New Blind Signatures Equivalent to Factorization

(Extended Abstract)

David Pointcheval *

Jacques Stern †

Abstract

In this paper, we present new blind signature schemes based on the factorization problem. They are the first blind signature schemes proved secure relatively to factorization. By security, we mean that no "one-more forgery" is possible even under a parallel attack. In other terms, a user that receives k electronic coins cannot manufacture $k+1$. Those security definitions have been introduced by Pointcheval and Stern [18] for use in electronic cash. In fact, blind signatures were defined with this aim and it is still their most important application, together with anonymous voting. In the following, we will present an efficient reduction of an attack to a factorization algorithm in the random oracle model [1].

1 Introduction

1.1 Electronic cash and blind signatures

In 1982, David Chaum's [8] pioneering work was devoted to create an electronic version of money. To this aim, he introduced the notions of "coins" and "randomized blind signatures" (or simply "blind signatures"). He claimed that it was the only one way to ensure anonymity. In fact, in real life, a coin cannot be easily traced from the bank to the shop. Furthermore, two spendings of a same user cannot be linked together. These are two privacy properties of real coins that Chaum wanted to obtain: untraceability and unlinkability.

In his first scheme, Chaum used blind signatures for the production of coins. The user makes the Bank sign, blindly, a coin. Then the user is in possession of a valid coin that the Bank itself cannot recognize nor link with the user. When the user spends the coin, the shop immediately returns it to the Bank. If the coin has already been spent, the Bank detects it and informs the shop so that it refuses payment. It is an "on-line" context. There is a continuous communication between the shop and the Bank in order to verify the validity of coins. For this scheme, Chaum defined the first blind signature, based on the RSA hypothesis. It is a by now classical transformation of the original RSA signature scheme [20] :

- The Bank has a large composite number n, a public key e, and a related secret key d. It also uses a public hash function H.
- The signature of a public message m is the e^{th} root of $H(m)$,
$$\sigma = H(m)^{1/e} = H(m)^d \bmod n.$$
- A coin is the concatenation of a number ρ, and its signature by the Bank. In order to ensure untraceability, the user needs a signature that the Bank won't be able to recognize later. He "blinds" it with a random value $r^e \bmod n$, and sends $m = H(\rho)r^e \bmod n$ to the signer. The latter returns a signature σ' of m such that ${\sigma'}^e = m = r^e H(\rho) \bmod n$. A coin is any pair (ρ, σ) which satisfies $\sigma^e = H(\rho) \bmod n$.

In this scheme, all coins have the same value, but in a real system, different values might be encoded by different exponents e.

in an "off-line" context, we cannot prevent a user from spending twice or more a coin. This fraud is called "double-spending", or more generally "over-spending". The only thing we can do is to discover the double-spender and punish him. Chaum, Fiat and Naor [9] opened a way in this direction by introducing the identity in the coin in such a way that it remains concealed, unless double spending happens. One more time, blind signatures were a critical point for anonymity, and as before, the authors used the blind RSA signature, together with the "cut-and-choose" technique :

- The Bank has a large composite number n, a public key $e = 3$, and a secret key d, the inverse of 3 modulo $\varphi(n)$. It uses two public two-parameters one-way functions f and g.
- A coin is the product π of k numbers t_i, which are blind signatures of $f(x_i, y_i)$, of the form $f(x_i, y_i)^d$, where k is the security parameter. Furthermore, for each i, $x_i = g(a_i, c_i)$ and $y_i = g(b_i, c_i \oplus I)$, where a_i, b_i and c_i are random values, and I is the identity of the user.

$$\pi = \prod_{i=1}^{i=k} t_i = \prod_{i=1}^{i=k} f(x_i, y_i)^d \bmod N.$$

* David.Pointcheval@ens.fr

† Jacques.Stern@ens.fr

Laboratoire d'Informatique, École Normale Supérieure, 45, rue d'Ulm, F – 75230 PARIS Cedex 05

Proceedings of the 4th ACM Conference on Computer and Communications Security. Pages 92–99. (april 1 – 4, 1997, Zurich, Switzerland)

