod\ q)$$

But the probability of the event is negligible because $\bar{r}, r, u, v$ are randomly picked in signing.

6 Conclusion

In the paper, we show the several blind signature schemes [1,2,3] are linkable. Our results show that they are not secure.

References

[1] Fangguo Zhang and Kwangjo Kim. ID-Based Blind Signature and Ring Signature from Pairings. ASIACRYPT2002, LNCS 2501, 533-547.

[2] G. Maitland and C. Boyd, A provably secure restrictive partiall blind signature scheme, PKC 2002, LNCS 2274, pp. 99-114, 2002. Springer-Verlag.

[3] Stefan Brands. Untraceable off-line cash in wallets with observers. In Douglas R. Stinson, editor, Advances in CryptologyCRYPTO'93, LNCS vol.773, Springer-Verlag, 302C318.

[4] D. Chaum, Blind signatures for untraceable payments, Advances in Cryptology- Crypto 82, 199-203.

[5] C.P. Schnorr, Eficient signature generation by smart cards. Journal of Cryptology, 4(3): 161-174, 1991.