http://www.zju.edu.cn/jzus; E-mail: jzus@zju.edu.cn
ISSN 1009-3095 *Journal of Zhejiang University SCIENCE* V.5, No.1, P.40-44, Jan., 2004

Untraceable partially blind signature based on DLOG problem*

HUANG Zheng(黄征)†1, CHEN Ke-fei(陈克非)†1, KOU Wei-dong(寇卫东)†2

(*[1]Department of Computer Science and Engineering, Shanghai Jiaotong University, Shanghai 200030, China*)
(*[2]E-Business Institute, Hong Kong University, Hong Kong, China*)

†E-mail: Huang-zheng@cs.sjtu.edu.cn; chen-kf@cs.sjtu.edu.cn; weidong-kou@eti.hku.hk

Received Jan.22, 2003; revision accepted June 11, 2003

Abstract: This paper proposes a new untraceable Partially Blind Signature scheme which is a cross between the traditional signature scheme and the blind signature scheme. In this proposed scheme, the message M that the signer signed can be divided into two parts. The first part can be known to the signer (like that in the traditional signature scheme) while the other part cannot be known to the signer (like that in the blind signature scheme). After having signed M, the signer cannot determine if he has made the signature of M except through the part that he knows. We draw ideas from Brands' "Restricted Blind Signature" to solve the Untraceable Partially Blind Signature problem. Our scheme is a probabilistic signature scheme and the security of our Untraceable Partially Blind Signature scheme relies on the difficulty of computing discrete logarithm.

Key words: Partially blind signature, Digital signature, Blind signature
Document code: A **CLC number:** TP309

INTRODUCTION

We consider the problem of a user who wants to get a message signed by a signer in a blind and untraceable way. The message signed can be divided into two parts. One part (public) can be known to the signer (as in the traditional signature scheme) while the other part (private) should not be known to the signer (as in the blind signature scheme). This type of signature is called an Untraceable Partially Blind Signature. For example, a user wants a bank to sign a cheque. The bank just cares about the value of the cheque (the part that the signer knows), but does not care about other information (the part that the signer should not know), such as who receives the cheque. Even after the signature is verified by a third party, the bank, cooperating with the third party, should not be able to link the user with the cheque except through the value of the cheque worth.

Related works

Blind signature scheme, first introduced by Chaum (1983; 1985), allows a person to get a message signed by another party without revealing any information about the message to the other party. In untraceable blind signature scheme, the party who signed the message cannot determine if he has signed the message. Untraceable blind signature can be used in electronic cash. It has drawn much focus (Okamoto, 1991; Chaum *et al*., 1990; Franklin and Yung, 1993). Abe and Fujisaki (1996) have proposed a Partially Blind Signature scheme whose security is based on RSA; and also proposed a Partially Blind Signature scheme based on Schnorr's signature scheme and proved the security of the signature scheme (Abe and Okamoto, 2000).

This paper proposes a new untraceable Partially Blind Signature scheme. We borrow ideas from Brands' "Restricted Blind Signature" (Brands, 1995; 1999) to solve the untraceable Partially Blind Signature problem. The security of our Untraceable Partially Blind Signature scheme relies on the difficulty of computing a discrete logarithm. Our scheme is a probabilistic signature scheme while the scheme in Abe and Fujisaki (1996) is a deterministic one. In our

* Project (Nos: 69973031 and 90104005) supported by the National Natural Science Foundation of China

scheme, the user starts the signature process while in Abe and Okamoto (2000) the signer starts the signature process. We believe that allowing the user to start the signature process is more natural.

Notations

$H(\ldots)$: an intractable hash function.

U: the User who has a *Message* and wants S to sign the message in an untraceable and partially blind way.

S: the Signer who makes a valid signature.

V: the Verifier who checks the validity of a signature.

Message: denotes the message that U wants S to sign. *Message* can be divided into two parts: *pubmsg* and *primsg*. The *pubmsg* can be seen by the signer, and we call it the public part of *Message*, while the *primsg* should not be known to the signer, and we call it the private part of *Message*.

M: denotes the hash value of the *Message* that S really signed. M can also be divided into two parts: m_1 and m_2 with $m_1 = H(pubmsg)$ and $m_2 = H(primsg)$.

