18

A Restrictive Blind Signature Scheme with Applications to Electronic Cash

C. Radu, R. Govaerts, J. Vandewalle
Katholieke Universiteit Leuven
Laboratorium ESAT-COSIC,Katholieke Universiteit Leuven,
Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium.
email: Cristian.Radu@esat.kuleuven.ac.be

Abstract

A restrictive blind signature scheme is a cryptographic primitive involved in the design of untraceable off-line electronic payment systems. The security of this primitive determines both the integrity of the bank and the anonymity of the payers. Brands proved that a restrictive blind issuing protocol for secret-key certificates can be derived from any signature scheme of Fiat-Shamir type, if the latter can be ordinary blinded. There is not a similar result for the restrictive blind issuing of public-key certificates. Only one such primitive is known. It is derived from Schnorr's identification protocol. Our paper presents another restrictive blind signature scheme, that can be used for public-key certificates. This solution is developed from the Identification Scheme type 1 and the corresponding signature scheme introduced by Okamoto. Using this blind signature protocol, we design an efficient untraceable electronic cash system.

Keywords

Blind signature schemes, public-key certificates, anonymity, electronic cash

1 INTRODUCTION

An electronic coin can be implemented like a secret key/public key used by the payer to sign the specification of a payment. The bank certifies the public key of a coin by digitally signing it with respect to its own public key. Latter on, this public-key certificate can be verified off-line by the payee, using the public key of the bank. The authenticity of the

P. Horster (ed.), *Communications and Multimedia Security II*

coins is essential for their acceptability by the bank at the deposit stage. The bank issues the public-key certificates of coins during withdrawal. The ability of the designer to make the signature of the bank a blind signature protocol is crucial in order to provide privacy for payers. The first requirement for this protocol is that the bank should not be able to link the public key of the coin and its certificate to a particular issuing protocol that has led to this pair. The protocol fulfilling this requirement is referred to as an *ordinary* blind signature protocol and is appropriate from the payer's point of view. However, the bank requires a stronger condition: the message to be signed in a blinded way must contain an invariant part with regard to the blinding operations carried out by the payer. Usually, this part allows the multiple spending detector to derive the identity of a payer who abused the system by spending copies of an electronic coin. The attribute *restrictive* refers to this kind of blind signature schemes.

In the framework of secret-key certificates, Brands (1995) proved that for any Fiat-Shamir type signature scheme for which an ordinary blind signature scheme can be constructed, a restrictive blind signature scheme can also be derived. There is not a similar result for the restrictive blind issuing of public-key certificates. There is only one restrictive blind signature scheme used for the issuing of public-key certificates. It is employed by the electronic payment systems described by Brands (1993), Ong and Okamoto (1994). This scheme is derived from Schnorr's signature scheme (Schnorr, 1991) based on a method presented for the first time by Chaum and Pedersen (1993). The same methodology can be immediately extended to Brickell-McCurley's signature scheme (Brickell and McCurley, 1992). However, it is not trivial extending this procedure to other Fiat-Shamir type signature schemes (Fiat and Shamir, 1987). The goal of this paper is to introduce a restrictive blind signature scheme derived from the Identification Scheme type 1 proposed by Okamoto (1993), following the principles introduced by Chaum and Pedersen (1993). Our scheme provides a better restrictiveness than the scheme in (Brands, 1993). We illustrate the functionality of our scheme through an efficient off-line payment system, providing privacy for payers. The design follows the lines of the payment system proposed by Brands (1993).

The remainder of the paper is organized as follows. In Section 2 we introduce the notations, definitions and the main cryptographic assumption we use. The interactive signature scheme and the corresponding basic proof system are described in Section 3. This is the starting point from which, in Section 4, we derive the proposed restrictive blind signature scheme. In the last section we outline the design of an electronic cash system, the withdrawal stage of which relies on the proposed blind signature scheme. Finally, our conclusions are presented.

2 NOTATIONS, DEFINITIONS AND ASSUMPTIONS

For any prime p, the set of positive integers smaller than p is denoted $\mathbb{Z}_p^*$. Let q be a prime such that q divides $p-1$. We denote by G_q the unique subgroup of $\mathbb{Z}_p^*$ of order q. This subgroup can be generated as follows:

1. choose at random $\xi \in_{\mathcal{R}} \mathbb{Z}_p^*$;
2. compute $\gamma \leftarrow \xi^{(p-1)/q}$;
3. If $\gamma = 1$ go to Step 1. Otherwise, compute G_q as $\left\{1, \gamma, \gamma^2, \ldots \gamma^{(q-1)}\right\}$.

