New ID-based Fair Blind Signatures

Girraj Kumar Verma
Department of Mathematics,
Hindustan College of Science and Technology, Farah, Mathura, India
girrajv@gmail.com

Abstract: A blind signature scheme is a cryptographic primitive in which a user can obtain a signature from the signer without revealing any information about message signature pair. Blind signatures are used in electronic payment systems, electronic voting machines etc. The anonymity of blind signature scheme can be misused by criminals by money laundering or by dubious money. To prevent these crimes, the idea of fair blind signature scheme was given by Stadler et al . In fair blind signature scheme there is a trusted third party judge who can provide a linking protocol for signer to link his view to the message signature pair. In this paper we are proposing some identity based fair blind signatures.

Key Words: ID-based signature, Fair Blind Signature, Blind Signature, Oblivious Transfer,

1. Introduction: The idea given by Diffey and Hillman [11] in their seminal paper “New directions in Cryptography”, in 1976 has played a critical role in Cryptography. This paper developed public key cryptography which developed the signature schemes for authenticity of the source and sender. In 1983 [5] D. Chaum gave the idea of blind signature scheme for electronic payment system. In 1993 [17] Micali has introduced the concept of fair cryptosystems to prevent the misuse of strong cryptographic systems by criminal. In 1995 [22] Stadler et al have given fair blind signature schemes using cut and choose method and oblivious transfer protocol.

In 1984 [21] Shamir has given the idea of identity based cryptosystems. The first ID based cryptosystem was proposed by Boneh and Franklin [1] in 2003 that uses bilinear pairing. In this paper we are proposing two fair blind signatures one using cut and choose and second using oblivious transfer protocol.

The paper is organized as follows:

In section 2 we have given the definition of fair blind signature scheme. In section 3 we have given the definition of bilinear pairing. In section 4 we have considered fair blind signatures by Stadler et al and our proposed schemes.

2. Fair Blind Signature Scheme: In a fair blind signature scheme there are several senders, one signer and one trusted entity, e.g. judge, and two protocols:

1- A signing protocol, involving the signer and a sender.
2- A link recovery protocol, involving the signer and the judge.

By executing the signing protocol, the sender obtains a valid signature on a message of his choice such that the signer cannot link his view of the protocol to the resulting message signature pair. By running the link recovery protocol, the signer obtains information from the judge that enables him to recognize the corresponding protocol view and message signature pair. There are two types of fair blind signatures, depending on the information the signer receives from the judge during link recovery protocol:

Type-1: Given signer's view of the protocol, the judge delivers information that enables the signer (or to every body) to efficiently recognize the corresponding message signature pair (e.g. judge can extract the message).

Type-2: Given the message signature pair, the judge delivers information that enables the signer to efficiently identify the sender of that message or to find the corresponding view of the signing protocol.

There are different applications of fair blind signatures. One is to provide a tool to prevent money laundering in anonymous payment systems. In a payment system based on type-II fair blind signature scheme the authorities can determine the origin of dubious money, while in systems based on type-I they can find out the destination of suspicious withdrawals..

Another application is the perfect crime scenario described in [23]: a customer is blackmailed and forced to anonymously withdraw digital money from his account, acting as an intermediary between the blackmailer and the bank. In a perfectly anonymous payment system, the ransom could not be recognized later, but if a (type-I) fair blind signature scheme had been used, the judge, when the bank's view of the withdrawal protocol, can trace the blackmailed coin.

3. Bilinear Pairing: Let G_1, G_2 be two groups of same prime order *q*. We view G_1 as additive group (group of points on elliptic curves) and G_2 as a multiplicative group. Let *P* be an arbitrary generator of G_1. Assume that DLP (discrete log problem) is hard, in both G_1 and G_2.

A mapping $e : G_1 \times G_1 \to G_2$ satisfying the following properties is called a bilinear map:

Bilinearity: $e(aP, bQ) = e(P, Q)^{ab} \forall P, Q \in G_1, \forall a, b \in \mathbb{Z}_q^*$.

