Asian Journal of Information Technology 5 (3) : 310-311, 2006

Zhang *et al.*'s Partially Blind Signature Revisited

[1]Wei Gao, [2]Xueli Wang and [3]Dongqing Xie
[1]College of Mathematics, Hunan University, Changsha,
[2]College of Mathematics, Guangzhou University, Guangzhou,
[3]College of Software, Hunan University, Changsha, Peoples Republic of China

Abstract: Partially blind signature is an important cryptographic primitive in privacy oriented e-commerce applications. In INDOCRYPT 2003, Zhang *et al.* proposed a new partially blind signature scheme more efficient than previous schemes. It was later showed linkable by Chow *et al.* and then respectively improved by both Chow *et al.* and Zhang *et al.* at the cost of poorer efficiency. However, in this short study we show that the cryptanalysis of Chow *et al.* is wrong. So the original partially blind signature scheme remains secure and the corresponding improvements are needless.

Key words: Zhang *et al.*, partially blind signature

INTRODUCTION

Blind signatures were first introduced by Chaum[1] and play a central role in cryptographic protocols such as e-cash or e-voting that require user anonymity. Partially blind signatures were introduced by Abe and Fujisaki[2] to allow the signer to explicitly include some agreed information in the blind signature. The partially blind signature is a regular digital signature, but it needs to satisfy two additional requirements (partial blindness):

- The signer assures that an issued signature contains the information that it desires and none can remove the embedded information from the signature.
- For the same embedded information, the signer cannot link a signature to the instance of the signing protocol that produces the corresponding blind signature.

In INDOCRYPT 2003, Zhang *et al.*[3] proposed a partially blind signature which is very efficient in terms of computation and communication and can provide batch verification. Unfortunately, it was later showed linkable by Chow *et al.*[4] and improved. And the original authors themselves, Zhang *et al.* also accepted this disadvantage and revised their original scheme. Of course, both improved schemes are less efficient than the original scheme. Especially, Chow *et al.*'s scheme lost a lot of efficiency since they applied the conventional paradigm mentioned in[2], i.e., converting a identity-based blind signature to a partially blind signature scheme.

REVIEW OF ZHANG *et al.*'s PARTIALLY BLIND SIGNATURE SCHEME

First, let us recall the corresponding mathematical tools used in the scheme. Let G_1 be a cyclic additive group generated by P whose order is a prime and G_2 be a cyclic multiplicative group with the same order. Let $e:G_1\times G_1\rightarrow G_2$ be a bilinear pairing with the following properties:

- Bilinearity: $e(aP,bQ) = e(P,Q)^{ab}$ for all $P,Q\in G_1$ and $a,b\in Z^*_q$
- Non-degeneracy: There exists $P,Q\in G_1$ such that $e(P,Q\in G_1$.
- Computability: There is an efficient algorithm to compute e(P,Q) for all $P,Q\in G_1$.

Zhang *et al.*'s scheme[3] is given as follows. The system parameters are params = $(G_1, G_2, e, q, P, H, H_0)$, where $G_1 = \langle P\rangle$, G_2, e, q are defined as above and $H:\{0,1\}^*\rightarrow Z_q, H:\{0,1\}^*\rightarrow G_1$ are hash functions.

KeyGen: The signers picks random $x\in_R Z^*_q$ and compute $P_{pub} = xP$. The public key is P_{pub} and the secret key is x.

Issue: Suppose the requester now wants to get the signature of message m and the requester has already negotiated with the signer on the agreed information c to be attached to the message. The interaction between the requester and the signer is as follows:

Blinding: The user randomly chooses a number $r\in_R Z^*_q$, $U = rH_0(m\|c)$ computes and sends U to the signer.

Corresponding Author: Wei Gao, College of Mathematics, Hunan University, Changsha, Peoples Republic of China

Signing: The signer sends back V, where $V = (H(c)+x)^{-1}U$.

Unblinding: The user computes $S = r^{-1}V$. Then (S,m,c) is the partially blind signature of the message m and public information c.

Verification: A verifier can accept this partially blind signature if and only if.

$$e(H(c)P, P_{pub}, S) = e(P, H_0(m \| c))$$

REVIEW OF CHOW *et al.*'S CRYPTANALYSIS AND OUR DISCUSSION

The cryptanalysis given by Chow *et al* is very simple as follows. Given a valid signature (S,m,c) and the view (U,V), any party can accept the partially blind signature (S,m,c) as the one produced by the instance of the Issue protocol (U,V) if and only if $e(S,U) = e(V,H_0(m\|c))$. However, the following theorem is enough to show their conclusion is wrong.

Theorem 1. Given any view (U,V) and any valid signature (S',m',c), the above mentioned equation $e(S',U) = e(V,H_0(m'\|c))$ always holds.

Proof. Let the signature and message corresponding to (U,V) is (S',m',c), then there exists $r \in Z^*_q$ such that:

$$U = rH_0(m \| c), V = \frac{1}{x + H(c)}U, S = \frac{1}{x + H(c)}H_0(m||c)$$

So, for some valid signature and message (S',m',c) satisfying

$$S' = \frac{1}{x + H(c)}H_0(m' || c)$$, we have:

and

$$e(V, H_0(m' || c)) = e(\frac{1}{x + H(c)}U, H_0(m' \| c)$$

$$= e(\frac{1}{x + H(c)}rH_0(m \| c), H_0(m' \| c)$$

$$= e(H_0(m' \| c), H_0(m||c)^{\frac{r}{x+H(c)}}$$

Now we have:

$$e(S',U) = e(V, H_0(m' \| c))$$

So, for any given valid signature (S',m',c) and the view of the execution of the issuing protocol (U,V) corresponding to any signature pair (S',m',c), the following equation always holds: $e(S,U') = e(V',H_0(m\|c))$. So we can not determine whether a signature (S,m,c) is issued by the view (U,V) through checking the above equation.

CONCLUSION

We point out the error in the cryptanalysis of the art-and-state partially blind signature based pairing in[4]. So we conclude that the original scheme remains secure and of course much more efficient than the so-called improved schemes in[4,3].

REFERENCE

1. Chaum, D., 1983. Blind Signatures for untraceable payments, Advances in Cryptology-Crypto 1982, Plenum Press, pp: 199-203.
2. Abe, M. and E. Fujisaki, 2002. How to date blind signatures, Advances in Cryptology-Asiacrypt 1996. LNCS 1163, Springer-Verlag, pp: 244-251.
3. Zhang, F., R. Safavi-Naini and W. Susilo, 2003. Efficient verifiably encrypted signature and partially blind signature from bilinear pairings'. Progress in Cryptology- INDOCRYPT 2003, LNCS 2904, Springer-Verlag and the Revised Version is Available at http://www.uow.edu.au/~fangguo. pp: 191-204.
4. Chow, S.S.M., L.C.K. Hui, S.M. Yiu and K.P. Chow, 2005. Two improved partially blind signature schemes from bilinear pairings', ACISP 2005. LNCS 3574, Springer-Verlag, pp: 316-328.