- To spend such a coin, Alice receives a "challenge" $d \in \{0,1\}^k$ from the shopkeeper, Bob. For each i, Alice returns an answer. In case $d_i = 0$, Alice sends a_i, c_i and y_i, and Bob can compute $x_i = g(a_i, c_i)$ and $\tau_i = f(x_i, y_i)$. In case $d_i = 1$, Alice sends b_i, $c_i \oplus I$ and x_i, and Bob can compute $y_i = g(b_i, c_i \oplus I)$ and $\tau_i = f(x_i, y_i)$. Then he checks whether the equality $\pi^3 = \prod \tau_i \bmod n$ is satisfied. Only the Bank could have produced such a product.
- In case of double-spending, with high probability, two different challenges are asked. This means that there exists i such that $d_i \neq d'_i$. Then Alice has to reveal c_i and $c_i \oplus I$, therefore anonymity disappears.
- To allow detection of double-spending, the coin has to respect the previous described form. In particular, the identity I must be correct. An attacker has no reason to be honest and may not follow the rules. The Bank has to control the structure of the coins. To do so, the Bank asks Alice to produce $2k$ numbers t_i, during this communication, the Bank chooses k of them to control the structure. Those values are no longer anonymous so that Alice throws them away and computes the coins with the k other values. The probability for a cheater to finally be in possession of a fraudulous coin is about 2^{-2k}.

The problem of the "cut-and-choose" technique is that coins are very large, as well as the amount of computations. Then, in 1993, Ferguson [12] and Brands [3] proposed new schemes without "cut-and-choose". The first one use once again the blind RSA signature whereas the Brands' scheme uses a new blind signature derived from the Schnorr's signature scheme [21] :

- Two large prime integers p and q are given 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, $x \in \mathbb{Z}/q\mathbb{Z}$, the secret one, and $y = g^{-x} \bmod p$, the public one. He publishes y.
- The signature of a secret message m is obtained as follows: First, Alice asks the signer to initiate a communication. The signer chooses a random $k \in \mathbb{Z}/q\mathbb{Z}$, computes and sends the "commitment" $r = g^k \bmod p$. Then, Alice blinds this value with two random elements $\alpha, \beta \in \mathbb{Z}/q\mathbb{Z}$, into $r' = rg^{-\alpha}y^{-\beta} \bmod p$, and computes the value $e' = H(m, r') \bmod q$. She sends the "challenge" $e = e' + \beta \bmod q$ to the signer who returns the value s such that $g^s y^e = r \bmod p$. Finally, she computes $s' = s - \alpha \bmod q$. This way, (e', s') is a valid Schnorr signature of m since it satisfies

$$e' = H(m, g^{s'} y^{e'} \bmod p).$$

In both schemes, Ferguson and Brands manage to hide the identity of the user in coins, in such a way it is revealed after a double-spending, without any kind of "cut-and-choose" methodology. Many extensions [11, 2, 6], attacks [4, 7] and repairs [5, 22] have been proposed. All of them use blind signatures, and the security of proposed schemes is totally dependent of the security of the blind signatures used. Surprisingly, no security proofs have been proposed for those blind signatures.

1.2 Security

Recently, Pointcheval and Stern [18] suggested a design for provably secure blind signatures. Their candidates are based on the "witness indistinguishable" [10] adaptation of the Schnorr's [21] and Guillou-Quisquater's [14, 15] identification schemes by Okamoto [16]. Furthermore their definition of security directly comes from electronic cash applications. They define two notions, the "one-more forgery" under "sequential" and "parallel" attacks (see figure 1).

Definition 1 (The "one-more forgery"). For any fixed ℓ, if an attacker $\mathcal{A}$ is able to compute, after ℓ interactions with the signer Σ, $\ell+1$ signatures with non-negligible probability, we say that it has performed an $(\ell, \ell+1)$-forgery. A "one-more forgery" is an $(\ell, \ell+1)$-forgery for some integer ℓ.

This definition comes from the natural property needed for any electronic cash system: if the Bank helps Alice to produce ℓ coins, then, after those interactions Alice must not hold more than ℓ coins. The Bank wants to be sure of the amount of money in circulation.