Or this can be restricted as follows: $\forall P, Q, R \in G_1, e(P+Q, R) = e(P, R)e(Q, R)$ and $e(P, Q+R) = e(P, Q)e(P, R)$

Nondegeneracy: If *P* is a generator of G_1 then $e(P, P)$ is a generator of G_2.

4. Fair Blind signatures by Stadler et al[22]: These signatures are based on Chaum's blind signatures and on cut and choose method. The system parameters are as follows:

- (n, e), the signer's public key as used in RSA signature.
- $E_J(\cdot)$, the enciphering function of a judge's public key cryptosystem.
- H, a one way hash function.
- *k* a security parameter.

The Protocol:

Sender **Signer**

For $i = 1, 2, ...2k$

Chooses randomly $r_i \in Z_n$

and strings α_i, β_i

$u_i = E_J(m \| \alpha_i)$

$v_i = E_J(ID \| \beta_i)$

$m_i = r_i^e H(u_i \| v_i) \bmod n$ $\xrightarrow{m_i}$

randomly choose a subset
$S \subset \{1, 2, ...2k\}$ of size k

$\xleftarrow{\text{S}}$

For all $i \in S$ $\xrightarrow{r_i, u_i, \beta_i}$ for every $i \in S$ check

$m_i = H(u_i \| E_J(ID \| \beta_i)) \bmod n$

$b = (\prod_{i \notin S} m_i)^{1/e} \bmod n$

$\xleftarrow{b}$

$s = b / (\prod_{i \notin S} r_i) \bmod n$

The resulting signature consists of *s* and the set of pairs $T = \{(\alpha_i, v_i) \mid i \notin S\}$.

The signatures can be verified by the checking that:

$$s^e = \prod_{(\alpha, v) \in T} H(E_J(m \| \alpha) \| v) \bmod n$$

At the end of an execution of the signing protocol, the signer is convinced that, with overwhelming probability, each v_i has been formed correctly. Since every v_i depends on *ID*, it is impossible for a dishonest signer to use information received during different sessions to generate a signature following the signing protocol.

Proposed fair blind signatures: In this section we are giving two fair blind signatures. Our first scheme is based on cut and choose method and second scheme is based on fair oblivious transfer.

4.1: Using cut and choose: This scheme is based on signature scheme given by K.G. Peterson [19]. Let G_1 be an additive group of prime order *q* and G_2 be a multiplicative group of same order *q*. We assume the existence of a bilinear map $e: G_1 \times G_1 \rightarrow G_2$ with the property that discrete logarithm problem in both G_1 and G_2 is hard. Typically G_1**,** will be a subgroup of the group of points on an elliptic curve over a finite field, G_2 will be a subgroup of the multiplicative group of a related finite field and map *e* will be derived from the Weil or Tate pairing on the elliptic curve. We also assume that an element $P \in G_2$, satisfying $e(P, P) \neq 1_{G_2}$ is known.

Let *ID_s* be a string denoting the identity of a signer, *ID* is the string denoting session identifier of a user and H_1, H_2 and H_3 be public cryptographic hash functions. We compute $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $H_3 : G_1 \rightarrow \mathbb{Z}_q$. In our scheme a signer's public key is $Q_{ID} = H_1(ID_s)$ and secret key is $D_{ID} = sQ_{ID}$ where $s \in_R \mathbb{Z}_q^*$ chooses by TA as his master key. We also assume $P_{pub} = sP$ publicly known.