Description of Untraceable Partially Blind Signature

Here, we give an informal description of untraceable Partially Blind Signature. Untraceable Partially Blind Signature is a digital signature scheme with the following properties:

Unforgeable: As in the traditional digital signature scheme, it must be easy to recognize the validity of the signature, but difficult to forge it.

Partially blind: Signer signs a message M with full knowledge of m_1, but has no idea about m_2.

Untraceable: If Signer later sees the message/signature pair, he should not be able to tell whether he has signed it except through the public part of M that he knows.

Note that a more formal definition of Partially Blind Signature could be found in (Abe and Okamoto, 2000).

Outlining

This paper is organized as follows. In the second section we will recapitulate Brands' restrictive blind signature. In the third section, we will introduce our Untraceable Partially Blind Signature scheme. In the fourth section, we will give an evaluation of the Untraceable Partially Blind Signature scheme and the conclusion will be given in the last section.

RESTRICTIVE BLIND SIGNATURE

Let us start by recapitulating Brands' restrictive blind signature. The arithmetical operations in the restrictive blind signature scheme are performed in a group G_q of prime order q for which polynomial-time algorithms must be known to multiply, and can determine equality of elements, test membership, and to randomly select elements. Furthermore, no feasible algorithms for computing discrete logarithms in G_q should be known. The signer begins with a generator g of a group G_q of prime order mod p, and the public key h of the signer: $h = g^x$. Here x is the signer's private key. All the calculations are done modulo p, for some large prime p, unless otherwise stated. The powers of generator g produce the q numbers in G_q, and the prime q divides $p-1$. Then $g^q = g^{(p-1)} = 1 \bmod p$.

Let m denote a message. Brands' restrictive blind signature begins as follows:

STEP1: The user U sends a message m to the Signer. It is intended that S signs m with its secret key x.

STEP2: The signer S generates a random number w in G_q and sends to U the following elements:

$$z = m^x,\ a = g^w,\ b = m^w$$

STEP3: U generates a challenge c. To do this U first generates four random numbers: s, t and u, v in G_q. Using s, t and u, v, U computes

$$m' = m^s g^t,\ z' = z^s h^t$$

$$a' = a^u g^v,\ b' = a^{ut} b^{us} m'^v$$

Then U computes the hash value $c' = H(m', z', a', b')$ and sends to S the challenge c:

$$c = c'/u \bmod q$$

STEP4: S responds with

$$r = w + cx \bmod q$$

STEP5: U uses the challenge c and the response r to check that:

$$ah^c = g^r \text{ and } bz^c = m^r$$

If so, U can accept the signature. Then U can bind the signature by computing:

$$r' = ur + v \bmod q = w' + c'x \bmod q$$

Hence the r' is the response to the challenge c', but is, however only known to the receiver. m' is the blinded message, the pair (z', a', b', r') is the signature issued by the signer on the message m'. S has nothing about the signature and U cannot forge a signature.

On receiving the message m' and the corresponding signature pair $(z', a', b,' r')$, every verifier can check that:

$$a'h^{c'} = g^{r'} \text{ and } b'z'^{c'} = m'^{r'}$$

where

$$c' = H(m' \| z' \| a' \| b') \bmod q$$

Here we only give part of Brands' restrictive blind signature that is related to the construction of our untraceable Partially Blind Signature scheme.

UNTRACEABLE PARTIALLY BLIND SIGNATURE

There are three participant types in the Untraceable Partially Blind Signature scheme: a User U, a Verifier V, and a Signer S.

Preliminary setup

S chooses a generator g from G_q in Z_p^* and also selects a secret key x in G_q, and announces its public key $h = g^x \bmod p$. S additionally selects a collision-free hash function $H(\ldots)$ that outputs a member of the set Z_q. S announces p, q, g, h, H as public information, but keeps x secret. All the calculations are done modulo p, unless otherwise stated.

Partially Blind Signature Protocol

U and S all participate in the Partially Blind Signature protocol. In the protocol, U asks S to partially blind sign *Message* for him. The protocol proceeds as following:

STEP1: U sends m_1(the public part of M) and *pubmsg* (the public part of *Message*) to S. It is intended that S sign M with its secret key x.

STEP2: S checks if $m_1 = H(pubmsg)$. If so, S generates a random number w in G_q and sends to U the following elements:

$$z = m_1^x, \quad a = g^w, \quad b = {m_1}^w$$

z could be viewed as S's signature on m_1. a and b are used for randomization purpose.