Definition 2 (Attacks). Two different attacks can be considered:

- the sequential attack where the attacker sequentially interacts with the signer.
- the parallel attack where the attacker can interact ℓ times with the signer and send the challenges whenever he wants.
  This attack is stronger. Indeed, the attacker can initiate new interactions with the signer before previous ones have been completed. Furthermore, the sequential attack is a particular case of the parallel one.

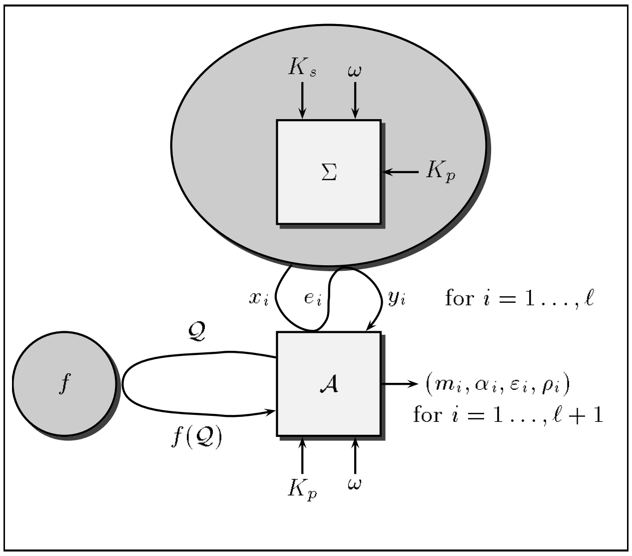

Figure 1: The $(\ell, \ell+1)$-forgery

Those definitions are related with the two scenarios for withdrawing money. We can assume that the Bank has only one communication line and cannot produce more than one coin at the same time. It is a great constraint for users and for attackers too. A much more suitable situation is the possibility to withdraw many coins at the same time, in parallel. This property can be used by the attacker.

1.3 Previous results

The technique used by Pointcheval and Stern [18] for their proof can be applied on both "witness indistinguishable" adaptations of Okamoto because, in both schemes, public keys have many secret keys associated. The results are given in the so-called "random oracle model" formalized by Bellare and Rogaway [1]. They simply assume that hash functions are really random, but this is now a current assumption.

Theorem 3. *Consider the Okamoto — Schnorr blind signature scheme (see figure 2) in the random oracle model. A "one-more forgery", even under a parallel attack, is equivalent to the discrete logarithm problem in a subgroup.*

Theorem 4. *Consider the Okamoto — Guillou–Quisquater blind signature scheme (see figure 3) in the random oracle model. A "one-more forgery", even under a parallel attack, is equivalent to the RSA problem.*

2 A new scheme

As we see, the provably secure schemes already known are related to the discrete logarithm problem or to RSA. In search for a scheme with the same security level as factorization, we consider the well-known "witness indistinguishable" protocol of Fiat-Shamir [13] with multiple secrets presented on figure 4.

On figure 5, the blind signature adapted from the Fiat-Shamir identification scheme appears. For this new scheme, with a slightly more technical proof than the one given by Pointcheval and Stern [18], we could obtain the following result.

Theorem 5. *Consider the Fiat-Shamir blind signature scheme (see figure 5) in the random oracle model. A "one-more forgery", even under a parallel attack, is equivalent to factorization.*

Proof (sketch). For the proof, we can present an efficient transformation of an attacker who performs a "one-more forgery" into an algorithm which factorizes Blum integers. A Blum integer N is a product of two primes p and q equal to 3 modulo 4. The property of such integers is that in $(\mathbb{Z}/N\mathbb{Z})^\star$, 1 has four square roots, $T_0 = 1, T_1 = T, T_2 = -1$ and $T_3 = -T$, and among these square roots, 1 is the only one to be a square. These square roots define a residuosity function C: for any $x \in (\mathbb{Z}/N\mathbb{Z})^\star$, $C(x) = i$ such that T_i/x is a square. We also define the binary residuosity, by $\eta(x) = C(x) \bmod 2$. This function satisfies the relation, for any $x, y \in (\mathbb{Z}/N\mathbb{Z})^\star$, $\eta(xy) = \eta(x) \oplus \eta(y)$. Furthermore, if we know x and y such that $x^2 = y^2 \bmod N$ with $\eta(x) \neq \eta(y)$, then $\gcd(x - y, N) \in \{p, q\}$ and thus we can factor N.

