Advances in Cryptology – Proceedings of ASIACRYPT '96 (november 3 – 7, 1996, Kyongju, S. Korea)
M. Y. Rhee and K. Kim Eds. Springer-Verlag, LNCS 1163, pages 252–265.

# Provably Secure Blind Signature Schemes

David Pointcheval and Jacques Stern

Laboratoire d'Informatique, cole Normale Suprieure,
45, rue d'Ulm, F – 75230 PARIS Cedex 05.
E-mail: {David.Pointcheval, Jacques.Stern}@ens.fr

**Abstract.** In this paper, we give a provably secure design for blind signatures, the most important ingredient for anonymity in off-line electronic cash systems. Previous examples of blind signature schemes were constructed from traditional signature schemes with only the additional proof of blindness. The design of some of the underlying signature schemes can be validated by a proof in the so-called random oracle model, but the security of the original signature scheme does not, by itself, imply the security of the blind version. In this paper, we first propose a definition of security for blind signatures, with application to electronic cash. Next, we focus on a specific example which can be successfully transformed in a provably secure blind signature scheme.

## 1 Introduction

### 1.1 Electronic Cash

With the growing importance of the Internet and trade, electronic cash has become a very active research area. Basic cryptographic notions that lay a firm foundation for E-cash were introduced by David Chaum [6–8]. His aim was to produce an electronic version of money which retains the same properties as paper cash, primarily anonymity and control by the Bank. He claimed that the way to ensure anonymity went through the use of coins together with the notion of blind signatures. When a user withdraws money from the Bank, the Bank

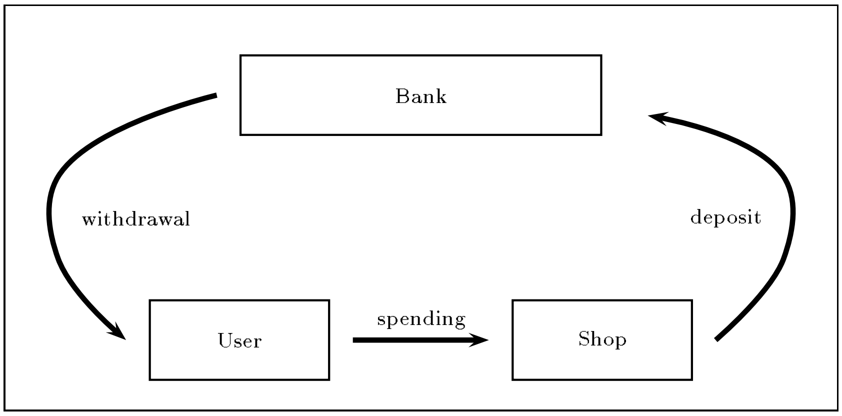


**Fig. 1.** Coin life

returns electronic coins which have been "blindly" signed. The user can then spend them at designated shops. Finally, the shops deposit the coins at the Bank (see figure 1). Blind signatures, on which this paper focus, will be defined below. They provide the tool by which the user gets a signature of a coin so that the Bank is unable to later recognize it. This technique is efficient in an one-line scenario. But if payment is off-line, there is no direct way to prevent a user to copy a coin and use it twice. This forgery is called "double spending". As a second step in the E-cash research, Chaum, Fiat and Naor [10] introduced the identity in the coin in such a way that the identity remains concealed, unless double spending happens, in which case it is revealed. This imposes a special format for the coin. Since it is created by the user, the Bank has to verify whether this format has been respected. Chaum, Fiat and Naor applied the "cut-and-choose" technique. The Bank signs many more coins than useful and, by random choice, requests the user to disclose the structure of some of them. The drawback of this technique is that this increases the communication load between the Bank and the user and the space needed to store coins. There were several improvements [9, 20], and in 1993, appeared schemes without the "cut-and-choose" methodology [4, 3, 14, 13]. More recently, unconditional anonymity has been criticized because of money laundering or other possible crimes [26], and escrow-based schemes were put forward as a new direction of the research [18].

### 1.2 Blind Signatures

Since the beginning of E-cash, blind signature has been the most important tool. It is an interactive protocol which involves two entities, a Bank and a user. It allows a user to get a message signed by the Bank without revealing this message. The message–signature pair received by the user is statistically uncorrelated to the view obtained by the Bank during the execution of the protocol.

Several signature schemes have been turned into blind signature schemes. Here are the most well-known. In what follows, $H$ is a hash function.

*The Blind RSA Signature* We first present a blind signature which is a transformation of the RSA signature scheme [23]. It was used by Chaum [6–8] for the withdrawal protocols of his first electronic cash system.

In the RSA context, we have a large composite number $n$, a public key $e$, and a secret key $d$. The signature of a message $m$ is the $e^{th}$ root of $H(m)$, $\sigma = H(m)^{1/e} = H(m)^d \bmod n$.

Now, in order to obtain the signature of a secret message $m$, the user blinds it with a random value $r^e \bmod n$, and sends $m' = H(m)r^e \bmod n$ to the signer. The latter returns a signature $\sigma'$ of $m'$ such that $\sigma'^e = m' = r^e H(m) \bmod n$. Then, it is easy to remark that $\sigma = \sigma' r^{-1} \bmod n$ is a valid signature of $m$.

*The Blind Schnorr Signature* The Schnorr signature scheme [24] can also be turned into a blind signature scheme. The transformation was used in the first electronic cash systems without "cut-and-choose".