In expressions involving elements in G_q we do not explicitly mention the reduction modulo p.

Definition 1 *A generator-pair $(g_1, g_2) \in G_q^2$ consists of a pair of different generators $g_1 \neq g_2 \in G_q$. A witness of $h \in G_q$ with respect to the generator-pair (g_1, g_2), denoted with $witness_{(g_1,g_2)}(h)$, is a pair $(s_1, s_2) \in \mathbb{Z}_q^2$ such that $h = g_1^{s_1} g_2^{s_2}$.*

The security of the interactive signature scheme and the corresponding basic proof system, as well as the security of the restrictive blind signature scheme rely on the following assumption:

Assumption 1 *Finding a witness $(s_1, s_2) \in \mathbb{Z}_q^2$ with respect to the generator-pair $(g_1, g_2) \in G_q^2$ of $h \in G_q$ is the Representation problem of degree 2, which we denote by $\mathbf{R}^2$. An algorithm is said to solve the problem $\mathbf{R}^2$ if, for inputs $(g_1, g_2) \neq (1, 1)$, h generated uniformly at random, it outputs (s_1, s_2) with at least non-negligible probability of success such that $h = g_1^{s_1} g_2^{s_2}$. The $\mathbf{R}^2$ assumption states that there is no polynomial-time algorithm that solves the $\mathbf{R}^2$ problem.*

It can be proved that the $\mathbf{R}^2$ problem is equivalent in computational difficulty to the Discrete Log problem for groups of prime order.

3 THE INTERACTIVE SIGNATURE SCHEME AND THE BASIC PROOF SYSTEM

An interactive signature scheme can be derived from Okamoto's Identification Scheme type 1 (Okamoto, 1993), using a similar procedure to that introduced by Chaum and Pedersen (1993). It allows a signer, represented by the public key $(p, q, (g_1, g_2) \in G_q^2 \setminus \{(1,1)\}, h \in G_q \setminus \{1\})$ and the corresponding secret key $(s_1, s_2) \in \mathbb{Z}_q^2$, to interactively sign

a message $m \in G_q$. The signature on m consists of $z = m^{s_1+s_2}$ and a proof of knowledge of a witness of h with respect to (g_1, g_2), the components of which verify z. This proof of knowledge is provided by the *basic proof system*, where the signer plays the prover's role.

Given m, the basic proof system is described by the following protocol:

1. The prover P generates $(w_1, w_2) \in \mathbb{Z}_q^2$ at random and sends $a \leftarrow g_1^{w_1} g_2^{w_2}$, $b \leftarrow m^{w_1+w_2}$ and $z = m^{s_1+s_2}$ to the verifier V.
2. V generates a challenge $c \in \mathbb{Z}_q$ at random, and sends it to P.
3. P computes the responses $r_1 \leftarrow w_1 - cs_1 \bmod q$, $r_2 \leftarrow w_2 - cs_2 \bmod q$ and sends (r_1, r_2) to V.
4. V accepts the proof if $a = g_1^{r_1} g_2^{r_2} h^c$ and $b = m^{r_1+r_2} z^c$.

We analyze the security of the basic proof system, considering the possibilities of cheating for P and V. Let $\tilde{P}$ (resp. $\tilde{V}$) denote a fraudulent P (resp. V). $\tilde{P}$(resp. $\tilde{V}$) may deviate from the protocol in computing $a, b, z, (r_1, r_2)$ (resp. c). $\tilde{P}$ does not know either the secret (s_1, s_2) or the sum of its components. $\tilde{V}$ can "learn" from P's proofs.

Proposition 1 *The basic proof system is complete and sound.*

Proof. If P is honest, in the sense that he knows a witness of h with respect to (g_1, g_2) verifying also z for a given m, then V always accepts P's proof of knowledge. This states the completeness of the basic proof system.