We assume we have an attacker $\mathcal{A}$ who succeeds, in his "one-more forgery", with non-negligible probability. Thus, there exists an integer ℓ such that after ℓ interactions with the authority, (x_i, e_i, y_i) for $i \in \{1, \ldots, \ell\}$, and Q queries asked to the hash function, $\mathcal{Q}_1, \ldots, \mathcal{Q}_Q$, $\mathcal{A}$ returns $\ell + 1$ valid signatures, $(m_i, \alpha_i, \varepsilon_i, \rho_i)$ for $i = 1, \ldots, \ell + 1$. Those signatures can be seen as valid coins which satisfy

$$\alpha_i = \rho_i^2 \prod_{j=1}^{j=k} V_j^{-\varepsilon_{i,j}} \bmod N.$$

We will create random secret keys, compute the associated public keys and finally use this attacker to find two square roots x and y of a single element with distinct binary residuosity, $\eta(x) \neq \eta(y)$.

Let $(S_j)_{j\in[1,k]}$ be such random secret keys. Changing their sign, we can assume that thay are between 0 and $N/2$. This does not change the binary residuosity. We compute the squares V_j. We denote by r the bit string defined by $r_j = \eta(S_j)$ for $j = 1, \ldots, k$. It is easy to remark that an attack is characterized by the random tapes of the attacker, ω, and of the signer, Ω, by the V_j and r, and by the hash function f. We will group ω, and the V_j under variable ν. The random tape Ω only defines the t_j that we regroup under the variable τ.

We play the attack (ν, r, τ, f) and obtain valid signatures $(m_i, \alpha_i, \varepsilon_i, \rho_i)$ for $i = 1, \ldots, \ell + 1$. Because of the unpredictability of the images of f, if the signatures are valid, we can assume that for each i, there exists and index Ind_i such that $\mathcal{Q}_{Ind_i} = (m_i, \alpha_i)$. We choose a random i and play again the attack with ν, r, τ and a hash function f' whose answers are the same as those of f but for $\mathcal{Q}_{Ind_i}$, $\mathcal{Q}_{Ind_i+1}$, ..., using the "oracle replay" technique [19]. We will not detail the proof, but with non-negligible probability, we obtain another success with $\mathcal{Q}'_{Ind_i} = (m_i, \alpha_i)$, but $\varepsilon'_i = f'(\mathcal{Q}'_{Ind_i}) \neq f(\mathcal{Q}_{Ind_i}) = \varepsilon_i$. Because of their validity, both i^{th} signatures satisfy

$$\rho_i^2 \prod_{\varepsilon_{i,j}=1} V_j^{-1} = \alpha_i = \rho'^2_i \prod_{\varepsilon'_{i,j}=1} V_j^{-1} \bmod N.$$

By an easy division, we obtain

$$\left(\rho_i^{-1} \prod_{\varepsilon_{i,j}=1} S_j\right)^2 = \left(\rho'^{-1}_i \prod_{\varepsilon'_{i,j}=1} S_j\right)^2 \bmod N$$

We only have to hope that

$$\left(\bigoplus_{\varepsilon_{i,j}=1} \eta(S_j)\right) \oplus \eta(\rho_i) = \left(\varepsilon_i \odot r\right) \oplus \eta(\rho_i)$$
$$\neq \left(\varepsilon'_i \odot r\right) \oplus \eta(\rho_i) = \left(\bigoplus_{\varepsilon'_{i,j}=1} \eta(S_j)\right) \oplus \eta(\rho'_i),$$

where $\odot$ is the dot product modulo 2. We thus define, for each i, the variable $\chi_i(\nu, r, \tau, f) = \left(\varepsilon_i \odot r\right) \oplus \eta(\rho_i)$. The main question we have to study is whether or not the random variable χ_i is sensitive to queries asked at steps Ind_i, $Ind_i + 1$, etc. We expect that the answer is yes. Following the idea of the Pointcheval and Stern's proof, we can define the following transformations:

Definition 6. For any $j \in \{1, \ldots, k\}$, we denote by Φ_j the transformation which maps any quadruple (ν, r, τ, f) to (ν, r', τ', f), where

$$\begin{aligned} r' &= r_1 \ldots r_{j-1} \bar{r}_j r_{j+1} \ldots r_k \\ \tau' &= (t'_1, \ldots, t'_k) \text{ with } t'_i = t_i T^{e_{i,j}} \bmod N. \end{aligned}$$

One can verify that executions corresponding to (ν, r, τ, f) and $\Phi_j(\nu, r, \tau, f)$ for any j are the same with respect to the view of the user. From this point, using a similar technique as Pointcheval and Stern [18] but with the k transformations Φ_j, we can prove that their exists an index i such that the random variable χ_i is sensitive to queries asked at steps Ind_i, $Ind_i + 1$, etc.

Authority		User

p and q are prime integers such that $q|(p-1)$

g and h are some elements of $(\mathbb{Z}/p\mathbb{Z})^\star$ of order q

Authority		User
secrets : $r, s \in \mathbb{Z}/q\mathbb{Z}$		
public : $y = g^{-r}h^{-s} \bmod p$		
$t, u \in \mathbb{Z}/q\mathbb{Z}$		
$a = g^t h^u \bmod p$	$\xrightarrow{a}$	
		$\beta, \gamma, \delta \in \mathbb{Z}/q\mathbb{Z}$
		$\alpha = ag^\beta h^\gamma y^\delta \bmod p$
		$\varepsilon = f(m, \alpha)$
	$\xleftarrow{e}$	$e = \varepsilon - \delta \bmod q$
$R = t + er \bmod q$		
$S = u + es \bmod q$	$\xrightarrow{R, S}$	
		$a \stackrel{?}{=} g^R h^S y^e \bmod p$
		$\rho = R + \beta \bmod q$
		$\sigma = S + \gamma \bmod q$

Then $\alpha = g^\rho h^\sigma y^\varepsilon \bmod p$

Figure 2: Okamoto – Schnorr blind signature scheme

Authority		User

$N = pq$ and λ prime and prime with $\varphi(N)$

$a \in (\mathbb{Z}/N\mathbb{Z})^\star$ of order greater than λ

Authority		User
secrets $r \in \{0, \ldots, \lambda - 1\}$		
$s \in (\mathbb{Z}/N\mathbb{Z})^\star$		
public $v = a^{-r}s^{-\lambda} \bmod N$		
$t \in \{0, \ldots, \lambda - 1\}, u \in (\mathbb{Z}/N\mathbb{Z})^\star$		
$x = a^t u^\lambda \bmod N$	$\xrightarrow{x}$	
		$\alpha, \gamma \in \{0, \ldots, \lambda - 1\}$
		$\beta \in (\mathbb{Z}/N\mathbb{Z})^\star$
		$x' = xa^\alpha \beta^\lambda v^\gamma \bmod N$
		$c' = f(m, x') \in \{0, \ldots, \lambda - 1\}$
	$\xleftarrow{c}$	$c = c' - \gamma \bmod \lambda$
$y = t + cr \bmod \lambda$		
$w = t + cr \div \lambda$		
$z = a^w u s^c \bmod N$	$\xrightarrow{y, z}$	
		$y' = y + \alpha \bmod \lambda$
		$w' = y + \alpha \div \lambda$
		$w'' = c' - c \div \lambda$
		$z' = a^{w'} v^{-w''} z\beta \bmod N$

Then $x' = a^{y'} z'^\lambda v^{c'} \bmod N$

Figure 3: Okamoto – Guillou-Quisquater blind signature scheme

Authority		User
	$N = pq$, product of two large primes	
secrets $S_i \in (\mathbb{Z}/N\mathbb{Z})^\star$ for $i \in \{1, \ldots, k\}$		
public $V_i = S_i^2 \bmod N$		
$t \in (\mathbb{Z}/N\mathbb{Z})^\star$		
$x = t^2 \bmod N$	$\xrightarrow{\quad x \quad}$	
	$\xleftarrow{\quad c \quad}$	$c = (c_1, \ldots, c_k) \in \{0,1\}^k$
$y = t \prod_{i=1}^{i=k} S_i{}^{c_i} \bmod N$	$\xrightarrow{\quad y \quad}$	
		$y^2 \stackrel{?}{=} x \prod_{c_i=1} V_i \bmod N$