We have two large prime integers $p$ and $q$, such that $q \,|\, p-1$. They are published together with an element $g$ of $(\mathbb{Z}/p\mathbb{Z})^\star$ of order $q$. The signer creates a pair of keys, $x \in \mathbb{Z}/q\mathbb{Z}$ and $y = g^{-x} \bmod p$. He publishes $y$. A user wants a blind signature of a message $m$. In order to issue this signature, the signer chooses a random $k \in \mathbb{Z}/q\mathbb{Z}$, computes and sends the "commitment"

$r = g^k \bmod p$. The user blinds it with two random elements $\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}$, into $r' = rg^{-\alpha}y^{-\beta} \bmod p$, and computes the value $e' = H(m, r') \bmod q$. He sends the "challenge" $e = e' + \beta \bmod q$ to the signer who returns the value $s$ such that $g^s y^e = r \bmod p$. One can easily verify that, with $s' = s - \alpha \bmod q$, $(e', s')$ is a valid Schnorr signature of $m$ since it satisfies $e' = H(m, g^{s'} y^{e'} \bmod p)$.

## 2 Security Proofs

### 2.1 The Random Oracle Model

In 1993, Bellare and Rogaway [1] formalized a model which allows proofs of security for various cryptographic schemes. Many of these algorithms use hash functions and cannot be proved secure from basic properties like one-wayness or collision freeness. Thus, hash functions are often an obstacle for proofs. In the random oracle model, hash functions are assumed to be really random functions and used as an oracle who answers a random value for each new query. Thus the obstacle disappears. The price to pay is the replacement of the hash function by some "ideal" object. Nevertheless, we feel that the resulting proof is a way to validate the design of a cryptographic scheme and to eliminate "poor" designs.

For example, in their paper [22], Pointcheval and Stern suggested that the original El Gamal's signature scheme [11] and DSS [19] did not follow a "good" design principle. This is in contrast with the Schnorr's signature scheme or, more generally, any transformation of a fair verifier zero-knowledge identification scheme, which are validated by a proof in the random oracle model. For the DSS design, Vaudenay [25] later showed a weakness which opens the way to a possible misuse of this scheme by the authority.

### 2.2 The Security of Signature Schemes

In recent years, general techniques for proving the security of signature schemes have been proposed. We refer the reader to [16] for the various definitions of security. The most general one is the "no-existential forgery under adaptively chosen-message attacks". It corresponds to a scenario where an attacker can ask the signature of new messages at any step of his computation and, still, is not be able to forge a new valid message–signature pair at the end. Both the RSA [23] and the Schnorr [24] signature schemes have been proved secure in the random oracle model. Proofs were given in the asymptotic framework of complexity theory. More recently, Bellare and Rogaway [2] modified the original RSA scheme in order to obtain an exact security result. At the same time, Pointcheval and Stern [22] obtained a proof of security for any signature scheme which comes from a fair verifier zero-knowledge identification scheme and also for a slight modification of El Gamal [11]. In these proofs, all entities are seen as probabilistic polynomial time Turing machines. Assuming that the attack exists, a collusion between the signer, the attacker and the random oracle, allows to construct a new Turing machine which solves a difficult problem (RSA or the discrete logarithm).

### 2.3 The Security of Blind Signatures

As far as we know, no formal notion of security has ever been studied, nor proved, in the context of blind signatures. However, it is a critical point in E-cash systems. In the context of blind signatures, the previous definitions of security are no longer significant. In fact, the existential forgery under an adaptively chosen-message is somehow the basis for blind signatures. Nevertheless, a fundamental property for E-cash systems is the guaranty that a user cannot forge more coins than the Bank gives him. In other words, after $\ell$ blind signatures of the Bank, the user must not be able to create more than $\ell$ coins. This form of security was more or less informally assumed in connection with several schemes, for example [5].

**Definition 1 (The "one-more" forgery).** For any integer $\ell$, an $(\ell, \ell+1)$-forgery comes from a probabilistic polynomial time Turing machine $\mathcal{A}$ that can compute, after $\ell$ interactions with the signer $\Sigma$, $\ell+1$ signatures with non-negligible probability. The "one-more forgery" is an $(\ell, \ell+1)$-forgery for some integer $\ell$.

As usual, an attacker has several methods to achieve this forgery. We will focus on two kinds of attacks :

- the sequential attack: the attacker interacts sequentially with the signer.
- the parallel attack: the attacker interacts $\ell$ times in parallel with the signer. This attack is stronger. Indeed, the attacker can initiate new interactions with the signer before previous ones have been computed.

Previous methods of proofs used to establish the security of signature schemes no longer work since, during the collusion between the signer, the attacker and the random oracle, we loose control over the message that the signer receives since it comes from the attacker. As a consequence, the signer cannot be simulated without the secret key.

## 3 The Proposed Blind Signature Scheme

### 3.1 Witness Indistinguishability

In the following, we will focus on a specific three-pass "witness indistinguishable" identification scheme, and its transformation into a blind signature scheme. The notion of "witness indistinguishability" was defined by Feige and Shamir in [12] for the purpose of identification. In such a scheme, many secret keys are associated to a same public key. Furthermore, the views of two identifications using two distinct secret keys associated to a same public key are indistinguishable. For example, in the Fiat-Shamir protocol [15], the verifier cannot distinguish which square root the prover uses. Okamoto, in [21], proposed a witness indistinguishable adaptation of both the Schnorr [24] and the Guillou-Quisquater [17] identification schemes.