The fraudulent $\tilde{P}$ can cheat by guessing the correct $c \in \mathbb{Z}_q$ and sending, with an arbitrary $(w_1, w_2) \in \mathbb{Z}_q^2$, the following items: $z \in_{\mathcal{R}} G_q$, $a \leftarrow g_1^{w_1} g_2^{w_2} h^c$, $b \leftarrow m^{w_1+w_2} z^c$ and $(r_1, r_2) \leftarrow (w_1, w_2)$. The probability of success for this attack is $1/q$.

It remains to prove that this success rate cannot be increased unless computing a valid witness of h with respect to (g_1, g_2) is easy. Suppose $\tilde{P}$ is able to convince V in time T with a probability at least $2^t/q$, for an integer $t \geq 1$. Then, given m, $\tilde{P}$ chooses in a suitable way a, b and z. Given these items, the prover must be able to correctly answer at least 2^t different challenges. Let c and c' be two such challenges, which can be found in expected time $2^{1-t}qT$. Let (r_1, r_2) and (r_1', r_2') be the corresponding responses, that respect the relations $r_1 = w_1 - cs_1 \bmod q, r_2 = w_2 - cs_2 \bmod q$ and $r_1' = w_1 - c's_1 \bmod q, r_2' = w_2 - c's_2 \bmod q$. Because the probability that $c' - c \equiv 0 \bmod q$ is less than 2^{-t}, then with a probability at least $1 - 2^{-t}$ the fraudulent $\tilde{P}$ is able to compute a valid witness of h with respect to (g_1, g_2), as $s_1 = (c' - c)^{-1}(r_1 - r_1') \bmod q$, $s_2 = (c' - c)^{-1}(r_2 - r_2') \bmod q$.

Thus, there is a contradiction with Assumption 1. Therefore, if $\tilde{P}$ does not know a valid witness of h with respect to (g_1, g_2) , there is not a strategy for him such that V accepts with non-negligible probability of success. This proves the soundness of the basic proof system. □

The following proposition shows that the prover in the basic proof system that uses an incorrect z is successful with negligible probability.

Proposition 2 *When $z \neq m^{s_1+s_2}$ in the basic proof system, then the verifier accepts with probability at most $1/q$.*

This three-move sound basic proof system is not "zero-knowledge" (Feige, Fiat and Shamir, 1988), but we conjecture that it does not leak useful information about the secret key of the signer.

If in the basic proof system we replace the challenge of the verifier by the value of a collision-resistant hash function applied to the message m and the information sent by the user in the first move, one can derive a Fiat-Shamir type signature scheme (Fiat and Shamir, 1987). It produces a signature on m of the form $sign(m) = (z, c, (r_1, r_2))$. The signature is correct if $c = \mathcal{H}(m, z, g_1^{r_1} g_2^{r_2} h^c, m^{r_1+r_2} z^c)$. Considering the security of the scheme, we first argue that it is not possible to forge signatures given only the public key. Indeed, if $\mathcal{H}(\cdot)$ is like a random oracle, in the sense that it is as difficult to convince a verifier who chooses $c = \mathcal{H}(m, z, a, b)$ as a verifier who chooses the challenge at random, it is not possible to make signatures without knowing the secret key (s_1, s_2). Furthermore, it is hopeless for a forger to derive more information about the secret key of the signer from the execution of the basic proof system, if we accept that a proof does not leak any useful information. Finally, we analyze the possibility to construct a false signature by combining various given signatures $(m_i, sign(m_i))$, where the forger can choose m_i adaptively (Goldwasser, Micali and Rivest, 1988). If we accept $z_i = m_i^{s_1+s_2}$, there is a multiplicative relation which might be useful for a forger $z_1 z_2 = (m_1 m_2)^{s_1+s_2}$. Therefore, the hash function must prevent the forger from combining different signatures into a new signature.

4 THE RESTRICTIVE BLIND SIGNATURE SCHEME

In this section we transform the interactive signature scheme to a blind signature scheme, applying the technique described by Okamoto and Ohta (1990). Therefore, we do not remove the interaction for converting the three-move sound basic proof system into a one-step signature protocol. Allowing the verifier to determine the challenge, the message-signature pair can be issued in a blind way.