The Protocol:

1. Let the user wants to obtain signature from signer on the message $m \in \{0,1\}^*$. For doing so, both of them agree upon $ID \in \{0,1\}^*$ as session identifier and $\alpha_i, \beta_i \in_R \{0,1\}^*$ for *i=1, 2 …, 2l*, where *l* is security parameter.
2. User computes $u_i = E_J(m \,||\, \alpha_i)$ and $v_i = E_J(ID \,||\, \beta_i)$, where $E_J(.)$ is encryption function of judge.
3. Then computes $m_i = H_2(u_i \,||\, v_i)$ and sends to signer.
4. Signer chooses $S \subseteq \{1, 2, ...2l\}$ of size *l* and sends to user.
5. User sends u_i, β_i for $i \in S$ to signer.
6. Signer receives and checks $m_i = H_2(u_i \,||\, E_J(ID \,||\, \beta_i))$ for $i \in S$.
7. Signer computes $R = kP, b = \prod_{i \notin S} m_i$ and $S_1 = k^{-1}(bP + H_3(R)D_{ID_s})$ and sends (*R*, *S₁)* to user.
8. User display (*R*, *S₁*, *T)* as signature, where $T = \{(\alpha_i, v_i)|\ \mathrm{i} \notin \mathrm{s}\}$.

Verification by receiver: To verify the signature, receiver runs the following steps:

1. Receiver computes $b = \prod_{i \notin S} H_2(E_J(m \,||\, \alpha_i) \,||\, v_i)$, $H_3(R)$ and $Q_{ID} = H_1(ID_s)$.
2. Computes $e(P,P)^b e(P_{pub}, Q_{ID})^{H_3(R)}$ and $e(R, S_1)$.
3. Accept the signature iff $e(P,P)^b e(P_{pub}, Q_{ID})^{H_3(R)} = e(R, S_1)$

Proof of Verification:

$$\begin{aligned} e(R, S_1) &= e(kP, k^{-1}(bP + H_3(R)D_{ID})) \\ &= e(P, bP + H_3(R)D_{ID}) \\ &= e(P, bP)e(P, H_3(R)D_{ID}) \\ &= e(P,P)^b e(P, D_{ID})^{H_3(R)} \\ &= e(P,P)^b e(P, sQ_{ID})^{H_3(R)} \\ &= e(P,P)^b e(sP, Q_{ID})^{H_3(R)} \\ &= e(P,P)^b e(P_{pub}, Q_{ID})^{H_3(R)} \end{aligned}$$

Blindness & Disclosure by judge: Since user sends the value of $u_i = E_J(m \,||\, \alpha_i)$ and β_i to the signer, so signer cannot link his view of protocol to the resulting message signature pair. Since signer can verify the m_is randomly, so user cannot obtain signature on a wrong message.

When signer wants to check *m* or ID (session identifier), he requests to Judge. The judge takes $u_i = E_J(m \| \alpha_i)$ and $v_i = E_J(ID \| \beta_i)$ and after decryption of these he does the following steps:
* Given the values $u_i, i \in S$, the judge can disclose the message *m* as in [22]. Therefore the scheme is of type-I.
* Given the signature *(R, S_1, T)*, the judge can easily compute the identification string *ID* as in [22]. Therefore the scheme is of type-II.

4.2 Using oblivious transfer: In this section we are giving the fair blind signature using oblivious transfer [13]. We are developing this scheme on a variation of Fiat-Shamir signature scheme as described in [22]. In [22] Stadler *et al* have explained the variation but they have not used identity of the signer, but here we are taking the identity version of the variation used in [22]. For more information about oblivious transfer please refer [13, 22].

ID-based variation of Fiat-Shamir signature: First we are giving Shamir signature scheme, and then we will give Fiat Shamir signature scheme.

Shamir signature:
Extraction: 1. Signer chooses two large primes *p* and *q* then computes $n = pq$.
2. Chooses *e* such that $(e, \phi(n)) = 1$ and computes $d = e^{-1} \bmod \phi(n)$.
3. Chooses a cryptographic one way hash function H.
Then Param = <*n, e,* H> and master key is <*p, q, d* >

Signing: Let ID be the user's identity such that $g = ID^d \bmod n$. Signer does the following steps:

1. Chooses $r \in_R \mathbb{Z}_n^*$ and computes $t = r^e \bmod n$.
2. Then computes $s = gr^{H(t,m)}$.
3. Then $\sigma = (s,t)$ is a signature.