### 3.2 Provably Secure Blind Signature Schemes

As was already remarked, the technical difficulty to overcome comes from the fact that, in the colluding step, we no longer can simulate the signer without the secret key. We will use a scheme which admits more than one secret key for a given public key. This will make the collusion possible and we will constrain the attacker to output a different secret key.

Our candidate scheme is one of the schemes designed by Okamoto in [21]. For the reader's convenience, the adaptation of the Schnorr's scheme is on figure 2 and its blind version is on figure 3.

| Prover | | Verifier |
|---|---|---|
| $p$ and $q$ are prime integers such that $q \mid (p-1)$ | | |
| $g$ and $h$ are some elements of $(\mathbb{Z}/p\mathbb{Z})^\star$ of order $q$ | | |
| secrets : $r, s \in \mathbb{Z}/q\mathbb{Z}$ | | |
| public : $y = g^{-r}h^{-s} \bmod p$ | | |
| $t, u \in \mathbb{Z}/q\mathbb{Z}$ | | |
| $a = g^t h^u \bmod p$ | $\xrightarrow{\quad a \quad}$ | |
| | $\xleftarrow{\quad c \quad}$ | $c \in \mathbb{Z}/2^t\mathbb{Z}$ |
| $R = t + cr \bmod q$ | | |
| $S = u + cs \bmod q$ | $\xrightarrow{\quad R, S \quad}$ | |
| | | $a \stackrel{?}{=} g^R h^S y^c \bmod p$ |

**Fig. 2.** Witness indistinguishable adaptation of the Schnorr's identification

| Authority | | User |
|---|---|---|
| $p$ and $q$ are prime integers such that $q \mid (p-1)$ | | |
| $g$ and $h$ are some elements of $(\mathbb{Z}/p\mathbb{Z})^\star$ of order $q$ | | |
| secrets : $r, s \in \mathbb{Z}/q\mathbb{Z}$ | | |
| public : $y = g^{-r}h^{-s} \bmod p$ | | |
| $t, u \in \mathbb{Z}/q\mathbb{Z}$ | | |
| $a = g^t h^u \bmod p$ | $\xrightarrow{\quad a \quad}$ | |
| | | $\beta, \gamma, \delta \in \mathbb{Z}/q\mathbb{Z}$ |
| | | $\alpha = a g^\beta h^\gamma y^\delta \bmod p$ |
| | | $\varepsilon = H(m, \alpha)$ |
| | $\xleftarrow{\quad e \quad}$ | $e = \varepsilon - \delta \bmod q$ |
| $R = t + er \bmod q$ | | |
| $S = u + es \bmod q$ | $\xrightarrow{\quad R, S \quad}$ | |
| | | $a \stackrel{?}{=} g^R h^S y^e \bmod p$ |
| | | $\rho = R + \beta \bmod q$ |
| | | $\sigma = S + \gamma \bmod q$ |
| | Then $\alpha = g^\rho h^\sigma y^\varepsilon \bmod p$ | |

**Fig. 3.** Okamoto-Schnorr blind signature

### 3.3 Okamoto-Schnorr Blind Signature Scheme

The scheme uses two large primes $p$ and $q$ such that $q \mid (p-1)$, and two elements $g, h \in (\mathbb{Z}/p\mathbb{Z})^\star$ of order $q$. The Bank chooses a secret key $(r, s) \in ((\mathbb{Z}/q\mathbb{Z})^\star)^2$ and publishes the public key, $y = g^{-r} h^{-s} \bmod p$. The protocol by which the user obtains a blind signature of the message $m$ is as follows.

- the Bank chooses $(t, u) \in ((\mathbb{Z}/t\mathbb{Z})^\star)^2$, computes and sends $a = g^t h^u \bmod p$;
- the user chooses $\beta, \gamma, \delta \in \mathbb{Z}/q\mathbb{Z}$ to blind $a$ into $\alpha = a g^\beta h^\gamma y^\delta \bmod p$. He computes the challenge $\varepsilon = H(m, \alpha)$ and sends $e = \varepsilon - \delta \bmod q$ to the Bank;
- the Bank computes $R = t + er \bmod q$ and $S = u + es \bmod q$, and sends a pair $(R, S)$ which satisfies $a = g^R h^S y^e \bmod p$;
- the user computes $\rho = R + \beta \bmod q$ and $\sigma = S + \gamma \bmod q$.

Straightforward computations show that $\alpha = g^\rho h^\sigma y^\varepsilon \bmod p$, with $\varepsilon = H(m, \alpha)$.