Figure 4: Fiat – Shamir identification scheme

Authority		User
	$N = pq$, product of two large primes $k \gg \log n$ where $n = \log N$	
secrets $S_i \in (\mathbb{Z}/N\mathbb{Z})^\star$ for $i \in \{1, \ldots, k\}$		
public $V_i = S_i^2 \bmod N$		
$t \in (\mathbb{Z}/N\mathbb{Z})^\star$		
$x = t^2 \bmod N$	$\xrightarrow{\quad x \quad}$	
		$\beta \in (\mathbb{Z}/N\mathbb{Z})^\star$ $\gamma_1 \ldots \gamma_k \in \{0,1\}^k$ $\alpha = x\beta^2 \prod_{\gamma_i=1} V_i \bmod N$
		$\varepsilon_1 \ldots \varepsilon_k = f(m, \alpha) \in \{0,1\}^k$
	$\xleftarrow{\quad e \quad}$	$e = \gamma \oplus \varepsilon$
$y = t \prod_{i=1}^{i=k} S_i{}^{e_i} \bmod N$	$\xrightarrow{\quad y \quad}$	
		$y^2 \stackrel{?}{=} x \prod_{i=1}^{i=k} V_i{}^{e_i} \bmod N$
		$\rho = y\beta \prod_{\gamma_i > e_i} V_i \bmod N$
	Then $\alpha = \rho^2 \prod_{i=1}^{i=k} V_i{}^{-\varepsilon_i} \bmod N$	

Figure 5: Fiat – Shamir blind signature scheme

Then, if we have guessed the good index i, with non negligible probability we obtain two elements

$$\begin{aligned} z &= \rho_i^{-1} \prod_{\varepsilon_{i,j}=1} S_j \bmod N \\ z' &= \rho_i'^{-1} \prod_{\varepsilon'_{i,j}=1} S_j \bmod N, \end{aligned}$$

such that $z^2 = z'^2 \bmod N$ and $\eta(z) \neq \eta(z')$, which concludes the proof. A much more complete proof will be given in the full paper. □

3 Extensions

Since the appearance of the Fiat-Shamir identification, several variants have been proposed. The most well known are those of Guillou-Quisquater [14, 15] and Ong-Schnorr [17]. They are both extensions with exponents greater than 2 in order to reduce the amount of interactions.

Guillou and Quisquater more or less suggested that the exponent has to be prime and to not divide the order of the multiplication group, $\varphi(N) = (p-1)(q-1)$. Their protocol becomes equivalent to RSA. Ong and Schnorr suggested to use exponents of the form 2^k, which are clearly not prime nor prime with $\varphi(N)$. Recently, Shoup [23] proved that the Ong-Schnorr scheme with large exponents k is secure against active attacks if N is a Blum integer. This scheme can be easily transformed for blind signatures, as presented on figure 6.

About this new and efficient blind signature scheme we can say:

Theorem 7. *Consider the Ong – Schnorr blind signature scheme (see figure 6) in the random oracle model. A "one-more forgery", under a sequential attack, is equivalent to factorization.*

Proof (Sketch). The proof, which will be much more complete in the full paper, provides, like in the Shoup's one [23], a non-uniform reduction between an attacker and an algorithm to factor Blum integers.

