A Provably Secure Restrictive Partially Blind Signature Scheme

Greg Maitland and Colin Boyd

Information Security Research Centre
Queensland University of Technology
Brisbane, Australia.
{g.maitland,c.boyd}@qut.edu.au

Abstract. The concept of partially blind signatures was first introduced by Abe and Fujisaki. Subsequently, in work by Abe and Okamoto, a provably secure construction was proposed along with a formalised definition for partially blind schemes. The construction was based on a witness indistinguishable protocol described by Cramer et al. and utilises a blind Schnorr signature scheme.
This paper investigates incorporating the restrictive property proposed by Brands into a partially blind signature scheme. The proposed scheme follows the construction proposed by Abe and Okamoto and makes use of Brands' restrictive blind signature scheme.

1 Introduction

Blind signature schemes were first introduced by Chaum [9] and allow a recipient to acquire a signature on a message m without revealing anything about the message to the signer. One of the first applications for blind signatures was in the area of electronic cash. However, the complete lack of control over the message being signed makes tasks such as including expiry information in the blind signature difficult. The signer cannot rely on the recipient to include any specific information in the blindly signed message. The typical solution to this difficulty has been to associate different signing keys with different classes of messages. This is undesirable as it leads to a proliferation of signing keys and a potential verifier must have access to all possible active certified keys.

In the context of electronic cash schemes based around the use of blind signatures, the specific problems arise because of the need to expire coins as well as the need to clearly nominate the denominational value of each coin. Practical schemes must allow exact payments and therefore usually accommodate coins of varying denominations. In addition, blindly issued coins require the bank to maintain a database of previously spent coins in order to detect double-spending. Without any extra measures, the size of the database would increase indefinitely over time and this would reduce the cost-effective and efficient operation of the database. In order to contain the size of the database, 'old' spent coins need to be removed after an appropriate amount of time. Thus, a coin must have an expiry date after which it is no longer acceptable in a payment transaction.

D. Naccache and P. Paillier (Eds.): PKC 2002, LNCS 2274, pp. 99–114, 2002.

A partially blind signature scheme allows a signer to produce a blind signature on a message for a recipient and the signature explicitly includes common agreed information which remains clearly visible despite the blinding process. Abe and Fujisaki [2] first introduced the concept in response to the need for the signer to regain some control over the signatures produced by a blind signature scheme. When used in electronic cash scheme design, the common agreed information allows expiry date and denominational information to be included in the blind signature while requiring that the verifier has access to only a single certified public key.

Early papers on the construction of partially blind signatures [1,13] based around Schnorr, DSS and Nyberg-Rueppel schemes concentrated on withstanding parallel algebraic attacks [**?**]. More recently, Abe and Okamoto [3] described a provably secure partially blind signature based on a witness indistinguishable protocol using blinded Schnorr signatures [15] as a building block.

However, the previously published partially blind signatures lack the restrictive property. Restrictive blind signature schemes were proposed by Brands [5] and allow a recipient to receive a blind signature on a message not known to the signer but the choice of message is restricted and must conform to certain rules. In practical applications such as Brands' cash [5,6], the signer is assured that the recipient's identity is embedded in some sense in the resulting blind signature.

While Brands' cash has received wide attention for its ability to detect and reveal the identity of double-spenders, it also possesses another property – transfer-resistance. That is, the spender of a coin must have access to the private key of the customer who withdrew the coin in order to spend it. This discourages the transfer of coins from one user to another as the withdrawing user must reveal private key information if another user is to spend the coin. Transfer-resistance is a useful tool in discouraging illegal activities such as money laundering and blackmail.

Main Contribution: Since Brands' cash remains an important building block in several cash schemes [7,4,14], it is relevant to consider ways of incorporating the property of partial blindness into Brands' restrictive blind signature scheme. Pointcheval [16] and Abe-Okamoto [3] have constructed security arguments for blind signatures based on witness indistinguishable protocols. Using the techniques proposed by Abe and Okamoto [3], we utilise a witness indistinguishable protocol to create a restrictive partially blind signature scheme with provable security. In the process, we introduce a multiplicative variant of the blind Schnorr signature, which to the authors' knowledge has not previously been published. We also utilise multiplicative (rather than additive) secret sharing in the construction of the witness indistinguishable protocol.

Organisation of the Paper: Section 2 describes the basic definitions associated with partially blind signatures while section 3 reviews both Schnorr [17] and Chaum-Pedersen [8] protocols in connection with the Cramer et al. construction for witness indistinguishable protocols. Section 4 discusses blinding operations

for both the Schnorr and Chaum-Pedersen protocols. A restrictive partially blind signature is presented in section 5 and its security is discussed in section 6.

2 Definitions

We follow the definitions provided by Abe and Okamoto [3] which have been adapted for partially blind signatures from the security definitions of Juels, Luby, and Ostrovsky [12].

In the context of partially blind signatures, the signer and the user are assumed to agree on a piece of common information, denoted by info. It may happen that info is decided by the signer; in other situations, info may just be sent from the user to the signer. This negotiation is considered to be done outside of the signature scheme. Abe and Okamoto [3] formalize this notion by introducing a function Ag which is defined outside of the scheme. Function Ag is a polynomial-time deterministic algorithm that takes two arbitrary strings info_s, and info_u, that belong to the signer and the user, respectively, and outputs info. To compute Ag, the signer and the user will exchange info_s and info_u with each other. If the signer is allowed to control the selection of info, then Ag is defined such that it depends only on info_s. In this case, the user does not need to send info_u.

