Fair Blind Signatures

Markus Stadler[1], Jean-Marc Piveteau[2], Jan Camenisch[1]

[1] Institute for Theoretical Computer Science
ETH Zürich
CH-8092 Zürich, Switzerland
Email: {stadler, camenisch}@inf.ethz.ch

[2] Union Bank of Switzerland
UBILAB
Bahnhofstrasse 45
CH-8021 Zürich, Switzerland
Email: piveteau@ubilab.ubs.ch

Abstract. A blind signature scheme is a protocol for obtaining a signature from a signer such that the signer's view of the protocol cannot be linked to the resulting message-signature pair. Blind signature schemes are used in anonymous digital payment systems. Since the existing proposals of blind signature schemes provide perfect unlinkability, such payment systems could be misused by criminals, e.g. to safely obtain a ransom or to launder money. In this paper, a new type of blind signature schemes called fair blind signature schemes is proposed. Such schemes have the additional property that a trusted entity can deliver information allowing the signer to link his view of the protocol and the message-signature pair. Two types of fair blind signature schemes are distinguished and several realizations are presented.
Keywords. Blind signatures, fair cryptosystems, electronic payment systems, cryptographic protocols.

1 Introduction

The concept of a blind signature scheme was introduced by Chaum [4]. A blind signature scheme is a cryptographic primitive involving two entities: a sender and a signer. It allows the sender to have a given message signed by the signer, without revealing any information about the message or its signature. Blind signature schemes have been used to realize cryptographic protocols providing the anonymity of some of the participants, e.g. voting protocols and secure electronic payment systems (e.g. [1, 3, 6, 7, 8, 11, 14])

Several realizations of blind signature schemes have been proposed [2, 4, 9]. All the existing proposals provide perfect unlinkability, i.e. it is impossible (in an information theoretical sense) except for the sender to link a message-signature pair to the corresponding instance of the signing protocol.

[1] The first and the third author are supported by the Swiss Federal Commission for the Advancement of Scientific Research (KWF) and by the Union Bank of Switzerland.

Unfortunately, this anonymity could be misused by criminals. In anonymous electronic payment systems blind signatures prevent linking the withdrawal of money and the payment made by the same customer. The impossibility to relate withdrawals and payments allows perfect black-mailing [16] or money-laundering. It has been argued that this is not a problem if such payment systems are only used for small amounts. We believe that the problem still exists, especially for fully digital payment systems: it could be possible to automatically perform a large number of payments and thereby transfer huge amounts of money anonymously. Therefore, it would be useful if the anonymity could be removed with the help of a trusted entity, when this is required for legal reasons.

In [13] Micali introduces the concept of fair cryptosystems to prevent the misuse of strong cryptographic systems by criminals. We pursue a similar goal for blind signature schemes by proposing a new type of blind signature schemes, called fair blind signature schemes. They have the additional property that, with the help of a trusted entity, it is possible to link a message-signature pair and the corresponding protocol view of the signer. This concept is discussed in Section 2. Several fair blind signature schemes are presented in the last three sections.

2 The Concept of Fair Blind Signatures

The model of a fair blind signature scheme consists of several senders, a signer and a trusted entity, e.g. a judge, and of two protocols (see Fig. 1):

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

By executing the signing protocol, the sender obtains a valid signature of 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 signature schemes, depending on the information the judge receives from the signer during the link-recovery protocol:

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

Theoretically, a type I fair blind signature scheme can also be used to link a given message-signature pair to a view of the protocol by running the link-recovery protocol with all views as inputs, but this is inefficient. The same holds for type II schemes.

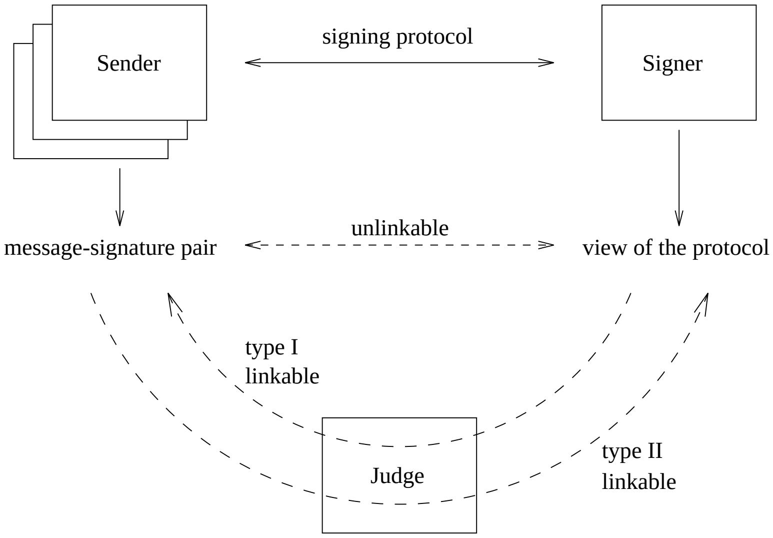


Fig. 1. The model of a fair blind signature scheme

There are different applications for 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 signatures the authorities can determine the origin of dubious money, while in systems based on type I signatures they can find out the destination of suspicious withdrawals.