A security proof for this scheme will be given below. It can be easily modified so as to cover other schemes that come from witness indistinguishable protocols. Especially, the blind Okamoto-Guillou-Quisquater signature scheme can be proposed (see figure 4) and proven relatively to the security of RSA.

| Authority | | User |
|---|---|---|
| | $N = pq$ and $\lambda$ prime and prime with $\varphi(N)$<br>$a \in (\mathbb{Z}/N\mathbb{Z})^\star$ of order greater than $\lambda$ | |
| secrets $r \in \{0, \ldots, \lambda - 1\}$<br>$s \in (\mathbb{Z}/N\mathbb{Z})^\star$<br>public $v = a^{-r} s^{-\lambda} \bmod N$<br>$t \in \{0, \ldots, \lambda - 1\}$<br>$u \in (\mathbb{Z}/N\mathbb{Z})^\star$<br>$x = a^t u^\lambda \bmod N$ | $\xrightarrow{\quad x \quad}$ | |
| | | $\alpha, \gamma \in \{0, \ldots, \lambda - 1\}$<br>$\beta \in (\mathbb{Z}/N\mathbb{Z})^\star$<br>$x' = x a^\alpha \beta^\lambda v^\gamma \bmod N$<br>$c' = H(m, x') \in \{0, \ldots, \lambda - 1\}$<br>$c = c' - \gamma \bmod \lambda$ |
| | $\xleftarrow{\quad c \quad}$ | |
| $y = t + cr \bmod \lambda$<br>$w = t + cr \div \lambda$<br>$z = a^w u s^c \bmod N$ | $\xrightarrow{\quad y, z \quad}$ | |
| | | $y' = y + \alpha \bmod \lambda$<br>$w' = y + \alpha \div \lambda$<br>$w'' = c' - c \div \lambda$<br>$z' = a^{w'} v^{-w''} z \beta \bmod N$ |
| | Then $x' = a^{y'} z'^\lambda v^{c'} \bmod N$ | |

**Fig. 4.** Okamoto-Guillou-Quisquater blind Signature

# 4 The Main Result

**Theorem 1.** *Consider the Okamoto-Schnorr blind signature scheme in the random oracle model. If there exists a probabilistic polynomial time Turing machine which can perform a "one-more" forgery, with non-negligible probability, even* *under a parallel attack, then the discrete logarithm can be solved in polynomial time.*

*Proof.* Before we prove this result, we state a well-known probabilistic lemma:

**Lemma 1 (The probabilistic lemma).** *Let $A$ be a subset of $X \times Y$ such that* $\Pr[A(x,y)] \geq \varepsilon$*, then there exists $\Omega \subset X$ such that*
*i)* $\Pr[x \in \Omega] \geq \varepsilon/2$
*ii) whenever $a \in \Omega$,* $\Pr[A(a,y)] \geq \varepsilon/2$.

With this lemma, we can split the set $X$ in two subsets, a non-negligible subset $\Omega$ consisting of "good" $x$'s which provide a non-negligible probability of success over $y$, and its complement, consisting of "bad" $x$'s.

We will first outline the proof, then, since the technicalities are a bit intricate, we will simplify notations. Finally, we will complete the proof.

*Outline of the Proof* Let $\mathcal{A}$ be the "attacker". It is a probabilistic polynomial time Turing machine which succeeds, in its "one-more forgery", with non-negligible probability $\varepsilon$. Thus, there exists an integer $\ell$ such that after $\ell$ interactions with the authority, $(a_i, e_i, R_i, S_i)$ for $i \in \{1, \dots, \ell\}$, and a polynomial number $Q$ of queries asked to the random oracle, $\mathcal{Q}_1, \dots, \mathcal{Q}_Q$, $\mathcal{A}$ returns $\ell + 1$ valid signatures, $(m_i, \alpha_i, \varepsilon_i, \rho_i, \sigma_i)$ for $i = 1, \dots, \ell+1$. These signatures verify the required equations with $\varepsilon_i = H(m_i, \alpha_i)$.

The public data consist of two large primes $p$ and $q$ such that $q \mid (p-1)$ and two elements, $g$ and $h$, of $(\mathbb{Z}/p\mathbb{Z})^\star$ of order $q$. The authority (or the Bank) possesses a secret key $(r,s)$ associated to public key $y = g^{-r}h^{-s}$, and a random tape $\Omega$. Formally, the secret key $(r,s)$ is stored in a specific part of the machine called the knowledge tape.

Through a collusion of the authority and the attacker, we want to compute the discrete logarithm of $h$ relatively to $g$. We will use the technique of oracle replay formalized in [22]. We first run the attack with random keys, tapes and oracle $f$. We randomly choose an index $j$. We then replay with the same keys and random tapes, but a different oracle $f'$ such that the $j-1$ first answers are unchanged. We expect that, with non-negligible probability, both executions output a common $\alpha_i$ coming from the $j^{th}$ oracle query having two distinct representations relatively to $g$ and $h$. In fact, $\alpha_i = g^r h^s = g^{r'} h^{s'}$, with $r' \neq r$, implies $\log_g h = (r - r')(s' - s)^{-1} \bmod q$. This collusion is represented on figure 5. Thus, the following lemma proves the theorem 1.

**Lemma 2 (The forking lemma).** *Randomly choose an index $j$, the keys and the random tapes. Run the attack twice with the same random tapes and two different random oracles, $f$ and $f'$, providing identical answers to the $j-1$ first queries. With non-negligible probability, the different outputs reveal two different representations of some $\alpha_i$, relatively to $g$ and $h$.*

*Cleaning up Notations* We now clear up notational difficulties. Firstly, without loss of generality, we can assume that all the $(m_i, \alpha_i)$ are queries which have been asked during the attack. Otherwise, the probability of success would be negligible because of the randomness of the random oracle outputs. Secondly,