Definition 1 (Partially Blind Signature Scheme). *A partially blind signature scheme is a four-tuple* $(\mathcal{G}, \mathcal{S}, \mathcal{U}, \mathcal{V})$.

- $\mathcal{G}$ *is a probabilistic polynomial-time algorithm, that takes security parameter* k *and outputs a public and secret key pair* (pk, sk).
- $\mathcal{S}$ *and* $\mathcal{U}$ *are a pair of probabilistic interactive Turing machines each of which has a public input tape, a private input tape, a private random tape, a private work tape, a private output tape, a public output tape, and input and output communication tapes. The random tape and the input tapes are read-only, and the output tapes are write-only. The private work tape is read-write. The public input tape of* $\mathcal{U}$ *contains* pk *generated by* $\mathcal{G}(1^k)$*, the description of* Ag*, and* info_u*. The public input tape of* $\mathcal{S}$ *contains the description of* Ag *and* info_s*. The private input tape of* $\mathcal{S}$ *contains* sk*, and that for* $\mathcal{U}$ *contains a message* msg*. The lengths of* info_s*,* info_u*, and* msg *are polynomial in* k*.* $\mathcal{S}$ *and* $\mathcal{U}$ *engage in the signature issuing protocol and stop in polynomial-time. When they stop, the public output tape of* $\mathcal{S}$ *contains either completed or not-completed. If it is completed, then its private output tape contains common information* info*. Similarly, the private output tape of* $\mathcal{U}$ *contains either* $\perp$ *or* $(\mathsf{info}, msg, sig)$.
- $\mathcal{V}$ *is a (probabilistic) polynomial-time algorithm.* $\mathcal{V}$ *takes* $(pk, \mathsf{info}, msg, sig)$ *and outputs either accept or reject.*

Definition 2 (Completeness). *If* $\mathcal{S}$ *and* $\mathcal{U}$ *follow the signature issuing protocol, the signature scheme is complete if, for every constant* $c > 0$*, there exists a*

bound k_0 such that $\mathcal{S}$ outputs completed and $\mathsf{info} = Ag(\mathsf{info}_s, \mathsf{info}_u)$ *on its proper tapes, and $\mathcal{U}$ outputs* $(\mathsf{info}, msg, sig)$ *that satisfies*

$$\mathcal{V}(pk, \mathsf{info}, msg, sig) = accept$$

with probability at least $1 - 1/k^c$ for $k > k_0$. The probability is taken over the coin flips of $\mathcal{G}$, $\mathcal{S}$ and $\mathcal{U}$.

A message-signature tuple $(\mathsf{info}, msg, sig)$ is considered valid with regard to pk if it leads $\mathcal{V}$ to accept. We define the partial blindness property as follows.

Definition 3 (Partial Blindness). *Let $\mathcal{U}_0$ and $\mathcal{U}_1$ be two honest users that follow the signature issuing protocol. Let $\mathcal{S}^*$ play the following game in the presence of an independent umpire.*

1. $(pk, sk) \leftarrow \mathcal{G}(1^k)$.
2. $(msg_0, msg_1, \mathsf{info}_{u_0}, \mathsf{info}_{u_1}, Ag) \leftarrow \mathcal{S}^*(1^k, pk, sk)$.
3. *The umpire sets up the input tapes of $\mathcal{U}_0$, $\mathcal{U}_1$ as follows:*
   - *The umpire selects $b \in_R \{0, 1\}$ and places msg_b and msg_{1-b} on the private input tapes of $\mathcal{U}_0$ and $\mathcal{U}_1$, respectively. b is not disclosed to $\mathcal{S}^*$.*
   - *Place info_{u_0} and info_{u_1} on the public input tapes of $\mathcal{U}_0$ and $\mathcal{U}_1$ respectively. Also place pk and Ag on their public input tapes.*
   - *Randomly select the contents of the private random tapes.*
4. *$\mathcal{S}^*$ engages in the signature issuing protocol with $\mathcal{U}_0$ and $\mathcal{U}_1$ in a parallel and arbitrarily interleaved fashion. If either signature issuing protocol fails to complete, the game is aborted.*
5. *Let $\mathcal{U}_0$ and $\mathcal{U}_1$ output $(\mathsf{info}_0, msg_b, sig_b)$ and $(\mathsf{info}_1, msg_{1-b}, sig_{1-b})$, respectively, on their private tapes. If $\mathsf{info}_0 \neq \mathsf{info}_1$ holds, then the umpire provides $\mathcal{S}^*$ with the no additional information. That is, the umpire gives $\perp$ to $\mathcal{S}^*$. If $\mathsf{info}_0 = \mathsf{info}_1$ holds, then the umpire provides $\mathcal{S}^*$ with the additional inputs $\{sig_b, sig_{1-b}\}$ ordered according to the corresponding messages $\{msg_0, msg_1\}$.*
6. *$\mathcal{S}^*$ outputs $b' \in \{0, 1\}$. The signer $\mathcal{S}^*$ wins the game if $b' = b$.*

A signature scheme is partially blind if, for every constant $c > 0$, there exists a bound k_0 such that for all probabilistic polynomial-time algorithm $\mathcal{S}^*$, $\mathcal{S}^*$ outputs $b' = b$ with probability at most $1/2 + 1/k^c$ for $k > k_0$. The probability is taken over the coin flips of $\mathcal{G}$, $\mathcal{U}_0$, $\mathcal{U}_1$, and $\mathcal{S}^*$.