The verifier can get a blind signature only on a message m of the form $m = m_0^t$, where $m_0 \in G_q$ is known to the signer and t is a random choice of the verifier in $\mathbb{Z}_q$. Given $m_0, z_0 = m_0^{s_1+s_2}$ the signer proves that he knows a witness of h with respect to (g_1, g_2) whose components also verify z_0, in a such a way that the messages exchanged between the prover and the verifier are blinded. The protocol is described by the following steps:

1. The signer generates at random $(w_{01}, w_{02}) \in_{\mathcal{R}} \mathbb{Z}_q^2$ and sends to the verifier $a_0 \leftarrow g_1^{w_{01}} g_2^{w_{02}}$, $b_0 \leftarrow m_0^{w_{01}+w_{02}}$.
2. The verifier generates at random $t, u \in \mathbb{Z}_q$, $(v_1, v_2) \in \mathbb{Z}_q^2$ and computes a new message $m = m_0^t$ and the corresponding value of a new $z = z_0^t$, both values being unknown to the signer. The verifier also computes the blinded versions of a_0, b_0 as $a \leftarrow a_0 g_1^{v_1} g_2^{v_2} h^u$ and $b \leftarrow (b_0 m_0^{v_1+v_2} z_0^u)^t$, respectively. Then he computes $c = \mathcal{H}(m, z, a, b)$ and sends $c_0 = c - u \bmod q$ to the signer.
3. The signer responds to this challenge with (r_{01}, r_{02}), where $r_{01} \leftarrow w_{01} - c_0 s_1 \bmod q$ and $r_{02} \leftarrow w_{02} - c_0 s_2 \bmod q$.
4. The verifier accepts if and only if $a_0 = g_1^{r_{01}} g_2^{r_{02}} h^{c_0}$ and $b_0 = m_0^{r_{01}+r_{02}} z_0^{c_0}$. The verifier also corrects the response (r_{01}, r_{02}) as (r_1, r_2), where $r_1 \leftarrow r_{01} + v_1 \bmod q$ and $r_2 \leftarrow r_{02} + v_2 \bmod q$. Finally, the blind signature on the message m consists of $sign(m) = (z, c, (r_1, r_2))$.

Proposition 3 *Whenever the verifier follows the blind signature protocol and accepts, then* $sign(m) = (z, c, (r_1, r_2))$ *is a correct signature on* m.

Proof. The signature $sign(m) = (z, c, (r_1, r_2))$ is a correct signature on m if the equality

$$c = \mathcal{H}(m, z, g_1^{r_1} g_2^{r_2} h^c, m^{r_1+r_2} z^c)$$

is verified. This is equivalent to prove that

$$a = g_1^{r_1} g_2^{r_2} h^c \text{ and } b = m^{r_1+r_2} z^c.$$

The first relation follows from:

$$g_1^{r_1} g_2^{r_2} h^c = g_1^{r_{01}+v_1} g_2^{r_{02}+v_2} h^{c_0+u} = (g_1^{r_{01}} g_2^{r_{02}} h^{c_0}) g_1^{v_1} g_2^{v_2} h^u = a_0 g_1^{v_1} g_2^{v_2} h^u = a,$$

because $a_0 = g_1^{r_{01}} g_2^{r_{02}} h^{c_0}$ if the verifier accepts. Similarly:

$$m^{r_1+r_2} z^c = m^{r_{01}+v_1+r_{02}+v_2} z^{c_0+u} \overset{\mathbf{P_1}}{=} \left(m_0^{r_{01}+r_{02}} z_0^{c_0} m_0^{v_1+v_2} z_0^u\right)^t =$$
$$= \left(b_0 m_0^{v_1+v_2} z_0^u\right)^t = b.$$

because we accept that $m = m_0^t$, $z = z_0^t$ and $b_0 = m_0^{r_{01}+r_{02}} z_0^{c_0}$. □

Proposition 4 *(Unconditional Unlinkability) Even with unlimited computing power, the signer gets no information about* m *and* $sign(m) = (z, c, (r_1, r_2))$ *if the verifier follows the protocol.*