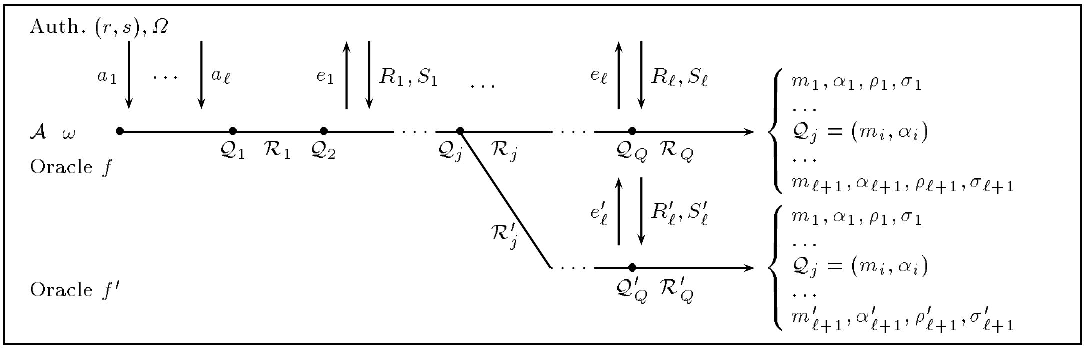


**Fig. 5.** Forking lemma

we can assume that the indexes, $(Ind_1, \ldots, Ind_{\ell+1})$, of $(m_1, \alpha_1), \ldots, (m_{\ell+1}, \alpha_{\ell+1})$ in the list of queries are constant. As a result, the probability of success decreases from $\varepsilon$ to $\rho \approx \varepsilon / Q^{\ell+1}$. The collusion is represented on figure 6, where the pair

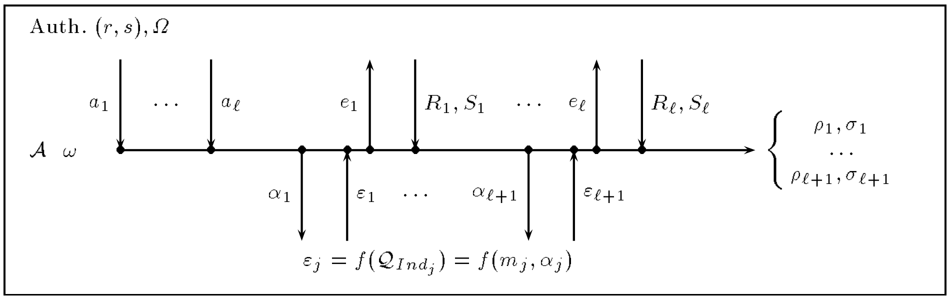


**Fig. 6.** General model

$(r, s)$ is the secret key used by the authority, and where the random tape $\Omega$ of the authority determines the pairs $(t_i, u_i)$ such that $a_i = g^{t_i} h^{u_i}$ for $i = 1, \ldots, \ell$. The distribution of $(r, s, y)$ where $r$ and $s$ are random and $y = g^{-r} h^{-s}$ is the same as the distribution of $(r, s, y)$ where $r$, $y$ are random and $s$ is the unique element in $(\mathbb{Z}/q\mathbb{Z})^\star$ such that $y = g^{-r} h^{-s}$. Accordingly, we will replace $(r, s)$ by $(r, y)$ and, similarly, each $(t_i, u_i)$ by $(t_i, a_i)$.

In the following, we will group $(\omega, y, a_1, \ldots, a_\ell)$ under variable $\nu$, and $\tau$ will represent the $\ell$-tuple $(t_1, \ldots, t_\ell)$. We will denote by $\mathcal{S}$ the set of all successful data, *i.e.* quadruples $(\nu, r, \tau, f)$ such that the attack succeeds. Then, $\Pr_{\nu,r,\tau,f}[(\nu, r, \tau, f) \in \mathcal{S}] \geq \rho$.

*Proof of the Forking Lemma* We want to prove that after a replay, we can obtain a common output $\alpha_i$ such that

$$\begin{aligned} \alpha_i &= g^{\rho_i} h^{\sigma_i} y^{\varepsilon_i} = g^{\rho_i - r\varepsilon_i} h^{\sigma_i - s\varepsilon_i} \\ &= g^{\rho'_i} h^{\sigma'_i} y^{\varepsilon'_i} = g^{\rho'_i - r\varepsilon'_i} h^{\sigma'_i - s\varepsilon'_i} \end{aligned} \text{ with } \rho_i - r\varepsilon_i \neq \rho'_i - r\varepsilon'_i.$$

We can remark that, for each $i$, $\alpha_i$ only depends on $\nu, r, \tau$ and the first $Ind_i - 1$ answers of $f$. The main question we have to study is whether or not the random variable $\chi_i = \rho_i - r\varepsilon_i$ is sensitive to queries asked at steps $Ind_i$, $Ind_i + 1$, etc. We expect that the answer is yes. A way to grasp the question is to consider the most likely value taken by this random variable when $(\nu, r, \tau)$ and the $Ind_i - 1$ first answers of $f$ are fixed. We are thus led to consider a function $c_i(\nu, r, \tau, f_i)$, where $f_i$ ranges over the set of answers to the first $Ind_i - 1$ possible queries. Set

$$\lambda_i(\nu, r, \tau, f_i, c) = \Pr_f \left[ \Big( \chi_i(\nu, r, \tau, f) = c \Big) \ \& \ \Big( (\nu, r, \tau, f) \in \mathcal{S} \Big) \Big| f \text{ extends } f_i \right].$$

We define $c_i(\nu, r, \tau, f_i)$ as any value $c$ such that $\lambda_i(\nu, r, \tau, f_i, c)$ is maximal. We then define the "good" subset $\mathcal{G}$ of $\mathcal{S}$ whose elements satisfy, for all $i$, $\chi_i(\nu, r, \tau, f) = c_i(\nu, r, \tau, f_i)$, where $f_i$ denotes the restriction of $f$ to queries of index strictly less than $Ind_i$, and the "bad" $\mathcal{B}$ its complement in $\mathcal{S}$.