Verification: Verifier accepts the signature iff $s^e = IDt^{H(t,m)} \bmod n$.
Variation of Fiat Shamir signature: Extraction phase of the scheme is same as in above, so param = <*n, e,* H> and the master key is <*p, q, d* >.
Signing: Let *ID* be the user's identity such that $g = ID^d \bmod n$. For a security parameter *k* (*k>80*) let us define $y_i = H(ID + i) \bmod n$ and $x_i = y_i^d \bmod n$ for *i=1,2,….k*. To sign the message *m,* signer does the following steps:

1. Chooses $r \in_R \mathbb{Z}_n^*$ and computes $t = r^e \bmod n$.
2. Computes $C = H(t \| m)$ and let c_i be the *i*th bit of *C*.
3. Computes $s = g\prod_{i=1}^{k} x_i^{c_i} \bmod n$.

Then $\sigma = (s,t)$ is a signature.

Verification: Verifier accept the signature iff $s^e = ID\prod_{i=1}^{k} H(ID + i)^{c_i} \bmod n$.

Proposed fair blind signature: The params and secret keys are same as above described and let message to be signed is *m*.

User **Signer**

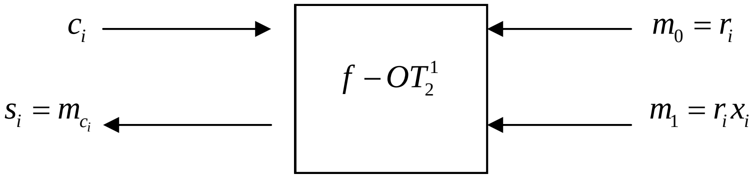
* Chooses $r_1, r_2, ...r_k \in_R \mathbb{Z}_n^*$ and computes

* User Chooses $\alpha \in_R \mathbb{Z}_n^*$ $\xleftarrow{\quad t \quad}$ $t = \prod_{i=1}^{k} r_i^e \bmod n$ and sends *t* to user.

and computes $\tilde{t} = t\alpha^e \bmod n$.

* Computes $C = H(\tilde{t} \,||\, m)$ and let c_i be the *i*th bit of *C*.

For $i = 1, 2, ...k$ do



* Computes $\tilde{s} = \alpha \prod_{i=1}^{k} s_i \bmod n$.

Then pair $\sigma = (\tilde{s}, \tilde{t})$ is a valid signature.

Verification: Verifier accepts the signature iff $\tilde{s}^e = \tilde{t} \prod_{i=1}^{k} (H(ID + i))^{c_i} \bmod n$.

Blind ness and fairness: Let us analyze the blindness of this scheme. We assume that the signer cannot determine the selection bit c_i (because of the $f - OT_2^1$). So *t* is the only value the signer could use to recognize the signature later. But for each valid signature $\sigma = (\tilde{s}, \tilde{t})$ of a message *m* there is exactly one α with $\tilde{t} = t\alpha^e \bmod n$ and therefore $\tilde{s} = \alpha \prod_{i=1}^{k} r_i x_i^{\tilde{c}_i} \bmod n$, where $\tilde{c}_i$ is the ith bit of $H(\tilde{t} \,||\, m)$. So the resulting signature is independent of the signing protocol and the signature scheme is perfectly blind (from the signer's point of view).

On the other hand considering the fairness of the scheme, if the signer sends the view of the protocol to the judge, the selection bit c_i can be determined and therefore the challenge *C* is known. This value could then be put onto a black list, so that everybody can be recognized that message signature pair later.

Conclusion: In the paper we have introduced two identity based fair blind signature schemes. However these schemes are not efficient, because more data is exchanged during signing but these provides an identity based solution for the misuses of anonymity in signature schemes. According our source of information both of the two schemes are discussed first time.

References:

[1]: D. Boneh and M. Franklin, *Identity based encryption from the Weil pairing*, SIAM J. of computing, 32(3), pp. 586-615, 2003, extended abstract in Crypto-2001.