Definition 4 (Unforgeability). *Let $\mathcal{S}$ be an honest signer that follow the signature issuing protocol. Let $\mathcal{U}^*$ play the following game in the presence of an independent umpire.*

1. $(pk, sk) \leftarrow \mathcal{G}(1^n)$.
2. $Ag \leftarrow \mathcal{U}^*(pk)$.
3. *The umpire places sk, Ag and a randomly taken info_s on the proper input tapes of $\mathcal{S}$.*

4. *$\mathcal{U}^*$ engages in the signature issuing protocol with $\mathcal{S}$ in a concurrent and interleaving way. For each* info*, let ℓ_{info} be the number of executions of the signature issuing protocol where $\mathcal{S}$ outputs completed and* info *is on its output tapes. (For* info *that has never appeared on the private output tape of $\mathcal{S}$, define $\ell_{\mathsf{info}} = 0$.)*
5. *$\mathcal{U}^*$ outputs a single piece of common information,* info*, and $\ell_{\mathsf{info}}+1$ signatures $(msg_1, sig_1), \ldots, (msg_{\ell_{\mathsf{info}}+1}, sig_{\ell_{\mathsf{info}}+1})$.*

A partially blind signature scheme is unforgeable if, for any probabilistic polynomial-time algorithm $\mathcal{U}^*$ that plays the above game, the probability that the output of $\mathcal{U}^*$ satisfies

$$\mathcal{V}(pk, \mathsf{info}, msg_j, sig_j) = accept$$

for all $j = 1, \ldots, \ell_{\mathsf{info}} + 1$ is at most $1/k^c$ where $k > k_0$ for some bound k_0 and some constant $c > 0$. The probability is taken over the coin flips of $\mathcal{G}$, $\mathcal{S}$, and $\mathcal{U}^*$.

The following definition of a restrictive blind signature is due to Brands [6].

Definition 5 (Restrictiveness). *Let msg be message such that the receiver-knows a representation $(a_1, \ldots, a_k)$ of msg with respect to a generator-tuple $(g_1, \ldots, g_k)$ at the start of a blind signature protocol. Let $(b_1, \ldots, b_k)$ be the representation the receiver knows of the blinded number msg' of msg after the protocol has finished. If there exist two functions I_1 and I_2 such that*

$$I_1(a, \ldots, a_k) = I_2(b_1, \ldots, b_k),$$

regardless of msg and the blinding transformations applied by the receiver, then the protocol is called a restrictive blind signature protocol. The functions I_1 and I_2 are called blinding-invariant functions of the protocol with respect to $(g_1, \ldots, g_k)$.

3 Witness Indistinguishable Protocols

The Okamoto-Schnorr identification protocol is a well known example of a witness indistinguishable protocol. Informally, a proof of knowledge is witness indistinguishable if the verifier cannot tell which witness the prover is using even if the verifier knows all possible witnesses [11]. Pointcheval [16] has presented security arguments for the blind Okamoto-Schnorr signature scheme. The witness indistinguishable property is necessary in order to prove security. Abe-Okamoto [3] have constructed security arguments for a partially blind signature scheme based on a witness indistinguishable protocol. We also seek to use a witness indistinguishable protocol as the basis for a provably secure scheme.

Cramer, Damgård, and Schoenmakers [10] presented a method for constructing witness indistinguishable protocols by combining suitable three-move proofs of knowledge with a compliant secret sharing scheme. In particular, the proofs of knowledge must possess the *special soundness* and *special honest verifier zero-knowledge* properties. A proof of knowledge has special soundness if, given two

transcripts of the protocol which share a common commitment, a witness can be computed in polynomial time. A protocol is *honest verifier zero-knowledge* if there is a simulator which produces conversations that are indistinguishable from real conversations between the honest prover and the honest verifier. *Special honest verifier zero-knowledge* requires that there is a procedure that can take any challenge as input and produce a conversation indistinguishable from the space of all conversations between the honest prover and honest verifier that involve this challenge.

As an example of the construction, Cramer, Damgård, and Schoenmakers [10] presented a proof of knowledge of d out of n secrets using Schnorr's protocol as the basic proof of knowledge and a 'matrix' method for the secret sharing scheme. It is this scheme (with $d = 1$ and $n = 2$) that Abe and Okamoto [3] use to construct a provably secure partially blind signature scheme. Note that the secret sharing scheme is reduced to a simple additive scheme where both shares sum to give the secret.

While Cramer, Damgård, and Schoenmakers [10] concentrate on a construction which utilises several instances of the same proof of knowledge, they note that it is also possible to combine instances of different proofs of knowledge. In this paper, we will combine a Schnorr proof of knowledge of a discrete log [17] with a Chaum-Pedersen proof of equivalence of discrete logs [8]. With this in mind, we now review both the Schnorr and Chaum-Pedersen schemes with particular focus on the special soundness and special honest verifier zero-knowledge properties.

3.1 Schnorr's Proof of Knowledge of a Discrete Log

Let two primes p and q be given such that q divides $p - 1$ and let $g \in \mathbb{Z}_p^*$ be an element of order q. The group generated by g is denoted by G_q. The private key is $x \in \mathbb{Z}_q^*$ and the public key is (p, q, g, y) where $y = g^x$. The underlying identification protocol is as follows:

- The prover chooses $r \in_R \mathbb{Z}_q$ at random and computes $a = g^r$. The commitment value, a, is sent to the verifier.
- The verifier chooses a random challenge $c \in_R \mathbb{Z}_q$ and sends it to the prover.
- The prover sends back the response $s = r + cx \mod q$.
- The verifier accepts the proof if and only if $a = g^s y^{-c}$.