Another application is the "perfect crime" scenario described in [16]: 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 given the bank's view of the withdrawal protocol, can trace the blackmailed coins. Unfortunately, our realizations of fair blind signatures do not solve the general problem of blackmailing: a cheating sender could try to force the signer to use a different, truly blind signing protocol. The solution of this general blackmailing problem seems to be difficult.

3 Fair Blind Signatures using Cut-and-Choose

We first present a fair blind signature scheme based on Chaum's blind signature scheme and on the well-known cut-and-choose method [4, 6]. The system parameters are as follows:

- (n, e), the signer's public key ($n = pq$ is the product of two large primes and e is an integer relatively prime to $\varphi(n) = (p-1)(q-1)$).
- $E_J(\cdot)$, the enciphering function of a judge's public key cryptosystem.

- $\mathcal{H}$, a one-way hash function.
- k, a security parameter (e.g. $k > 20$).

The sender and the signer first agree on a session identifier ID (each instance of the signing protocol should correspond to a different value of ID). Then, they perform the following protocol (where $||$ denotes the concatenation of strings).

Sender		**Signer**
for $i = 1, \ldots, 2k$ randomly choose $r_i \in \mathbb{Z}_n$ and strings α_i, β_i $u_i = E_J(m\|\|\alpha_i)$ $v_i = E_J(ID\|\|\beta_i)$ $m_i = r_i^e \mathcal{H}(u_i\|\|v_i) \pmod n$	$\xrightarrow{m_i}$	
	$\xleftarrow{S}$	randomly choose a subset $S \subset \{1, \ldots, 2k\}$ of size k
for all $i \in S$	$\xrightarrow{r_i,\ u_i,\ \beta_i}$	
		for every $i \in S$ check $m_i \stackrel{?}{=} r_i^e \mathcal{H}(u_i\|\|E_J(ID\|\|\beta_i)) \pmod n$
		$b = \left(\prod_{i \notin S} m_i\right)^{1/e} \pmod n$
	$\xleftarrow{b}$	
$s = b / \prod_{i \notin S} r_i \pmod n$		

The resulting signature consists of s and the set of pairs $T = \{(\alpha_i, v_i) | i \notin S\}$. The signature can be verified by checking that:

$$s^e \stackrel{?}{=} \prod_{(\alpha,v) \in T} \mathcal{H}(E_J(m||\alpha)||v) \pmod n .$$

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 sender to use information received during different sessions to generate a signature without following the signing protocol. Furthermore, the probability that the sender can obtain a correct signature with forged u_i is negligible.
It is easy to see that this is a fair blind signature scheme of type I and II:

- Given the values u_i, $i \in S$, the judge can disclose the message m (note that it is very unlikely that all of the u_i are forged). Therefore, the scheme is of type I.

- Given the signature (s, T), the judge can easily compute the identification string ID by decrypting the v's in T. Therefore, the scheme is of type II.

The scheme can now be modified in order to be of type I or type II, only:

- Compute all v_i as $v_i = \mathcal{H}(ID||\beta_i)$. Since the judge cannot disclose the session identifier ID anymore, this scheme is of type I, only.
- Compute all u_i as $u_i = \mathcal{H}(m||\alpha_i)$. Since the judge cannot disclose the message m anymore, this scheme is of type II, only.

Unfortunately, this fair blind signature scheme is inefficient: a large amount of data is exchanged during the signing protocol, and the resulting signature is long. More efficient implementations are considered in the next sections.

4 Type I Fair Blind Signatures using Oblivious Transfer

The type I fair blind signature scheme presented in this section is based on a variation of the Fiat-Shamir signature scheme [12] and on the concept of one-out-of-two oblivious transfer [10]. Although the signing protocol is still inefficient, the resulting signature is very short.