[2]: S. Brands, *Untraceable off-line cash in wallets with observers*, Proceedings of Crypto93, LNCS#773, Springer Verlag, pp. 302-318, 1993.

[3]: J. Camenisch, J. M. Piveteau, M. Stadler, *Blind signatures based on the Discrete logarithm problem*, Proceedings of Eurocrypt94, LNCS#950, Springer Verlag, pp. 428-432, 1994.

[4]: J. Camenisch, J. M. Piveteau, M. Stadler, *An efficient payment system protecting privacy*, Proceedings of ESORICS 94, LNCS#875, Springer Verlag, pp. 207-215, 1994.

[5]: D. Chaum, *Blind signature systems*, Proceedings of Crypto 83, Springer Verlag, pp. 153-158, 1983.

[6]. D. Chaum, E. Van Heyst, *Group signatures,* Proceedings of Eurocrypt 91, LNCS#547, Springer Verlag, pp.257-265, 1991.

[7]: D. Chaum, A. Fiat, M. Naor, *Untraceable electronic cash,* Proceedings of Crypto 88, LNCS#403, Springer Verlag, pp. 319-327, 1988.

[8]: D. Chaum, *Privacy protected systems,* SMART CARDS 2000, Elseveir Science Publishers B. V. (North Holland), 1989, pp. 69-93.

[9]: D. Chaum, B. DenBoer, E. Van Heyst, S. MjFlsnes, A. Steenbeek, *Efficient offline electronics checks,* Proceedings of Eurocrypt 89, LNCS#434, Springer Verlag, pp. 294-301, 1989.

[10]: D. Chaum, T. Pedersen, *Wallet databases with observers*, Proc. Crypto-92, LNCS#740, Springer Verlag, pp. 89-105, 1992.

[11]: W. Diffey and M. E. Hellman. *New directions in cryptography*, IEEE transaction on Information Theory, 22(6),pp. 74-84, June 1977.

[12]: Ratna Dutta, Rana Barua and Palash Sarkar, *Pairing based cryptographic protocols: A survey,* available at http://eprint.iacr.org/2004/064.

[13]: S. Even, O. Goldreich, A. Lempel, *A randomized protocol for signing contracts*, Communications of the ACM, 28, pp. 637-647, 1985.

[14]: N. Ferguson, *Single term offline coins,* Proc Eurocrypt-93, LNCS#765, Springer Verlag, pp. 318-328, 1993.

[15]: A. Fiat and A. Shamir, *How to prove yourself: Practical solution to identification and signature problems*, Proc. Of Crypto-86, LNCS#263, Springer Verlag, pp. 186-194, 1986.

[16]: F. Hess, *Efficient identity based signature schemes based on pairing*, Selected areas in Cryptography 9th annual workshop, SAC 2003, LNCS#2595, Springer Verlag, pp. 310-324, 2003.

[17]: S. Micali, *Fair cryptosystems*, Technical Report MIT/LCS/TR-579, 1993.

[18]: T. Okamoto, K. Ohta, *Universal electronic cash,* Proc. Crypto-91, LNCS#576, Springer Verlag, pp. 324-337, 1991.

[19]: K. G. Peterson, *Identity based signatures from pairing on elliptic curves,* available at http://eprint.iacr.org/2002/004.

[20]: R. L. Rivest, A Shamir, and L. Adleman, *A method for obtaining digital signatures and public key cryptosystems,* Communications of the ACM 21, pp. 120-126, 1978.

[21]: A. Shamir, *Identity based cryptosystems and signature schemes,* Proc. Crypto-84, LNCS#196, Springer Verlag, pp. 47-53, 1984.

[22] M. Stadler, M. Piveteau, and J. Camenisch, *Fair blind signatures,* Eurocrypt-95, LNCS#921, Springer Verlag, pp. 209-219, 1995.

[23]: S. Von Solms and D. Naccache, *On blind signatures and perfect crime,* Computer & Security -11, pp. 581-583, 1992.