Proof. Let m_0, z_0, a_0, b_0, c_0 and (r_{01}, r_{02}) be the signer's view in a successful execution of the blind signature protocol, such that $a_0 = g_1^{r_{01}} g_2^{r_{02}} h^{c_0}$ and $b_0 = m_0^{r_{01}+r_{02}} z_0^{c_0}$. It is sufficient to prove that for any valid pair $m, sign(m) = (z, c, (r_1, r_2))$, verifying $c = \mathcal{H}(m, z, a, b)$, where $a = g_1^{r_1} g_2^{r_2} h^c$ and $b = m^{r_1+r_2} z^c$, there is exactly one set of values of the random variables $t, u, (v_1, v_2)$ such that:

$$
\begin{aligned}
m &= m_0^t; \\
z &= z_0^t; \\
a &= a_0 g_1^{v_1} g_2^{v_2} h^u; \\
b &= \left(b_0 m_0^{v_1+v_2} z_0^u\right)^t; \\
c &= c_0 + u \bmod q; \\
r_1 &= r_{01} + v_1 \bmod q; \\
r_2 &= r_{02} + v_2 \bmod q.
\end{aligned}
$$

First, given m_0 and m we can compute the value of t as $t = \log_{m_0} m$. The values of u and (v_1, v_2) can be computed from c, c_0 and $(r_1, r_2), (r_{01}, r_{02})$ as $u = c - c_0 \bmod q$ and $(v_1 = r_1 - r_{01} \bmod q, v_2 = r_2 - r_{02} \bmod q)$.

It remains to prove that these values of t, u and (v_1, v_2) verify the equalities $z = z_0^t$, $a = a_0 g_1^{v_1} g_2^{v_2} h^u$ and $b = (b_0 m_0^{v_1+v_2} z_0^u)^t$. In order to prove the first equality, it can be assumed that $z_0 = m_0^{s_1+s_2}$ and $z = m^{s_1+s_2}$, because the signer actually proves that z_0 equals $m_0^{s_1+s_2}$ when making a blind signature. Hence, $m = m_0^t$ implies that:

$$z = m^{s_1+s_2} = \left(m_0^t\right)^{s_1+s_2} = m_0^{t(s_1+s_2)} = (m_0^{s_1+s_2})^t = z_0^t.$$

The other two relations can be proved as follows:

$$
\begin{aligned}
a &= g_1^{r_1} g_2^{r_2} h^c = g_1^{r_{01}+v_1} g_2^{r_{02}+v_2} h^{c_0+u} = (g_1^{r_{01}} g_2^{r_{02}} h^{c_0}) g_1^{v_1} g_2^{v_2} h^u = a_0 g_1^{v_1} g_2^{v_2} h^u; \\
b &= m^{r_1+r_2} z^c = m^{r_{01}+v_1+r_{02}+v_2} z^{c_0+u} = m^{r_{01}+r_{02}} z^{c_0} m^{v_1+v_2} z^u = \\
&= m_0^{t(r_{01}+r_{02})} z_0^{tc_0} m_0^{t(v_1+v_2)} z_0^{tu} = (m_0^{r_{01}+r_{02}} z_0^{c_0} m_0^{v_1+v_2} z_0^u)^t = (b_0 m_0^{v_1+v_2} z_0^u)^t.
\end{aligned}
$$

□

Assumption 2 *(Restrictiveness) The signer can obtain only one signature for each execution of the blind signature protocol. The signature is on a message that can be only of the form $m = m_0{}^t, m_0 \in G_q$, where the verifier chooses $t \in \mathbb{Z}_q$. Moreover, if there is*

$(\mu_{01}, \mu_{02}) \in \mathbb{Z}_q^2$ *that verifies the following two predicates:*

$\mathcal{S}(m_0, (\mu_{01}, \mu_{02})) :: m_0 = g_1^{\mu_{01}} g_2^{\mu_{02}}$ *(the structural predicate)* ,
$\mathcal{I}((\mu_{01}, mu_{02})) :: \mu_{01}/\mu_{02} \bmod q = i$ *(the blinding-invariant predicate)* .

then there is $(\mu_1, \mu_2) \in \mathbb{Z}_q^2$ *that verifies the same two predicates:*

$\mathcal{S}(m, (\mu_1, \mu_2)) :: m = g_1^{\mu_1} g_2^{\mu_2}$,
$\mathcal{I}((\mu_1, \mu_2)) :: \mu_1/\mu_2 \bmod q = i$.