4.1 A Variation of the Fiat-Shamir Signature Scheme

Let $n = pq$ be the product of two large primes chosen by the signer such that 3 is relatively prime to $\varphi(n) = (p-1)(q-1)$ and let y be a random value in $\mathbb{Z}_n^*$. The pair (n, y) is the signer's public key. Let further $\mathcal{H}$ denote a one-way hash function and k be a security parameter (e.g. $k > 80$). In contrast to the original Fiat-Shamir signature scheme, this scheme uses third roots instead of square roots. Let us define the sequences

$$y_i = \mathcal{H}(y + i) \pmod{n} \ , \quad x_i = y_i^{1/3} \pmod{n} \ , \quad i = 1 \ldots k$$

Note that only the signer, knowing the factorization of n, can compute the sequence x_i. To sign a message m the signer proceeds as follows:

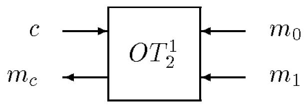
- randomly choose $r \in \mathbb{Z}_n^*$, compute $t = r^3 \pmod{n}$
- compute $c = \mathcal{H}(t||m)$, let c_i denote the i-th bit of c
- compute $s = r \prod_{i=1}^{k} x_i^{c_i} \pmod{n}$
- (s, t) is the signature of the message m and can be verified by checking

$$s^3 \stackrel{?}{=} t \prod_{i=1}^{k} y_i^{c_i} \pmod{n} \ .$$

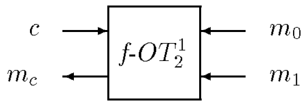
4.2 Fair one-out-of-two Oblivious Transfer

One-out-of-two oblivious transfer (OT_2^1, see [10]) is a protocol between a sender and a receiver which allows the receiver to choose one of two messages sent by the sender in a way such that he receives only the chosen message and the sender does not know which message he has chosen (note that we allow the receiver to choose the message in contrast to the original concept introduced in [10]).

Let m_0 and m_1 denote the two messages sent by the sender and let c be the selection bit of the receiver. An execution of an OT_2^1 protocol is then denoted by



Let us now consider a modified implementation which allows a judge, but not the sender, to determine the selection bit. Let us denote an execution of such a "fair"-OT_2^1 by



A fair one-out-of-two oblivious transfer could be realized as follows: Let $n_J = p_J q_J$ be the product of two large primes so that the factorization of n_J is known to the judge only. Let further $g \in QR_{n_J}$ have a large order, and let h be a quadratic non-residue in $\mathbb{Z}_{n_J}^*$ with positive Jacobi symbol. The functions "encr" and "decr" are simple encryption and decryption functions (e.g. DES) used to transfer the messages of the sender.

Receiver		**Sender**
randomly choose $r \in \mathbb{Z}_{n_J}$ $t = g^r h^c \pmod{n_J}$	$\xrightarrow{\quad t \quad}$	
		randomly choose $\alpha \in \mathbb{Z}_{n_J}$ $A = g^\alpha \pmod{n_J}$ $k_0 = t^\alpha \pmod{n_J}$ $k_1 = (th^{-1})^\alpha \pmod{n_J}$ $y_0 = \mathrm{encr}(m_0, k_0)$ $y_1 = \mathrm{encr}(m_1, k_1)$
	$\xleftarrow{\quad A,\ y_0,\ y_1 \quad}$	
$k_c = A^r \pmod{n_J}$ $m_c = \mathrm{decr}(y_c, k_c)$		

Because of the quadratic residuosity assumption the sender cannot find out whether the receiver got m_0 or m_1. But the judge can easily compute the selection bit c by checking whether t is a quadratic residue in $\mathbb{Z}_{n_J}^*$ or not. On the other hand, the receiver cannot compute m_{1-c} because he cannot compute k_{1-c} due to the Diffie–Hellman assumption.

4.3 Fair Blind Fiat-Shamir Signatures

With *fair-*OT_2^1 we can now convert the signature scheme from Section 4.1 into a fair blind signature scheme of type I.

Sender		**Signer**
		choose $r_1, \ldots, r_k \in \mathbb{Z}_n^*$ $t = \prod_{i=1}^{k} r_i^3 \pmod n$
	$\xleftarrow{\quad t \quad}$	
randomly choose $\alpha \in \mathbb{Z}_n^*$, $\tilde{t} = t\alpha^3 \pmod n$ $c = \mathcal{H}(\tilde{t}\|\|m)$, c_i is the i-th bit of c for $i = 1 \ldots k$ do		
$c_i \longrightarrow$	$\boxed{f\text{-}OT_2^1}$	$\longleftarrow m_0 = r_i$
$s_i = m_{c_i} \longleftarrow$		$\longleftarrow m_1 = r_i x_i$
od $\tilde{s} = \alpha \prod_{i=1}^{k} s_i \pmod n$		