Special Soundness: Let (c, s) and (c', s') be two signatures that are derived from the same commitment a. Then, the witness x can be found by observing that

$$a = g^s y^{-c} = g^{s'} y^{-c'} \text{ which implies that}$$
$$y = g^{\frac{s-s'}{c-c'}} = g^x \text{ and so}$$
$$x = \frac{s - s'}{c - c'} \mod q.$$

Special Honest Verifier Zero-knowledge: A simulator can generate transcripts of the Schnorr protocol as follows:

- Select $c', s' \in_R \mathbb{Z}_q^*$
- Calculate $a' = g^{s'} y^{-c'}$

The transcript (a', c', s') satisfies $a' = g^{s'} y^{-c'}$ by construction and is statistically indistinguishable from actual protocol transcripts.

3.2 Chaum-Pedersen Signature

We review the Chaum-Pedersen [8] protocol and properties. Let two primes p and q be given such that q divides $p-1$ and let $g \in \mathbb{Z}_p^*$ be an element of order q. The group generated by g is denoted by G_q. The private key is $x \in \mathbb{Z}_q^*$ and the public key is (p, q, g, y) where $y = g^x$. The underlying identification protocol (utilising a message m) is as follows:

- The prover chooses $r \in_R \mathbb{Z}_q$ at random and computes $(z, a, b) = (m^x, g^r, m^r)$. The tuple (z, a, b) is sent to the verifier.
- The verifier chooses a random challenge $c \in_R \mathbb{Z}_q$ and sends it to the prover.
- The prover sends back the response $s = r + cx \mod q$.
- The verifier accepts the proof if and only if $a = g^s y^{-c}$ and $b = m^s z^{-c}$.

Special Soundness: Let (z, c, s) and (z, c', s') be two signatures that are derived from the same commitment a. Then, the witness x can be found by observing that

$$
\begin{aligned}
&a = g^s y^{-c} = g^{s'} y^{-c'} \text{ which implies that} \\
&y = g^{\frac{s-s'}{c-c'}} = g^x \text{ and so} \\
&x = \frac{s-s'}{c-c'} \mod q
\end{aligned}
$$

Special Honest Verifier Zero-knowledge: A simulator can generate transcripts of the Chaum-Pedersen protocol involving a message m as follows:

- Select $z', c', s' \in_R \mathbb{Z}_q^*$
- Calculate $a' = g^{s'} y^{-c'}$
- Calculate $b' = (m)^{s'} (z')^{-c'}$

The transcript (z', a', b', c', s') satisfies $a' = g^{s'} y^{-c'}$ and $b' = (m)^{s'} (z')^{-c'}$ by construction and is statistically indistinguishable from actual protocol transcripts.

4 Blinding Techniques

In this section, we review the blinding techniques which may be applied to the Schnorr [17] and Chaum-Pedersen [8] protocols. As detailed below, the standard blinding of the challenge for the Chaum-Pedersen protocol is multiplicative in nature. The usual blind Schnorr protocol [15] uses an additive blinding of the challenge. Since our aim is to combine these two types of proof of knowledge to form a witness indistinguishable protocol which we can subsequently blind, we need blinding operations which are consistently either additive or multiplicative. To this end, the blinding of the Schnorr protocol outlined below uses a multiplicative (rather than the more usual additive) blinding of the challenge.

4.1 Brands' Restrictive Blind Signature

The restrictive blind signature scheme described in this section is derived from the Chaum-Pedersen scheme [8] described in section 3.2 and is Brands' original restrictive blind signature scheme [5,6].

Let g be a generator of a cyclic group G of order q. Let $y = g^x$ be the public key of the signer, and m 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 Chaum-Pedersen protocol can be diverted to form a restrictive blind signature in the following fashion.

- The signer generates a random number $r \in_R \mathbb{Z}_q$, and sends $z = m^x$, $a = g^r$ and $b = m^r$ to the receiver.
- The receiver generates at random numbers $\alpha, \beta \in_R \mathbb{Z}_q$ and computes

$$m' = m^\alpha g^\beta \text{ and}$$
$$z' = z^\alpha y^\beta.$$

  The receiver also chooses $u, v \in_R \mathbb{Z}_q$ and computes a' and b' as follows:

$$a' = a^u g^v \text{ and}$$
$$b' = a^{u\beta} b^{u\alpha} (m')^v$$

  The receiver then computes $c' = \mathcal{H}(m' \parallel z' \parallel a' \parallel b')$ 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

$$c' = \mathcal{H}\left(m' \parallel z' \parallel g^{s'} y^{-c'} \parallel (m')^{s'} (z')^{-c'}\right).$$

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.

Correctness

$$\begin{aligned}
g^{s'}y^{-c'} &= g^{us+v}y^{-cu} = (g^s y^{-c})^u g^v = a^u g^v = a' \\
(m')^{s'}(z')^{-c'} &= (m')^{us+v}(z')^{-cu} = (m')^v (m')^{us}(z')^{-cu} \\
&= (m')^v ((m')^s (z')^{-c})^u \\
&= (m')^v ((m^\alpha g^\beta)^s (z^\alpha y^\beta)^{-c})^u \\
&= (m')^v ((m^{s\alpha} g^{s\beta})(m^{-c\alpha} y^{-c\beta}))^u \\
&= (m')^v ((m^{s\alpha} z^{-c\alpha})(g^{s\beta} y^{-c\beta}))^u \\
&= (m')^v ((m^s z^{-c})^\alpha (g^s y^{-c})^\beta)^u \\
&= (m')^v (b^\alpha a^\beta)^u \\
&= a^{u\beta} b^{u\alpha} (m')^v \\
&= b'
\end{aligned}$$