**Definition 2.** We denote by $\Phi$ the transformation which maps any quadruple $(\nu, r, \tau, f)$ to $(\nu, r+1, \tau - e, f)$, where $\tau - e = (t_1 - e_1, \ldots, t_\ell - e_\ell)$.

This transformation has useful properties (see figure 7).

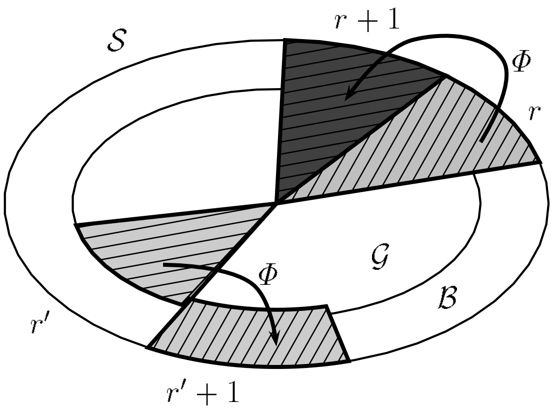


**Fig. 7.** Properties of $\Phi$

**Lemma 3.** *Both executions corresponding to $(\nu, r, \tau, f)$ and $\Phi(\nu, r, \tau, f)$ are totally identical w.r.t. the view of the attacker. Especially, outputs are the same.*

*Proof.* Let $(\nu, r, \tau, f)$ be an input for the collusion. Replay with $r' = r + 1$ and $\tau' = \tau - e$, the same $\nu$ and the same oracle $f$. The answers of the oracle are unchanged and the interactions with the authority become

$$R'_i(r', t'_i, e_i) = t'_i + r'e_i = (t_i - e_i) + (r+1)e_i = t_i + re_i = R_i(r, t_i, e_i).$$

Thus, everything remains the same.

**Corollary 1.** *$\Phi$ is a one-to-one mapping from $\mathcal{S}$ onto $\mathcal{S}$.*

The following lemma shows that $\Phi$ sends the set $\mathcal{G}$ into $\mathcal{B}$, except for a negligible part.

**Lemma 4.** *For fixed $(\nu, r, \tau)$, the probability*

$$\Pr_f[((\nu, r, \tau, f) \in \mathcal{G}) \,\&\, (\Phi(\nu, r, \tau, f) \in \mathcal{G})]$$

*is bounded by $1/q$.*

*Proof.* Assume that $\Pr_f[(\nu, r, \tau, f) \in \cup_{e_1,\ldots,e_\ell} Y(e_1, \ldots, e_\ell)] > 1/q$, where the set $Y(e_1, \ldots, e_\ell)$ is defined by the conditions $(\nu, r, \tau, f) \in \mathcal{G}$, $\Phi(\nu, r, \tau, f) \in \mathcal{G}$ and $(e_1, \ldots, e_\ell)$ are the successive questions asked to the authority. Then, there exists a $\ell$-tuple $(e_1, \ldots, e_\ell)$ such that $\Pr_f[Y(e_1, \ldots, e_\ell)] > \frac{1}{q^{\ell+1}}$. Thus, there exist two oracles $f$ and $f'$ in $Y(e_1, \ldots, e_\ell)$ which provide distinct answers for some queries $\mathcal{Q}_{Ind_j} = (m_j, \alpha_j)$ to the oracle, for some $j \in \{1, \ldots, \ell+1\}$, and are such that answers to queries not of the form $\mathcal{Q}_{Ind_j}$ are similar. We will denote by $i$ the smallest such index $j$. Then $f_i = f'_i$ and $\varepsilon_i \neq \varepsilon'_i$. Furthermore, we have $(\nu, r, \tau, f) \in \mathcal{G}$, $\Phi(\nu, r, \tau, f) \in \mathcal{G}$ and similarly $(\nu, r, \tau, f') \in \mathcal{G}$, $\Phi(\nu, r, \tau, f') \in \mathcal{G}$. Because of the property of $\Phi$ (see lemma 3), and by definition of $\mathcal{G}$,

$$\begin{aligned}
c_i(\nu, r, \tau, f_i) &= \rho_i(\nu, r, \tau, f) - r\varepsilon_i \\
&= \rho_i(\Phi(\nu, r, \tau, f)) - r\varepsilon_i = c_i(\nu, r{+}1, \tau\text{-}e, f_i) + ((r{+}1) - r)\varepsilon_i \\
c_i(\nu, r, \tau, f'_i) &= \rho_i(\nu, r, \tau, f') - r\varepsilon'_i \\
&= \rho_i(\Phi(\nu, r, \tau, f')) - r\varepsilon'_i = c_i(\nu, r{+}1, \tau\text{-}e', f'_i) + ((r{+}1) - r)\varepsilon'_i
\end{aligned}$$

The equality $f_i = f'_i$ implies $c_i(\nu, r, \tau, f_i) = c_i(\nu, r, \tau, f'_i)$. Since we have assume $(e_1, \ldots, e_\ell) = (e'_1, \ldots, e'_\ell)$, then $c_i(\nu, r+1, \tau - e, f_i)) = c_i(\nu, r+1, \tau - e', f'_i))$. Thus $\varepsilon_i = \varepsilon'_i$, which contradicts the hypothesis.