Then the pair $(\tilde{s}, \tilde{t})$ is a valid signature of m (c_i is the i-th bit of $\mathcal{H}(\tilde{t}||m)$):

$$\tilde{s}^3 = \tilde{t} \cdot \prod_{i=1}^{k} y_i^{c_i} \pmod n$$

Let us analyze the blindness of this scheme. We assume that the signer cannot determine the selection bits c_i (because of the *fair-*OT_2^1). So t is the only value the signer could use to recognize the signature later. But for each valid signature $(\hat{s}, \hat{t})$ of a message $\hat{m}$ there is exactly one α with $\hat{t} = t\alpha^3 \pmod n$ and therefore $\hat{s} = \alpha \prod_{i=1}^{k} r_i x_i^{\hat{c}_i} \pmod n$, where $\hat{c}_i$ is the i-th bit of $\mathcal{H}(\hat{t}||\hat{m})$. 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 bits 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 recognize that message-signature pair later.

5 Fair Blind Signatures with Registration

Our last proposal is again of type I and II, simultaneously. The main idea is that the sender has two pseudonyms registered at the judge. One of the pseudonyms is used during the signing protocol, whereas the other one is part of the signature. Thus the judge, who knows the two corresponding pseudonyms, can link a view of the signing protocol and the corresponding signature.

If the sender uses the same pseudonyms twice, then the signer can link the two corresponding views of the signing protocol, and everyone can easily link the two resulting signatures. So, if different messages are to be unlinkable, the sender has to be registered at the judge for each single message to be signed. This scheme is therefore not suited if perfect anonymity is required, i.e. if different message-signature pairs of the same sender are to be unlinkable.

The system parameters are as follows:

- a group G of prime order q, for which it is hard to compute discrete logarithms, and a publicly known element $g \in G$.
- $y = g^x$, the signer's public key (where x is his secret key).
- $\mathrm{Sig}_J(\cdot)$, the judge's signature scheme, so that everybody can verify messages signed by the judge.
- $\mathcal{H}$, a one-way hash function.

The scheme consists of two protocols, one for registration at the judge, and one for blind signature generation.

The registration protocol

Sender		**Judge**
	$\xrightarrow{\text{request}}$	
		randomly choose $A \in G$, $\alpha \in \mathbb{Z}_q$
		$\tilde{A} = A^\alpha$
		store $(A, \tilde{A})$
	$\xleftarrow{A,\ \mathrm{Sig}_J(A\|\|0)}$	
	$\xleftarrow{\alpha,\ \mathrm{Sig}_J(\tilde{A}\|\|1)}$	
$\tilde{A} = A^\alpha$		

The bit appended to the pseudonyms A and $\tilde{A}$ in the signature of the judge prevents a dishonest sender to permute the two pseudonyms.

The signature generation protocol

Sender		**Signer**
	$\xrightarrow{A,\ \mathrm{Sig}_J(A\|\|0)}$	
		verifies $\mathrm{Sig}_J(A\|\|0)$
		$z = A^x$
	$\xleftarrow{z}$	
$\tilde{z} = z^\alpha$		
		randomly choose $r \in \mathbb{Z}_q$
		$t_1 = g^r,\ t_2 = A^r$
	$\xleftarrow{t_1,\ t_2}$	
randomly choose $\beta, \gamma \in \mathbb{Z}_q$		
$\tilde{t}_1 = t_1^\beta g^\gamma$		
$\tilde{t}_2 = t_2^{\alpha\beta} \tilde{A}^\gamma$		
$\tilde{c} = \mathcal{H}(m\|\|\tilde{A}\|\|\tilde{z}\|\|\tilde{t}_1\|\|\tilde{t}_2) \pmod q$	$\xrightarrow{c = \tilde{c}/\beta \pmod q}$	
		$s = r + cx \pmod q$
	$\xleftarrow{s}$	
$\tilde{s} = \beta s + \gamma \pmod q$		

The resulting signature is the 6-tuple

$$(\tilde{A}, \mathrm{Sig}_J(\tilde{A}||1), \tilde{z}, \tilde{t}_1, \tilde{t}_2, \tilde{s})$$

It can be verified by first verifying $\mathrm{Sig}_J(\tilde{A}||1)$ and then by checking whether

$$g^{\tilde{s}} \stackrel{?}{=} \tilde{t}_1 y^{\tilde{c}}, \quad \text{and} \quad \tilde{A}^{\tilde{s}} \stackrel{?}{=} \tilde{t}_2 \tilde{z}^{\tilde{c}}$$

with $\tilde{c} = \mathcal{H}(m||\tilde{A}||\tilde{z}||\tilde{t}_1||\tilde{t}_2) \pmod q$.