Blindness: Let (m, r, z, a, b, c, s) be *any* of the views of the protocol as seen by the signer. Therefore, $a = g^s y^{-c}$, $b = m^s z^{-c}$ and $s = r + cx$. Let (z', c', s') be a valid signature on a message m' obtained by the receiver. Choose the unique blinding factors

$$\begin{aligned}
u &= c'/c \mod q \\
v &= s' - us \mod q
\end{aligned}$$

and determine a representation $m' = m^\alpha g^\beta$. (While finding a representation is difficult, we only need to exploit the existence of such representations. In fact, there are q representations of m'.) Note that the fact that $z = m^x$ and $z' = m'^x$ has been established by the interactive proof provided by the signer during blind signature formation and the fact that the blind signature is valid. Therefore, $z' = (m')^x = (m^\alpha g^\beta)^x = z^\alpha y^\beta$.

By setting $a' = a^u g^v$ and $b' = a^{u\beta} b^{u\alpha} (m')^v$, we find that

$$\begin{aligned}
g^{s'}y^{-c'} &= g^{v+su}y^{-cu} = g^v (g^s y^{-c})^u = g^v a^u = a' \\
(m')^{s'}(z')^{-c'} &= (m')^{v+su}(z')^{-cu} = (m')^v ((m')^s (z')^{-c})^u \\
&= (m')^v \Big((m^\alpha g^\beta)^s (z^\alpha y^\beta)^{-c} \Big)^u \\
&= (m')^v \Big((m^s z^{-c})^\alpha (g^s y^{-c})^\beta \Big)^u \\
&= (m')^v \big(b^\alpha a^\beta \big)^u \\
&= (m')^v b^{u\alpha} a^{u\beta} \\
&= b'
\end{aligned}$$

Hence, there exist blinding factors that could have been used to transform any view into the particular signature (z', c', s') on m'. Therefore, the signer's view is statistically independent of the receiver's signature (z', c', s') on m'.

Restrictiveness: The restrictive nature of the protocol is captured by the following assumption.

Assumption 1 (Restrictiveness). *The recipient obtains a signature on a message that can only be of the form $m' = m^{\alpha}g^{\beta}$ with α and β randomly chosen by the recipient. In addition, in the particular case where $\beta = 0$, if there exists a representation (μ_1, μ_2) of m with respect to bases g_1 and g_2 such that $m = g_1^{\mu_1} g_2^{\mu_2}$ and if there exists a representation (μ_1', μ_2') of m' with respect to bases g_1 and g_2 such that $m' = g_1^{\mu_1'} g_2^{\mu_2'}$, then the relation $I_1(\mu_1, \mu_2) = \mu_1/\mu_2 = \mu_1'/\mu_2' = I_2(\mu_1', \mu_2')$ holds.*

4.2 Schnorr Blind Signature Scheme – Multiplicative Variant

As discussed previously, we seek a blind variant of the Schnorr [17] protocol which uses multiplicative (rather than the standard additive operation) to blind the challenge. This can be accomplished with the following protocol.

- The signer generates a random number $r \in_R \mathbb{Z}_q$, and sends $a = g^r$ to the receiver.
- The receiver chooses blinding factors $u, v \in_R \mathbb{Z}_q$ and computes a' as follows:

  $$a' = a^u g^v$$

  The receiver then computes $c' = \mathcal{H}(m \parallel a')$ 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 $a = g^s y^{-c}$.
- If the receiver accepts, compute $s' = us + v \mod q$.

(c', s') is a valid signature on m satisfying $c' = \mathcal{H}\left(m \parallel g^{s'} y^{-c'}\right)$.

Correctness

$$g^{s'} y^{-c'} = g^{us+v} y^{-cu} = (g^s y^{-c})^u g^v = a^u g^v = a'$$

Blindness: Let (r, a, c, s) be *any* of the views of the protocol as seen by the signer. Therefore, $a = g^s y^c$ and $s = r + cx$. Let (c', s') be a valid signature on a message m obtained by the receiver. By choosing blinding factors

$$\begin{aligned} u &= c'/c \\ v &= s' - su (= s' - sc'/c = \frac{cs' - c's}{c}) \\ a' &= a^u g^v \end{aligned}$$

we find that

$$g^{s'} y^{c'} = g^{v+su} y^{cu} = g^v (g^s y^c)^u = a^u g^v = a'.$$

Hence, there exist blinding factors that could have been used to transform any view into the particular signature (c', s') on m. Therefore, the signer's view is statistically independent of the receiver's signature (c', s') on m.

5 A Restrictive Partially Blind Signature Scheme

The construction of Cramer et al. [10] for proving knowledge of d out of n secrets uses a homogeneous collection of proofs of knowledge. However, Cramer et al. [10] note that it is possible to combine different proofs of knowledge. We mix Schnorr [17] and Chaum-Pedersen [8] proofs of knowledge in the particular case when $d = 1$ and $n = 2$. That is, the prover demonstrates knowledge of either the private key related to a Schnorr public key or knowledge of the private key related to a Chaum-Pedersen public key. As discussed in section 3, the Schnorr and Chaum-Pedersen proofs of knowledge met the requirements (special soundness and special honest verifier zero-knowledge) for the construction of a witness indistinguishable protocol as described by Cramer et al. [10].