Indeed, if there is a pair $(\mu_{01}, \mu_{02}) \in \mathbb{Z}_q^2$ that verifies:

$\mathcal{S}(m_0, (\mu_{01}, \mu_{02})) :: m_0 = g_1^{\mu_{01}} g_2^{\mu_{02}}$,
$\mathcal{I}((\mu_{01}, \mu_{02})) :: \mu_{01}/\mu_{02} \bmod q = i$,

and if we accept that $m = m_0^t$ then we can write $m = (g_1^{\mu_{01}} g_2^{\mu_{02}})^t = g_1^{t\mu_{01}} g_2^{t\mu_{02}}$. Therefore, we accept that there is $(\mu_1, \mu_2) \in \mathbb{Z}_q^2$, $\mu_1 = t\mu_{01} \bmod q$,$\mu_2 = t\mu_{02} \bmod q$ that verifies:

$\mathcal{S}(m, (\mu_1, \mu_2)) :: m = g_1^{\mu_1} g_2^{\mu_2}$ and ,
$\mathcal{I}((\mu_1, \mu_2)) :: \mu_1/\mu_2 \bmod q = t\mu_1/t\mu_2 \bmod q = i$.

5 AN UNTRACEABLE ELECTRONIC CASH SYSTEM

The main particularity of the electronic cash system outlined in this section is that the withdrawal protocol relies on the restrictive blind signature scheme we have introduced. The form of the electronic coin and the design procedure are similar to those used by Brands (1993). In the following we consider only three roles in the system: bank, payer and payee. Moreover, in order to avoid the overhead involved by the existence of a clearing system, we assume that both payer and payee are clients of the same bank. Each payer is represented in the system by an electronic purse implemented as a tamper-resistant smart card. The financial instruments that carry out the signature transport in the system are electronic coins. Each coin is untraceable, unless the payer tries to spend it more than once.

Let consider the generator-pair $(g_1, g_2) \in G_q^2$. These numbers are generated and published by the bank during the initialization of the system. For security reasons, we accept that the relative logarithms of g_1 and g_2 are unknown to the payers and payees. In order to issue signatures on the electronic coins, the bank uses the secret key $(S_1, S_2) \in_{\mathcal{R}} \mathbb{Z}_q^2$ and

the corresponding public key $P = g_1^{S_1} g_2^{S_2}$, in the framework of the blind signature issuing protocol described in the previous section.

When Alice wants to become a payer in the system she opens an account and registers at the bank. The bank issues a smart card (SC) for Alice, containing her secret key $s_a \in \mathbb{Z}_q$. This key is jointly generated by Alice and the bank, such that nobody is able to derive it. Otherwise, Alice can build a fake purse and the bank can frame Alice. The bank learns and stores Alice's public key $p_a = g_1^{s_a}$ during the SC's activation. In addition, Alice proves to the bank that she knows the secret key s_a corresponding to p_a. To this end, she uses the Schnorr identification protocol (Schnorr, 1991), considering as a common input p_a. The registration protocol is outlined in Figure 1.

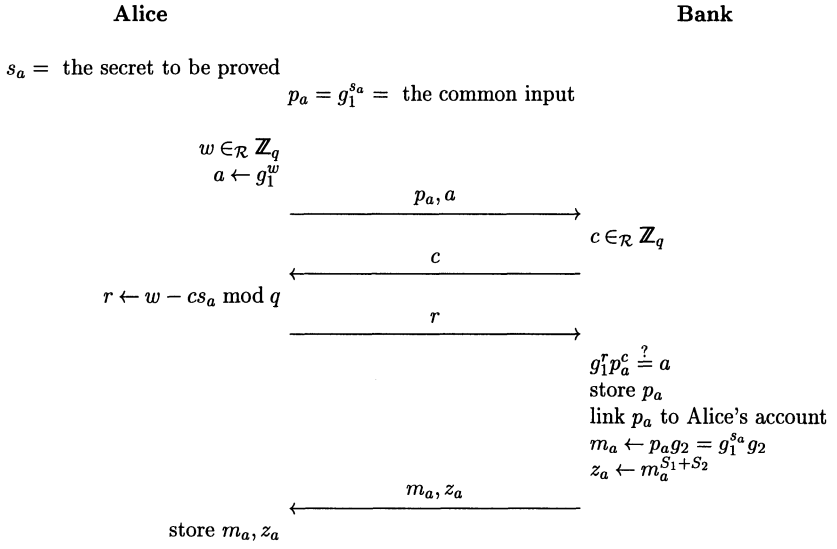

Figure 1 The registration protocol

The public key p_a links the SC of Alice to her account, which will be debited whenever Alice withdraws electronic coins. During the activation stage, the bank also computes and stores in Alice's SC two customized items for her, namely $m_a = p_a g_2 = g_1^{s_a} g_2$ and $z_a = m_a^{S_1+S_2}$. The message m_a encodes Alice's secret key s_a. The blinding operations carried out by Alice during the withdrawal protocol preserve a certain blinding-invariant structure of m_a, embedding Alice's secret key.