STEP3: U generates a challenge c. To do this U first generates four random numbers: s, t and u, v in G_q. These variables are used for blinding purpose. Using s, t and u, v, U computes

$$m' = {m_1}^s g^t, \quad z' = z^s h^t$$

$$a' = a^u g^v, \quad b' = a^{ut} b^{us} m'^v$$

m' could be viewed as the blinded message and z' could be viewed as S's signature on m'. a' and b' are also used for randomization purpose. Then U computes the hash value $c' = H(m_1 \| s \| t \| z' \| a' \| b' \| m_2)$ and sends to S the challenge c:

$$c = c'/u \bmod q$$

STEP4: S responds to the challenge by calculating:

$$r = w + cx \bmod q$$

Then, S sends r to U.

STEP5: U uses the challenge c and the response r to check that:

$$ah^c = g^r \text{ and } bz^c = {m_1}^r$$

If the two equations hold, U can accept what was generated by S. Then U can calculate the blinded signature by computing:

$$r' = ur + v \bmod q$$

The valid Signature token is the pair $\{(m_1, m_2), (s, t, z', a', b', r')\}$.

Definition a valid Partially Blind Signature is a pair $\{(m_1, m_2), (s, t, z'a', b', r')\}$ which has the following relationships:

$$a'h^{c'} = g^{r'}$$
$$b'z'^{c'} = m'^{r'}$$

where

$$m' = {m_1}^s g^t$$
$$c' = H(m_1 \| s \| t \| z' \| a' \| b' \| m_2)$$

Verify protocol

After an untraceable Partially Blind Signature is made, every party can verify the validity of the signature. To do so, the Verifier (V) interacts with U as follows:

STEP1: U sends $\{(m_1, m_2), (s, t, z', a', b', r')\}$ and *Message* to V.

STEP2: V checks if $m_1 = H(pubmsg)$ and $m_2 = H(primsg)$. If the check passes, V calculates $c' = H(m_1 \| s \| t \| z' \| a' \| b' \| m_2)$, $m' = m_1^s g^t$ and checks if

$$a' h^{c'} = g^{r'} \tag{1}$$

And

$$b' z'^{c'} = m'^{r'} \tag{2}$$

If so, the signature is valid, V can accept it.

EVALUATION OF UNTRACEABLE PARTIALLY

Correctness

If all the players follow the protocol, correctness of our untraceable Partially Blind Signature is straightforward. Eq.(1) holds because:

$$\text{Eq.(1): left} = a' h^{c'} = a^u g^v h^{uc} = g^{wu} g^v g^{xuc} = g^{u(cx+w)+v} = g^{ur+v} = g^{r'} = \text{right}$$

Eq.(2) holds because:

$$\text{Eq.(2): left} = b' z'^{c'} = a^{ut} b^{us} m_1^{vs} g^{tv} z^{ucs} h^{tuc} = g^{wut} m_1^{usw} m_1^{vs} g^{tv} m_1^{xucs} g^{xuc} = m_1^{usw+uscx+vs} g^{utw+utcx+tv} = m_1^{us(w+cx)+vs} g^{ut(w+cx)+tv} = m_1^{sr'} g^{tr'} = m'^{r'} = \text{right}$$

Unforgeable

Proposition 1 Given that Brands' restrictive blind signature is unforgeable and the intractability of the hash function H, our untraceable Partially Blind Signature is unforgeable.

Proof We do not prove the unforgeability of our untraceable Partially Blind Signature scheme directly. What we show in this proof is that if U could forge a valid untraceable Partially Blind Signature, U could also forge a valid restrictive blind signature of Brands. Provided that Brands' restrictive blind signature is unforgeable this will lead to a contradiction.