The protocol is converted into a blind signature issuing protocol by applying the blinding operations previously described for both the Schnorr and Chaum-Pedersen protocols. In order to achieve partial blindness, we apply the same adaptation used by Abe and Okamoto [3] and use a specialised hash function to map the agreed common information, info, into the public key of the Schnorr proof of knowledge. As a result, no one can know the private key associated with the Schnorr public key. A signer who knows the private key associated with the Chaum-Pedersen protocol can complete the blind issuing protocol as it is only necessary to demonstrate knowledge of one of the two private keys. Since the blinding operations do not alter the public keys, the association between info and Schnorr public key remains visible in spite of any blinding operations.

The restrictive property of the resulting scheme follows from the application of the same blinding operations used in Brands' original restrictive blind signature [5,6].

The setup for the scheme is as follows. Let two primes p and q be given such that q divides $p - 1$ and let $g \in \mathbb{Z}_p^*$ be an element of order q. The group generated by g is denoted by G_q. Choose a key pair (x_1, y_1) for the Chaum-Pedersen proof of knowledge. That is, let $x_1 \in_R \mathbb{Z}_q$ be a private key associated with the corresponding public key $y_1 = g^{x_1}$. Let $\mathcal{H} : \{0,1\}^* \rightarrow \mathbb{Z}_q$ be a public hash function.

The common information, info, is placed in the Schnorr public key y_2 by setting $y_2 = \mathcal{F}(\mathsf{info})$, where $\mathcal{F} : \{0,1\}^* \rightarrow G_q$ is a public hash function which maps arbitrary strings into elements in G_q. Abe and Okamoto [3] show two deterministic constructions for $\mathcal{F}$. The signer then signs with private key x_1 which is associated with y_1. Since the resulting signature is bound to both public keys, y_1 and y_2, the common information info is also bound to the signature. This adaptation preserves witness indistinguishability which is needed for the proof of security. It is assumed that the signer $\mathcal{S}$ and the recipient $\mathcal{R}$ have previously agreed on the common information info. The full signature issuing protocol is shown in fig. 1. Note that additional group membership tests have been omitted for the sake of clarity.

Signer $\mathcal{S}$ (knows x_1 s.t. $y_1 = g^{x_1}$)		Recipient $\mathcal{R}$ (knows y_1)
info is agreed common information.		
$y_2 = \mathcal{F}(\mathsf{info})$		$y_2 = \mathcal{F}(\mathsf{info})$
	$\xleftarrow{\text{message } m}$	
Commitment Phase for Chaum-Pedersen (C-P)		
$r_1 \in_R \mathbb{Z}_q^*$		
$z_1 = m^{x_1}$		
$a_1 = g^{r_1}$		
$b_1 = m^{r_1}$		
Simulate Schnorr transcript		
$c_2, s_2 \in_R \mathbb{Z}_q^*$		
$a_2 = g^{s_2} y_2^{-c_2}$		
	$\xrightarrow{z_1, a_1, b_1, a_2}$	
		Brands' blinding for C-P
		$\alpha_1, \beta_1 \in_R \mathbb{Z}_q$
		$m_1' = m^{\alpha_1} g^{\beta_1}$
		$z_1' = z_1^{\alpha_1} y_1^{\beta_1}$
		$u_1, v_1 \in_R \mathbb{Z}_q$
		$a_1' = a_1^{u_1} g^{v_1}$
		$b_1' = a_1^{u_1\beta_1}\ b_1^{u_1\alpha_1}\ (m_1')^{v_1}$
		Multiplicative Schnorr blinding
		$u_2, v_2 \in_R \mathbb{Z}_q$
		$a_2' = a_2^{u_2} g^{v_2}$
		Generate the challenge
		$K = g \parallel y_1 \parallel y_2$
		$c' = \mathcal{H}(K \parallel m_1' \parallel z_1' \parallel a_1' \parallel b_1' \parallel a_2')$
		Blind the challenge
		$c = c'/u_1 u_2 \mod q$
	$\xleftarrow{c}$	
Share c between c_1 and c_2		
$c_1 = c/c_2 \mod q$		
Calculate response		
$s_1 = r_1 + c_1 x_1 \mod q$	$\xrightarrow{c_1, s_1, c_2, s_2}$	
		Check Sharing: $c \stackrel{?}{=} c_1 c_2$
		Check C-P and unblind
		$a_1 \stackrel{?}{=} g^{s_1} y_1^{-c_1}$
		$b_1 \stackrel{?}{=} m^{s_1} z_1^{-c_1}$
		$c_1' = c_1 u_1$
		$s_1' = u_1 s_1 + v_1 \mod q$
		Check Schnorr and unblind
		$a_2 \stackrel{?}{=} g^{s_2} y_2^{-c_2}$
		$c_2' = c_2 u_2$
		$s_2' = u_2 s_2 + v_2 \mod q$

Fig. 1. Restrictive Partially Blind Signature on a message $m_1' \in G_q$

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

$$c_1' \cdot c_2' = \mathcal{H}\left(K \parallel m_1' \parallel z_1' \parallel g^{s_1'} y_1^{-c_1'} \parallel (m_1')^{s_1'} (z_1')^{-c_1'} \parallel g^{s_2'} \mathcal{F}(\mathsf{info})^{-c_2'}\right) \mod q$$

where $K = g \parallel y_1 \parallel \mathcal{F}(\mathsf{info})$.