A coin is represented by the pair $(K, A) \in G_q^2$, where $K = m_a^t = g_1^{ts_a} g_2^t$, $A = g_1^{\sigma_1} g_2^{\sigma_2}$. The

numbers t, σ_1, σ_2 are random choices by Alice in $\mathbb{Z}_q$. The secret key of the coin is $(ts_a, t) \in \mathbb{Z}_q^2$. The coin (K, A) is authenticated by a signature of the bank. The authentication is carried out during withdrawal, when Alice (playing the role of verifier) and the bank (playing the role of the signer) execute the blind signature protocol, with respect to the bank's secret key/public key $(S_1, S_2)/P = g_1^{S_1} g_2^{S_2}$. The protocol is adapted from that described in Section 4 as follows. The bank ensures that K really encodes s_a, whereas Alice can choose A freely. However, A is included in the signature such that if Alice attempts to double-spend a coin she is forced to use the same A. The signature on (K, A) is the triple $(z, c, (r_1, r_2))$ satisfying $c = \mathcal{H}(K, z, A, a, b)$, where a and b are computed as $a = g_1^{r_1} g_2^{r_2} P^c$ and $b = K^{r_1 + r_2} z^c$. The withdrawal protocol is depicted in Figure 2.

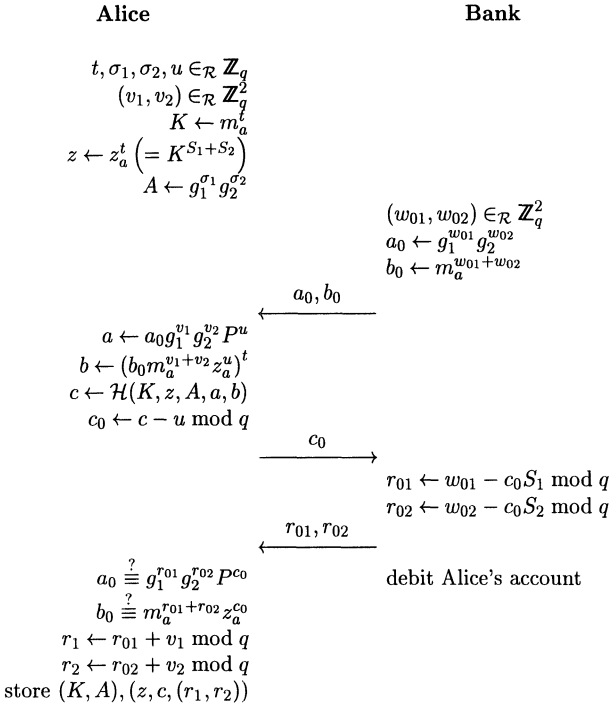

Figure 2 The withdrawal of electronic coins

In a payment transaction, Alice first sends the coin (K, A) and the bank's signature on it $(z, c, (r_1, r_2))$ to the payee Bob. He checks the authenticity of the coin, verifying

the correctness of the bank's signature. Then, Bob sends to Alice a challenge, which is composed by the specification of the current payment transaction (amount, date, Bob's identity) and a random sequience. Alice runs a proof of knowledge of the secret key of the coin (ts_a, t), using Okamoto's Identification Scheme type 1. As the commitment she must use the part $A = g_1^{\sigma_1} g_2^{\sigma_2}$ of the coin. Bob verifies the proof and if it is correct Alice can get her purchases. The payment protocol is depicted in Figure 3.