Lemma 4 says that for any $(\nu, r, \tau)$,

$$\Pr_f\left[\Big((\nu, r, \tau, f) \in \mathcal{G}\Big) \ \&\ \Big(\Phi(\nu, r, \tau, f) \in \mathcal{G}\Big)\right] \leq 1/q.$$

By making the sum over all triplets $(\nu, r, \tau)$, and using the bijectivity of $\Phi$ (corollary 1), we obtain

$$\begin{aligned}
\Pr[\mathcal{G}] &= \Pr_{\nu,r,\tau,f}\left[\Big((\nu, r, \tau, f) \in \mathcal{G}\Big) \ \&\ \Big(\Phi(\nu, r, \tau, f) \in \mathcal{G}\Big)\right] \\
&\quad + \Pr_{\nu,r,\tau,f}\left[\Big((\nu, r, \tau, f) \in \mathcal{G}\Big) \ \&\ \Big(\Phi(\nu, r, \tau, f) \in \mathcal{B}\Big)\right] \\
&\leq \frac{1}{q} + \Pr_{\nu,r,\tau,f}[\Phi(\nu, r, \tau, f) \in \mathcal{B}] \ \leq\ \frac{1}{q} + \Pr[\mathcal{B}]
\end{aligned}$$

Then, $\Pr[\mathcal{B}] \geq (\Pr[\mathcal{S}] - 1/q)/2$. Since $1/q$ is negligible w.r.t. $\Pr[\mathcal{S}]$, for enough large keys, we have, $\Pr[\mathcal{B}] \geq \Pr[\mathcal{S}]/3 \geq \rho/3$.

*Conclusion* We will use this probability to show the success of forking.

$$\begin{aligned}
\frac{\rho}{3} \ \leq\ \Pr[\mathcal{B}] &= \Pr_{\nu,r,\tau,f}\left[\mathcal{S} \ \&\ \Big((\exists i)\ \chi_i(\nu, r, \tau, f) \neq c_i(\nu, r, \tau, f_i)\Big)\right] \\
&\leq \sum_{i=1}^{\ell+1} \Pr_{\nu,r,\tau,f}\left[\mathcal{S} \ \&\ \Big(\chi_i(\nu, r, \tau, f) \neq c_i(\nu, r, \tau, f_i)\Big)\right].
\end{aligned}$$

There exists $k$ such that $\Pr\left[\mathcal{S} \ \&\ \Big(\chi_k(\nu, r, \tau, f) \neq c_k(\nu, r, \tau, f_k)\Big)\right] \geq \rho/3(\ell+1)$. Let us randomly choose the forking index $i$. With probability greater than $1/(\ell+1)$, we have guessed $i = k$. The probabilistic lemma 1 ensures that there exists a set $X$ such that

i) $\Pr_{\nu,r,\tau,f}[(\nu, r, \tau, f_i) \in X] \geq \rho/6(\ell+1)$;

ii) for all $(\nu, r, \tau, f_i) \in X$,

$$\Pr_f\left[(\nu, r, \tau, f) \in \mathcal{S} \ \&\ \Big(\chi_i \neq c_i\Big) \Big| f \text{ extends } f_i\right] \geq \rho/6(\ell+1).$$

Let us choose a random quadruple $(\nu, r, \tau, f)$. With probability greater than $\left(\rho/6(\ell+1)\right)^2$, $(\nu, r, \tau, f) \in \mathcal{S}$, $(\nu, r, \tau, f_i) \in X$ and $\chi_i(\nu, r, \tau, f) \neq c_i(\nu, r, \tau, f_i)$. We will denote by $d$ the value $\chi_i(\nu, r, \tau, f)$ and by $c$ the value $c_i(\nu, r, \tau, f_i)$.
Then, two cases appear relatively to $\lambda_i(\nu, r, \tau, f_i, d)$:
– if $\lambda_i(\nu, r, \tau, f_i, d) \geq \rho/12(\ell+1)$, then, by definition of $c_i$, we know that $\lambda_i(\nu, r, \tau, f_i, c) \geq \rho/12(\ell+1)$.
– otherwise,

$$\begin{aligned}
&\lambda_i(\nu, r, \tau, f_i, d) + \Pr_{f'}\left[\mathcal{S} \,\&\, \left(\chi_i(\nu, r, \tau, f') \neq d\right) \middle| f' \text{ extends } f_i\right] \\
&= \Pr_{f'}[\mathcal{S} \mid f' \text{ extends } f_i] \\
&\geq \Pr_{f'}\left[\mathcal{S} \,\&\, \left(\chi_i(\nu, r, \tau, f') \neq c\right) \middle| f' \text{ extends } f_i\right] \geq \rho/6(\ell+1).
\end{aligned}$$

Both cases lead to $\Pr_{f'}\left[\mathcal{S} \,\&\, \left(\chi_i(\nu, r, \tau, f') \neq d\right) \middle| f' \text{ extends } f_i\right] \geq \rho/12(\ell+1)$.
Thus, if we replay with the same keys and random tapes but another random oracle $f'$ such that $f'_i = f_i$, we obtain, with probability at least $\rho/12(\ell+1)$, a new success with $\chi_i(\nu, r, \tau, f') \neq d$. Then, both executions provide two different representations of $\alpha_i$ relatively to $g$ and $h$.