Assume that we are given an attacker $\mathcal{A}$ who succeeds, in his "one-more forgery" under a sequential attack, with non-negligible probability $\varepsilon \geq 1/P$. In other words, after ℓ sequential interactions, (x_i, e_i, y_i) for i in $\{1, \ldots, \ell\}$, with the signer and Q queries $\mathcal{Q}_1, \ldots, \mathcal{Q}_Q$, to the hash function, $\mathcal{A}$ can return $\ell + 1$ valid signatures $(m_i, \alpha_i, \varepsilon_i, \rho_i)$ for i in $\{1, \ldots, \ell+1\}$ which satisfy $\rho_i^{2^k} = \alpha_i I^{\varepsilon_i} \bmod N$. As previously seen, w.l.o.g. we can assume that there exist indexes $Ind_1, \ldots, Ind_{\ell+1}$ such that $(m_i, \alpha_i) = Q_{Ind_i}$ for $j = i, \ldots, \ell+1$. Furthermore, there exist indexes $j_1, \ldots, j_{\ell+1}$ such that

$$\Pr[\text{Success and } Ind_i = j_i\ \forall i] \geq \frac{1}{PQ^{\ell+1}}.$$

If we randomly choose those indexes, then, with probability greater than $1/Q^{\ell+1}$ we have chosen good ones. Then, with a similar technique as the Pointcheval and Stern's one, we can choose a forking index β. But we cannot really play the attack with a real secret key. We need to use, as Shoup made, a pseudo-secret-key S', and compute the public one $I = S'^{2^{k-\lambda}} \bmod N$ with $\lambda = \lceil \log(\ell PQ^{\ell+1}) + 1 \rceil$ (since $k \gg \log n$, for an enough large n, $k > \lambda$). Then, the simulation of the signer, presented by Shoup, cannot succeed each time, but a reset when a failure happens provides a polynomial simulation. Now, we can play the attack and play again with a fork at the β^{th} answer of the hash function. With non-negligible probability, $\varepsilon_\beta \neq \varepsilon'_\beta \bmod 2^\lambda$ but

$$\alpha_\beta = \rho_\beta^{2^k} I^{-\varepsilon_\beta} = \rho'^{2^k}_\beta I^{-\varepsilon'_\beta} \bmod N.$$

If we let

$$\begin{aligned} 2^t u &= \varepsilon'_\beta - \varepsilon_\beta, \text{ necessarily } t < \lambda, \\ \text{and} \quad z &= (\rho'_\beta / \rho_\beta)^{2^{\lambda - t}} \bmod N, \end{aligned}$$

then $I^{2^t u} = z^{2^{k-\lambda+t}} \bmod N$. Clearly, this implies

$$I^u = (S'^u)^{2^{k-\lambda}} = z^{2^{k-\lambda}} \bmod N,$$

and $z^2 = \left(S'^u\right)^2 \bmod N$. Then, we can remark that z is a quadratic residu, and S'^u has a random residuosity (the same as S'). With probability of an half, S'^u and z provide a factor of N. □

We must remark that the proof only provides the security against sequential attacks because of the simulator which succeeds in the signature with a polynomially small probability.

Furthermore, the reduction has a polynomial but very large complexity. Nevertheless, the scheme admits a proof of security that very few schemes have.

4 Conclusion

Our new blind signature schemes are the first ones to be proved as secure as factorization. Because of the importance of blind signatures in electronic cash systems, those schemes may open new ways to build secure E-cash protocols. According to the prevailing scenario, one can use the Fiat-Shamir blind signature scheme if the security against parallel attacks is needed, or the much more efficient Ong-Schnorr blind signature scheme if security against sequential attacks is enough.

References

[1] Bellare, M., and Rogaway, P. Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. In *Proc. of the 1st CCCS* (1993), ACM press, pp. 62–73.

[2] Brands, S. A. An Efficient Off-line Electronic Cash System Based On The Representation Problem. Tech. rep., CWI, 1993. CS-R9323.

[3] Brands, S. A. Untraceable Off-line Cash in Wallets with Observers. In *Crypto '93* (1994), LNCS 773, Springer-Verlag, pp. 302–318.

[4] Brands, S. A. A Note on Parallel Executions of Restrictive Blind Issuing Protocols for Secret-Key Certificates. Tech. rep., CWI, 1995. CS-R9519.

[5] Brands, S. A. More on Restrictive Blind Issuing of Secret-key Certificates in Parallel Mode. Tech. rep., CWI, 1995. CS-R9534.

[6] Brands, S. A. Off-Line Electronic Cash Based on Secret-Key Certificates. In *LATIN '95* (1995).