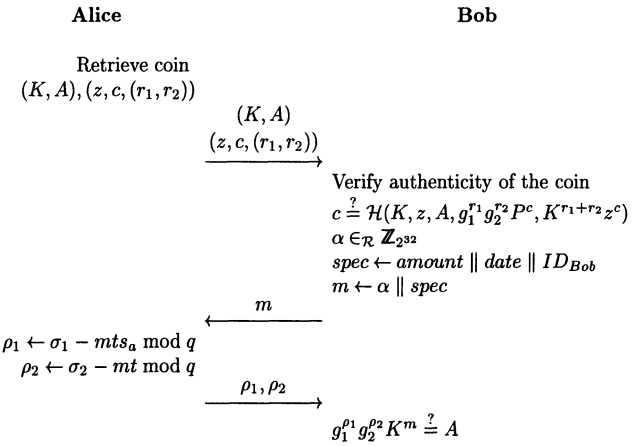

Figure 3 The payment protocol

At the deposit stage, Bob shows a transcript of the payment $(K, A), (z, c, (r_1, r_2))$, (m, ρ_1, ρ_2) to the bank. After the bank performs the same verifications that Bob has carried out in the payment, the coin is checked against double-deposit by Bob and against double-spending by Alice. On one hand, if m is the same in two transcripts, Bob attempted to double-deposit and the bank refuses to refund him. On the other hand, if a coin is used in more than one payment transcript

$$(K, A), (z, c, (r_1, r_2)), (m, \rho_1, \rho_2),$$
$$(K, A), (z, c, (r_1, r_2)), (m', \tau_1, \tau_2).$$

the bank can derive the secret key and public-key of the double-spender like

$$s_a = (\rho_1 - \tau_1)/(\rho_2 - \tau_2) \bmod q$$

and $p_a = g^{s_a}$. Therefore, the bank can derive the real identity of Alice.

6 CONCLUSION

We have introduced a restrictive blind signature scheme that is derived from Okamoto's Identification Scheme type 1, using the public key certificates technique. Our scheme provides a good level of security, relying only on classical cryptographic assumptions. The scheme can be successfully used as the basic cryptographic primitive in the design of the withdrawal stage of an efficient electronic cash system.

7 REFERENCES

Brands, S. (1993) Untraceable off-line cash in wallet with observers. *Advances in Cryptology - CRYPTO'93*, volume **773** of *Lecture Notes in Computer Science*, 302–318, Berlin, 1993. Springer-Verlag.

Brands, S. (1995) Restrictive blinding of secret-key certificates. *Advances in Cryptology - EUROCRYPT'95*, volume **921** of *Lecture Notes in Computer Science*, 231–247, Berlin, 1995. Springer-Verlag.

Brickell, E.F. and McCurley, K.S. (1992) An interactive identification scheme based on discrete logarithms and factoring. *Journal of Cryptology*, **5(1)**, 29–39.

Chaum, D. and Pedersen, T.P. (1993) Wallet databases with observers. *Advances in Cryptology - CRYPTO'92*, volume **740** of *Lecture Notes in Computer Science*, 89–105, Berlin, 1993. Springer-Verlag.

Feige, U., Fiat, A. and Shamir, A. (1988) Zero-knowledge proofs of identity. *Journal of Cryptology*, **1(2)**, 77–94.

Fiat, A. and Shamir, A. (1987) How to prove yourself: Practical solutions to identification and signature problems. *Advances in Cryptology - CRYPTO'86*, volume **263** of *Lecture Notes in Computer Science*, 186–194, New York, 1987. Springer-Verlag.

Goldwasser, S., Micali, S. and Rivest, R. (1988) A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, **17(2)**, 281–308.

Okamoto, T. (1993) Provably secure and practical identification schemes and and corresponding signature schemes. *Advances in Cryptology - CRYPTO'92*, volume **740** of *Lecture Notes in Computer Science*, 31–53, Berlin, 1993. Springer-Verlag.

Okamoto, T. and Ohta, K. (1990) Divertible zero-knowledge interactive proofs and commutative random self-reducibility. *Advances in Cryptology - EUROCRYPT'89*, volume **434** of *Lecture Notes in Computer Science*, 134–149, Heidelberg, 1990. Springer-Verlag.

Ong, T. and Okamoto, T. (1994) Single-term divisible electronic coins. *Advances in Cryptology - EUROCRYPT'94*, volume **950** of *Lecture Notes in Computer Science*, 306–319, Berlin, 1994. Springer-Verlag.

Schnorr, C.P. (1991) Efficient signature generation by smart cards. *Journal of Cryptology*, **4(3)**, 161–174.