*Global Complexity of the Reduction* By using a replay oracle technique with a random forking index, the probability of success is greater than

$$\frac{1}{\ell+1} \times \left(\frac{\rho}{6(\ell+1)}\right)^2 \times \frac{\rho}{12(\ell+1)} = \frac{1}{2(\ell+1)} \times \left(\frac{1}{6(\ell+1)} \times \frac{\varepsilon}{Q^{\ell+1}}\right)^3$$

where $\varepsilon$ is the probability of success of an $(\ell,\, \ell+1)$-forgery and $Q$ the number of queries asked to the random oracle.

## 5 Conclusion

Our result appears to be the first security result which opens a way towards provably secure E-cash systems by providing candidates for secure blind signatures. However, an open problem still remains: the complexity of the reduction is polynomial in the size of the keys but exponential in $\ell$. We do not know whether it is possible to achieve polynomial time both in $\ell$ and the size of the keys.

## Acknowledgements

The definition of "one-more" forgery came up during a discussion with Stefan Brands. We thank him for the time he spent explaining his scheme.

## References

1. M. Bellare and P. Rogaway. Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. In *Proc. of the 1st CCCS*, pages 62–73. ACM press, 1993.
2. M. Bellare and P. Rogaway. The Exact Security of Digital Signatures – How to Sign with RSA and Rabin. In *Eurocrypt '96*, LNCS 1070, pages 399–416. Springer-Verlag, 1996.
3. S. A. Brands. An Efficient Off-line Electronic Cash System Based On The Representation Problem. Technical report, CWI, 1993. CS-R9323.

4. S. A. Brands. Untraceable Off-line Cash in Wallets with Observers. In *Crypto '93*, LNCS 773, pages 302–318. Springer-Verlag, 1994.
5. S. A. Brands. Off-Line Electronic Cash Based on Secret-Key Certificates. In *LATIN '95*, 1995.
6. D. Chaum. Blind Signatures for Untraceable Payments. In *Crypto '82*, pages 199–203. Plenum, NY, 1983.
7. D. Chaum. Security Without Identification: Transaction Systems to Make Big Brother Obsolete. *Communications of the ACM 28*, 10, October 1985.
8. D. Chaum. Privacy Protected Payments: Unconditional Payer And/Or Payee Untraceability. In *Smartcard 2000*, pages 69–93, 1989.
9. D. Chaum, B. den Boer, E. van Heyst, S. Mjlsnes, and A. Steenbeek. Efficient Off-line Electronic Checks. In *Eurocrypt '89*, LNCS 434, pages 294–301. Springer-Verlag, 1990.
10. D. Chaum, A. Fiat, and M. Naor. Untraceable Electronic Cash. In *Crypto '88*, LNCS 403, pages 319–327. Springer-Verlag, 1989.
11. T. El Gamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. In *IEEE Transactions on Information Theory*, volume IT–31, no. 4, pages 469–472, July 1985.
12. U. Feige and A. Shamir. Witness Indistinguishable and Witness Hiding Protocols. In *Proc. of the 22nd STOC*, pages 416–426. ACM Press, 1990.
13. N. Ferguson. Extensions of Single Term Coins. In *Crypto '93*, LNCS 773, pages 292–301. Springer-Verlag, 1994.
14. N. Ferguson. Single Term Off-Line Coins. In *Eurocrypt '93*, LNCS 765, pages 318–328. Springer-Verlag, 1994.
15. A. Fiat and A. Shamir. How to Prove Yourself: practical solutions of identification and signature problems. In *Crypto '86*, LNCS 263, pages 186–194. Springer-Verlag, 1987.
16. S. Goldwasser, S. Micali, and R. Rivest. A Digital Signature Scheme Secure Against Adaptative Chosen-Message Attacks. *SIAM Sournal of Computing*, 17(2):281–308, April 1988.
17. L. C. Guillou and J.-J. Quisquater. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. In *Eurocrypt '88*, LNCS 330, pages 123–128. Springer-Verlag, 1988.
18. M. Jakobsson and M. Yung. Revokable and Versatile Electronic Money. In *Proc. of the 3rd CCCS*, pages 76–87. ACM press, 1996.
19. NIST. Digital Signature Standard (DSS). Federal Information Processing Standards PUBlication 186, November 1994.
20. K. Ohta and T. Okamoto. Universal Electronic Cash. In *Crypto '91*, LNCS 576, pages 324–337. Springer-Verlag, 1992.
21. T. Okamoto. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In *Crypto '92*, LNCS 740, pages 31–53. Springer-Verlag, 1992.
22. D. Pointcheval and J. Stern. Security Proofs for Signature Schemes. In *Eurocrypt '96*, LNCS 1070, pages 387–398. Springer-Verlag, 1996.
23. R. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM*, 21(2):120–126, February 1978.
24. C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *Crypto '89*, LNCS 435, pages 235–251. Springer-Verlag, 1990.
25. S. Vaudenay. Hidden Collisions on DSS. In *Crypto '96*, LNCS 1109, pages 83–88. Springer-Verlag, 1996.
26. S. von Solms and D. Naccache. On Blind Signatures and Perfect Crimes. *Computers & Security*, 11:581–583, 1992.