[7] Brands, S. A. Restrictive Blind Issuing of Secret-key Certificates in Parallel Mode. Tech. rep., CWI, 1995. CS-R9523.

Authority		User
	$N = pq$, product of two large primes $k \gg \log n$ where $n = \log N$	
secret $S \in (\mathbb{Z}/N\mathbb{Z})^\star$ public $I = S^{2^k} \bmod N$		
$t \in (\mathbb{Z}/N\mathbb{Z})^\star$ $x = t^{2^k} \bmod N$	$\xrightarrow{x}$	
		$\beta \in \{0, \ldots, 2^k - 1\}$ $\gamma \in \mathbb{Z}/N\mathbb{Z}$ $\alpha = xI^\beta \gamma^{2^k} \bmod N$ $\varepsilon = f(m, \alpha)$
	$\xleftarrow{e}$	$e = \varepsilon + \beta \bmod 2^k$
$y = tS^e \bmod N$	$\xrightarrow{y}$	
		$\tau = (\varepsilon + \beta) \div 2^k$ $\rho = y\gamma I^\tau \bmod N$
	$\rho^{2^k} = \alpha I^\varepsilon \bmod N$	

Figure 6: Ong – Schnorr blind signature scheme

[8] Chaum, D. Blind Signatures for Untraceable Payments. In *Crypto '82* (1983), Plenum, NY, pp. 199–203.

[9] Chaum, D., Fiat, A., and Naor, M. Untraceable Electronic Cash. In *Crypto '88* (1989), LNCS 403, Springer-Verlag, pp. 319–327.

[10] Feige, U., and Shamir, A. Witness Indistinguishable and Witness Hiding Protocols. In *Proc. of the 22nd STOC* (1990), ACM Press, pp. 416–426.

[11] Ferguson, N. Extensions of Single Term Coins. In *Crypto '93* (1994), LNCS 773, Springer-Verlag, pp. 292–301.

[12] Ferguson, N. Single Term Off-Line Coins. In *Eurocrypt '93* (1994), LNCS 765, Springer-Verlag, pp. 318–328.

[13] Fiat, A., and Shamir, A. How to Prove Yourself: practical solutions of identification and signature problems. In *Crypto '86* (1987), LNCS 263, Springer-Verlag, pp. 186–194.

[14] Guillou, L. C., and Quisquater, J.-J. A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory. In *Eurocrypt '88* (1988), LNCS 330, Springer-Verlag, pp. 123–128.

[15] Guillou, L. C., and Quisquater, J.-J. A "Paradoxal" Identity-Based Signature Scheme Resulting from Zero-Knowledge. In *Crypto '88* (1989), LNCS 403, Springer-Verlag, pp. 216–231.

[16] Okamoto, T. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In *Crypto '92* (1992), LNCS 740, Springer-Verlag, pp. 31–53.

[17] Ong, H., and Schnorr, C. Fast Signature Generation with a Fiat-Shamir-Like Scheme. In *Eurocrypt '90* (1991), LNCS 473, Springer-Verlag, pp. 432–440.

[18] Pointcheval, D., and Stern, J. Provably Secure Blind Signature Schemes. In *Asiacrypt '96* (1996), LNCS 1163, Springer-Verlag, pp. 252–265.

[19] Pointcheval, D., and Stern, J. Security Proofs for Signature Schemes. In *Eurocrypt '96* (1996), LNCS 1070, Springer-Verlag, pp. 387–398.

[20] Rivest, R., Shamir, A., and Adleman, L. A Method for Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM 21*, 2 (February 1978), 120–126.

[21] Schnorr, C. P. Efficient Identification and Signatures for Smart Cards. In *Crypto '89* (1990), LNCS 435, Springer-Verlag, pp. 235–251.

[22] Schoenmakers, L. A. M. An Efficient Electronic Payment System Withstanding Parallel Attacks. Tech. rep., CWI, 1995. CS-R9522.

[23] Shoup, V. On The Security of a Practical Identification Scheme. In *Eurocrypt '96* (1996), LNCS 1070, Springer-Verlag, pp. 344–353.