A valid restrictive blind signature is a message m' with the corresponding signature pair (z', a', b', r') which satisfy Eq.(1) and Eq.(2), where

$$c' = H(m', z', a', b') \bmod q$$

Our untraceable Partially Blind Signature is a message pair (m_1, m_2) with the corresponding signature pair (s, t, z', a', b', r') which satisfy Eq.(1) and Eq.(2), where

$$m' = m_1^s g^t \quad \text{and}$$
$$c' = H(m_1 \| s \| t \| z' \| a' \| b' \| m_2)$$

Suppose that U could fake a valid untraceable Partially Blind Signature. Because of the intractability of hash function H, U has to fix $m_1, s, t, z', a', b', m_2$ to compute c'. This means that given m' (determined by m_1, s, t), z', a', b', m_2, c' (determined by hash function), U could calculate a value r' which satisfies the Eq.(1) and Eq.(2). This implies that by setting m_2 to $\perp$, U could calculate the pair $\{m', z', a', b', r'\}$, which is a valid restrictive blind signature.

Partially blinding

Proposition 2 Given that the intractability of the hash function H and u is selected at random, our untraceable Partially Blind Signature satisfies the partially blinding property.

Proof Obviously, in our Untraceable Partially Blind Signature scheme, S knows m_1 which is the public part of M because U had sent m_1 to S in plain text. The information that S knows about m_2 is just $c' = H(m_1 \| s \| t \| z' \| a' \| b' \| m_2)$ and $c = c'/u \bmod q$. u is selected by U randomly and is unknown to S. S could by no means calculate m_2.

Untraceable

Proposition 3 Given the intractability of the hash function H and that it is hard to solve the D-LOG problem, we declare that even if the signer S cooperates with a verifier V, the signer could not figure out if the signature is signed by him except through the public part of the message that is known to him.

Proof Let us define $View(P, protocol)$ as the set that contains all the elements which P can see in *protocol*. So $View(S, signature)$ represents what S sees in the signature protocol and we can compute that $View(S, signature) = \{m_1, z, a, b, c, w\}$. $View(V, verify)$ represents what V sees in the verify protocol and we can compute $View(V, verify) = \{m_1, s, t,$

z', a', b', r', m_2}. U could not be traced out iff S cannot link *View*(S, *signature*) with *View*(V, *verify*) except through m_1. In our system, U does not leak any information about the pair $\{u, v\}$ that U chooses randomly. So if S cannot solve the problem of D-LOG, in no way could S calculate from the elements in *View*(V, *verify*) to any element in *View*(S, *signature*) except the element m_1 and vice versa. This means S cannot link the two *Views* and the Untraceable Partially Blind Signature cannot be traced except through the value m_1.

CONCLUSIONS

Untraceable Blind Signature protects the privacy of the User well, but makes the Signer uneasy because he knows nothing about what he has signed. The traditional digital signature scheme makes the signer very confident, but the User loses privacy. There is a request that when signing a message, the user just shows the signer the part that the signer cares about and lets the other part (the privacy of the user) be unknown to the signer. Our Untraceable Partially Blind Signature scheme solves the problem well. We solve the Untraceable Partially Blind Signature problem by borrowing ideas from Brands' Restricted Blind Signature scheme. The computation in the signature scheme is quite efficient.

References

Abe, M. and Fujisaki, E., 1996. How to date blind signatures. Advances in Cryptology – ASIACRYPT '96, LNCS, **1163**: 244 – 251.

Abe, M. and Okamoto, T., 2000. Provably Secure Partially Blind Signatures. Advances in Cryptology – Crypto' 2000, LNCS, **1880**: 271 – 299.

Brands, S., 1995. Off-Line Electronic Cash Based on Secret-Key Certificates. Proceedings of the Second International Symposium of Latin American Theoretical Informatics (LATIN'95), p.131 – 166.

Brands, S, 1999. Rethinking Public Key Infrastructures and Digital. Certificates-Building in Privacy, Doctoral Dissertation, Ponsen & Looijen BV, Set. **4**: 287.

Chaum, D. , Fiat, A. and Naor, M., 1990. Untraceable Electronic Cash. Advances in Cryptology – Crypto'88, Spinger-Verlag, p.319 – 327.

Chaum, D., 1983. Blind signatures for untraceable payments. Advances in Cryptology – Crypto'82, Springer-Verlag, p.199 – 203.

Chaum, D., 1985. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, **28**(10): 1030 – 1044.

Franklin, M. and Yung, M., 1993. Secure and efficient off-line digital money. Proceedings of ICALP' 93, LNCS, **700**: 265 – 276.

Okamoto, T., 1991. Universal Electronic Cash. Advances in Cryptology – Crypto'91, LNCS, **576**: 324 – 337.