Correctness

$$\begin{aligned}
c' &= u_1 u_2 c = u_1 u_2 c_1 c_2 = (u_1 c_1)(c_2 u_2) = c_1' c_2' \\
g^{s_1'} y_1^{-c_1'} &= g^{u_1 s_1 + v_1} y_1^{-c_1 u_1} = (g^{s_1} y_1^{-c_1})^{u_1} g^{v_1} = {a_1}^{u_1} g^{v_1} = a_1' \\
(m_1')^{s_1'} (z_1')^{-c_1'} &= (m_1')^{u_1 s_1 + v_1} (z_1')^{-c_1 u_1} = \left((m_1')^{s_1} (z_1')^{-c_1}\right)^{u_1} (m_1')^{v_1} \\
&= \left((m^{\alpha_1} g^{\beta_1})^{s_1} (z_1^{\alpha_1} y_1^{\beta_1})^{-c_1}\right)^{u_1} (m_1')^{v_1} \\
&= \left((m^{s_1} z_1^{-c_1})^{\alpha_1} (g^{s_1} y_1^{-c_1})^{\beta}\right)^{u_1} (m_1')^{v_1} \\
&= a_1^{u_1 \beta_1} \; b_1^{u_1 \alpha_1} \; (m_1')^{v_1} = b_1' \\
g^{s_2'} y_2^{-c_2'} &= g^{u_2 s_2 + v_2} y_2^{-c_2 u_2} = (g^{s_2} y_2^{-c_2})^{u_2} g^{v_2} = {a_2}^{u_2} g^{v_2} = a_2'
\end{aligned}$$

Restrictiveness: As previously noted, since the blinding operations for the Chaum-Pedersen protocol are the same as those used for Brands' restrictive blind signature [5,6], the restrictive nature of our protocol follows from the properties attributed to Brands' restrictive blind signature [5,6].

6 Security

This section discusses the security of the scheme under the assumption of the intractability of the discrete logarithm problem and ideal randomness of hash functions $\mathcal{H}$ and $\mathcal{F}$.

Lemma 1. *The proposed scheme is partially blind.*

Proof. When $\mathcal{S}^*$ is given $\perp$ in step 5 of the game defined in definition 3, $\mathcal{S}^*$ determines b with a probability $\frac{1}{2}$ (the same probability as randomly guessing b).

Suppose that in in step 5, $\mathsf{info}_1 = \mathsf{info}_0$. Let $(c_1', s_1', c_2', s_2', m_1')$ be one of the signatures subsequently given to $\mathcal{S}^*$. Let $(r_1, z_1, a_1, b_1, c_1, s_1, a_2, c_2, s_2, \mathsf{info}, m)$ be data appearing in the view of $\mathcal{S}^*$ during one of the executions of the signature

issuing protocol at step 4 of definition 3. It is sufficient to show that there exists a tuple of random blinding factors $(\alpha_1, \beta_1, u_1, v_1, u_2, v_2)$ that maps

$$(r_1, z_1, a_1, b_1, c_1, s_1, a_2, c_2, s_2, m) \mapsto (c'_1, s'_1, c'_2, s'_2, m'_1).$$

Choose the unique blinding factors

$$\begin{aligned} u_1 &= c'_1/c_1 \mod q \\ v_1 &= s'_1 - u_1 s_1 \mod q \\ u_2 &= c'_2/c_2 \mod q \\ v_2 &= s'_2 - u_2 s_2 \mod q \end{aligned}$$

and determine a representation $m'_1 = m^{\alpha_1} g^{\beta_1}$ (which is known to exist).

The fact that $z_1 = m^{x_1}$ and $z'_1 = {m'_1}^{x_1}$ has been established by the interactive proof provided by the signer during blind signature formation and the fact that the blind signature is valid. Therefore, $z'_1 = (m'_1)^{x_1} = (m^{\alpha_1} g^{\beta_1})^{x_1} = {z_1}^{\alpha_1} y_1^{\beta_1}$. Since $a_1 = g^{s_1} y_1^{-c_1}$ and $a_2 = g^{s_2} y_2^{-c_2}$, we find that

$$\begin{aligned} c'_1 c'_2 &= \mathcal{H}\left(K \parallel m'_1 \parallel z'_1 \parallel g^{s'_1} y_1^{-c'_1} \parallel (m'_1)^{s'_1} (z'_1)^{-c'_1} \parallel g^{s'_2} y_2^{-c'_2}\right) \\ &= \mathcal{H}\left(K \parallel m'_1 \parallel z'_1 \parallel g^{v_1 + u_1 s_1} y_1^{-u_1 c_1} \parallel (m'_1)^{v_1 + u_1 s_1} (z'_1)^{-u_1 c_1} \parallel g^{v_2 + u_2 s_2} y_2^{-u_2 c_2}\right) \\ &= \mathcal{H}\left(K \parallel m'_1 \parallel z'_1 \parallel {a_1}^{u_1} g^{v_1} \parallel {a_1}^{u_1 \beta_1} {b_1}^{u_1 \alpha_1} (m')^{v_1} \parallel {a_2}^{u_2} g^{v_2}\right) \\ &= \mathcal{H}\left(K \parallel m'_1 \parallel z'_1 \parallel a'_1 \parallel b'_1 \parallel a'_2\right) \end{aligned}$$

where $a'_1 = {a_1}^{u_1} g^{v_1}$, $b'_1 = {a_1}^{u_1 \beta_1} {b_1}^{u_1 \alpha_1} (m')^{v_1}$, and $a'_2 = {a_2}^{u_2} g^{v_2}$.

Thus blinding factors always exist which lead to the same relation defined in the signature issuing protocol. Therefore, even an infinitely powerful $\mathcal{S}^*$ succeeds in determining b with probability $\frac{1}{2}$. □

Lemma 2. *The proposed scheme is unforgeable if* $\ell_{\mathsf{info}} < poly(\log n)$ *for all* info.