This scheme can be viewed as a modification of the Chaum-Pedersen blind signature scheme [9], with the pair $(\tilde{A}, m)$ playing here a role similar to the message in [9]. Therefore, the security of our scheme is strongly related to the security of the Chaum-Pedersen blind signature scheme. Furthermore, the blindness property is easy to verify: as in [9], for any signature $(\tilde{A}, \mathrm{Sig}_J(\tilde{A}||1), \tilde{z}, \tilde{t}_1, \tilde{t}_2, \tilde{s})$ and for any signer's view, there exist α, β, γ such that the signer's view leads to that signature.

6 Conclusions

We have introduced the concept of fair blind signatures, and presented possible realizations. When applied to the design of payment systems protecting privacy, fair blind signatures allow to meet the requirements of all parties: on one hand the customers, who like to have as much privacy protection as possible, on the other hand the authorities (the bank and the judge in our model), who like to prevent criminals from misusing this privacy protection. In the usual case (which means that the judge is not involved in a transaction), the anonymity of the customer's payment is guaranteed. However, in particular situations (e.g. for legal reasons) it is possible to remove this anonymity with the help of the judge.

Fair blind signature offer a satisfactory solution against abuses of the system, like money laundering or blackmailing of customers (as it is the case for a "perfect crime" in the sense of [16]). A solution to the general blackmailing attack seems to be an open problem.

Another subject of investigation is the development of more efficient fair blind signature schemes.

Acknowledgement

We would like to thank U. Maurer and H.P. Frei for their valuable support.

References

1. S. Brands: Untraceable Off-line Cash in Wallets with Observers, *Proceedings of Crypto '93*, LNCS 773, Springer Verlag, pp. 302-318.
2. J. Camenisch, J.-M. Piveteau, M. Stadler: Blind Signatures Based on the Discrete Logarithm Problem, to appear in the proceedings of Eurocrypt '94.
3. J. Camenisch, J.-M. Piveteau, M. Stadler: An Efficient Payment System Protecting Privacy, *Proceedings of ESORICS '94*, Lecture Notes in Computer Science 875, Springer Verlag, pp. 207-215.
4. D. Chaum: Blind Signature Systems, *Proceedings of Crypto '83*, Plenum, p. 153.
5. D. Chaum, E. van Heyst: Group Signatures, *Proceedings of Eurocrypt '91*, Lecture Notes in Computer Science 547, Springer Verlag, pp. 257-265.
6. D. Chaum, A. Fiat, M. Naor: Untraceable Electronic Cash, *Proceedings of Crypto '88*, LNCS 403, Springer Verlag, pp. 319-327.
7. D. Chaum: Privacy Protected Payment, SMART CARD 2000, Elsevier Science Publishers B.V. (North-Holland), 1989, pp. 69-93.
8. D. Chaum, B. den Boer, E.van Heyst, S. Mjølsnes, A. Steenbeek: Efficient Offline Electronic Checks, *Proceedings of Eurocrypt '89*, LNCS 434, Springer Verlag, pp. 294-301.
9. D. Chaum, T. Pedersen: Wallet databases with observers, *Proceedings of Crypto '92*, LNCS 740, Springer Verlag, pp. 89-105.
10. S. Even, O. Goldreich, A. Lempel: A Randomized Protocol for Signing Contracts, *Communications of the ACM*, **28**, 1985, pp. 637-647.
11. N. Ferguson: Single Term Off-line Coins, *Proceedings of Eurocrypt '93*, LNCS 765, Springer Verlag, pp. 318-328.
12. A. Fiat, A. Shamir: How to prove yourself: Practical solutions to identification and signature problems, *Proceedings of Crypto '86*, LNCS 263 , Springer Verlag, pp. 186-194.
13. S. Micali: Fair Cryptosystems, Technical Report MIT/LCS/TR-579.b, 1993.

14. T. Okamoto, K. Ohta: Universal Electronic Cash, *Proceedings of Crypto '91*, LNCS 576, Springer Verlag, pp. 324-337.
15. R.L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public Key Cryptosystems, *Communications of the ACM*, **21**, 1978, pp. 120-126.
16. S. von Solms, D. Naccache: On Blind Signatures and Perfect Crime, *Computer & Security*, **11**, 1992, pp. 581-583.