Due to space considerations, a proof of this lemma is omitted. The security argument given by Abe and Okamoto [3] is acknowledged as being more generic than the particular application detailed by Abe and Okamoto [3]. The proof of our lemma follows the same general construction.

7 Conclusions

The blinding of the Schnorr protocol utilised by our scheme uses multiplicative blinding for the challenge rather than the more usual additive method. As a result, the consequent witness indistinguishable protocol uses a novel multiplicative sharing scheme in its construction.

We have shown a particular construction of a restrictive partially blind signature scheme based on a witness indistinguishable protocol which combines both the Schnorr and Chaum-Pedersen signature schemes. The provable security of

the construction has been considered in terms of the formal definitions proposed by Abe and Okamoto [3]. The scheme uses Brands' restrictive blind signature [5,6] as a building block and is suitable for inclusion in cash schemes which currently utilise Brands' restrictive blind signature. The partially blind property aids in the practical deployment of these cash schemes as it allows for the easy implementation of coin expiration dates and multiple coin denominations.

Acknowledgments

We would like to thank the anonymous referees for their insightful observations and suggestions. This research is part of an ARC SPIRT project undertaken jointly by Queensland University of Technology and Telstra (Australia).

References

1. Masayuki Abe and Jan Camenisch. Partially blind signature schemes. In *Symposium on Cryptography and Information Security*. IEICE, January 1997.
2. Masayuki Abe and Eiichiro Fujisaki. How to date blind signatures. In Kwangjo Kim and Tsutomu Matsumoto, editors, *International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'96)*, volume 1163 of *Lecture Notes in Computer Science*, pages 244–251. Springer-Verlag, November 1996.
3. Masayuki Abe and Tatsuaki Okamoto. Provably secure partially blind signatures. In Mihir Bellare, editor, *Advances in Cryptology—CRYPTO 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 271–286. Springer-Verlag, 20–24 August 2000.
4. C. Boyd, E. Foo, and C. Pavlovski. Efficient electronic cash using batch signatures. In J. Pieprzyk, R. Safavi-Naini, and J. Seberry, editors, *Australasian Conference on Information Security and Privacy (ACISP'99)*, volume 1587 of *Lecture Notes in Computer Science*, pages 244–257. Springer-Verlag, 1999.
5. Stefan Brands. An efficient off-line electronic cash system based on the representation problem. Technical Report CS-R9323, Centrum voor Wiskunde en Informatica (CWI), March 1993.
6. Stefan Brands. Untraceable off-line cash in wallets with observers. In Douglas R. Stinson, editor, *Advances in Cryptology—CRYPTO '93*, volume 773 of *Lecture Notes in Computer Science*, pages 302–318. Springer-Verlag, 22–26 August 1993.
7. A. Chan, Y. Frankel, and Y. Tsiounis. Easy come — easy go divisible cash. In Kaisa Nyberg, editor, *Advances in Cryptology—EUROCRYPT 98*, volume 1403 of *Lecture Notes in Computer Science*, pages 561–576. Springer-Verlag, 1998.
8. D. Chaum and T. Pryds Pedersen. Wallet databases with observers. In Ernest F. Brickell, editor, *Advances in Cryptology—CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 89–105. Springer-Verlag, 1993, 16–20 August 1992.
9. David Chaum. Blind signatures for untraceable payments. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology: Proceedings of Crypto 82*, pages 199–203. Plenum Press, New York and London, 1983, 23–25 August 1982.

10. Ronald J. F. Cramer, Ivan B. Damgård, and L. A. M. Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In *116*, page 18. Centrum voor Wiskunde en Informatica (CWI), ISSN 0169-118X, February 28 1994. AA (Department of Algorithmics and Architecture).
11. U. Feige and A. Shamir. Witness indistinguishable and witness hiding protocols. In Baruch Awerbuch, editor, *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing*, pages 416–426, Baltimore, MY, May 1990. ACM Press.
12. A. Juels, M. Luby, and R. Ostrovsky. Security of blind digital signatures. In Burton S. Kaliski Jr., editor, *Advances in Cryptology—CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 150–164. Springer-Verlag, 17–21 August 1997.
13. Shingo MIYAZAKI, Masayuki ABE, and Kouichi SAKURAI. Partially blind signature schemes for the dss and for a discrete log. based message recovery signature. In *Korea-Japan Joint Workshop on Information Security and Cryptology*, pages 217–226, 1997.
14. DaeHun Nyang and JooSeok Song. Preventing double-spent coins from revealing user's whole secret. In J.S. Song, editor, *Second International Conference on Information Security and Cryptology (ICISC'99)*, volume 1787 of *Lecture Notes in Computer Science*, pages 13–20. Springer-Verlag, 1999.
15. T. Okamoto. Provably secure and practical identification schemes and corresponding signature schemes. In Ernest F. Brickell, editor, *Advances in Cryptology—CRYPTO '92*, volume 740 of *Lecture Notes in Computer Science*, pages 31–53. Springer-Verlag, 1993, 16–20 August 1992.
16. D. Pointcheval. Strengthened security for blind signatures. In Kaisa Nyberg, editor, *Advances in Cryptology—EUROCRYPT 98*, volume 1403 of *Lecture Notes in Computer Science*, pages 391–403. Springer-Verlag, 1998.
17. C. P. Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*, 4(3):161–174, 1991.
18. L. A. M. Schoenmakers. An efficient electronic payment system withstanding parallel attacks. Technical Report CS-R9522, CWI - Centrum voor Wiskunde en Informatica, March 31, 1995.