Proceedings of the 2000 International Workshop on Practice and Theory in Public Key Cryptography (PKC'2000)
(18 – 20 january 2000, Melbourne, Australia) – H. Imai and Y. Zheng Eds. Springer-Verlag, LNCS 1751, pages 113–128.

The Composite Discrete Logarithm and Secure Authentication

David Pointcheval

Dépt Informatique, ENS – CNRS, 45 rue d'Ulm, 75230 Paris Cedex 05, France.
E-mail: David.Pointcheval@ens.fr – URL: http://www.di.ens.fr/∼pointche.

Abstract. For the two last decades, electronic authentication has been an important topic. The first applications were digital signatures to mimic handwritten signatures for digital documents. Then, Chaum wanted to create an electronic version of money, with similar properties, namely bank certification and users' anonymity. Therefore, he proposed the concept of blind signatures.
For all those problems, and furthermore for online authentication, zero-knowledge proofs of knowledge became a very powerful tool. Nevertheless, high computational load is often the drawback of a high security level. More recently, witness-indistinguishability has been found to be a better property that can conjugate security together with efficiency. This paper studies the discrete logarithm problem with a composite modulus and namely its witness-indistinguishability. Then we offer new authentications more secure than factorization and furthermore very efficient from the prover point of view. Moreover, we significantly improve the reduction cost in the security proofs of Girault's variants of the Schnorr schemes which validates practical sizes for security parameters. Finally, thanks to the witness-indistinguishability of the basic protocol, we can derive a blind signature scheme with security related to factorization.

Keywords: Composite Discrete Logarithm, Zero-Knowledge, Witness-Indistinguishability, Identification, Signatures and Blind Signatures

1 Introduction

Provably secure schemes have ever been an important goal in cryptography. However, efficiency had hardly been an associated property. Even if authentication has been widely studied, very few schemes reach both efficiency and security. The reason is the large use of zero-knowledge protocols.

Identification. Concerning identification schemes, the first theoretical paper was the famous paper about zero-knowledge [19] which claimed that it was possible to prove the knowledge of a secret without revealing any information about it. Unfortunately, such a property, which guarantees security even against active attacks, often requires many iterations to actually reach a high security level and therefore results into inefficient protocols, either from the computational point of view [14, 12, 20, 21, 43, 28, 6, 17] or from the communication load [45, 49, 50, 31], and even both. Recently, a very efficient scheme has been proposed by Poupard and Stern [38], with security relative to the discrete logarithm problem. However, the cost of the reduction is so high that the proof can not validate realistic parameters.

Few years ago, Feige and Shamir [13] defined weaker but sufficient properties for secure identification protocols, the "witness-hiding" and the "witness-indistinguishable" properties. They are indeed weaker than the zero-knowledge

property in the sense that some information about the secret may be leaked, but not enough to efficiently find the secret. In other words, concerning the "witness hiding" property, if an attacker can find the secret after an active attack, she would have been able to find it without any interaction with the prover, within almost the same time. Whereas the "witness indistinguishable" property means that the view of the attacker is independent of the witness used as secret key: many secret keys are related to a public one and the proof only transfers the information that such a secret key is used, but not which one. In the following, we focus on this latter property which provides three-pass identification schemes secure against active attacks. Okamoto [26] presented some variants of the Schnorr [44] and Guillou-Quisquater [20] identification schemes, therefore related to the discrete logarithm in subgroups of prime order and to the RSA assumption [41] respectively.

The Random Oracle Model. For the last years, the so-called "random oracle model" [1] has boosted researches, providing an interesting tool for the designers since it helps to prove the security of very efficient schemes.

Indeed, this model, where some concrete cryptographic objects are idealized, namely the hash functions which are assumed to be really random ones, helped to provide security proofs for many encryption schemes [1, 2, 48, 27, 15, 32, 16, 29, 33] and digital/blind signature schemes [3, 35, 34, 36, 25, 37], etc.

In spite of the recent paper [7] making people to be careful with the random oracle model, this latter is widely considered robust since it is more and more used. For example, the encryption scheme OAEP [2] which is proven secure in this model has been incorporated in SET, the Secure Electronic Transaction system [23] proposed by VISA and Master Card, and will become the new RSA encryption standard PKCS #1 v2.0 [42]. The security of many other schemes has been validated in this model.

1.1 Related Work

Identification and Signatures. Few years ago, Schnorr [43, 44] presented a very efficient identification scheme, and the signature variant, based on the discrete logarithm problem in subgroups of prime order. We do not recall this famous scheme. However, the identification scheme is well-known to be zero-knowledge but only using a fixed-size challenge after many sequential iterations. Therefore, high security level against active attacks implies a high communication cost and either large memory for storing precomputations or high computation load, since no secure preprocessing has ever been proposed [10, 11]. Nevertheless, many applications assume its security even with the basic three-pass protocol, using large challenges. Such a security would rely on the unproven assumption that this scheme is "witness-hiding".

After the definitions of witness-hiding and witness-indistinguishable properties [13], Brickell and McCurley [6] proposed a variant of the Schnorr identification scheme dealing with the witness-hiding property. Then, Okamoto presented efficient three-pass identification schemes [26] provably secure even against active

attacks, thanks to witness-indistinguishability. One of them uses the representation problem [4] and is therefore based on the discrete logarithm problem in subgroups of prime order. The second relies on the RSA assumption [41]. However, all of the above schemes remained less efficient than the original Schnorr's scheme.

In 1991, Girault [17] presented a variant of the Schnorr identification scheme using a composite modulus instead of a prime one. It also allows an improved efficiency from the prover point of view. Few years ago, Poupard and Stern [38] provided a proof of the statistical zero-knowledge property of this scheme and the security relative to the composite discrete logarithm problem of both the identification scheme and the signature variant. However, the security proof, based on the zero-knowledge property of the identification scheme, also requires many iterations for a high level of security, and moreover uses an expansive reduction which can only validate large, and impractical, parameters They recently improved their reduction [39, 40], making security just relative to factorization. It is also the direction taken in the present work.

Concerning signatures, thanks to the Pointcheval–Stern's [37] and Ohta–Okamoto's [25] papers, one can efficiently transform any three-pass identification scheme into a signature scheme. Therefore, an efficient solution for identification furthermore solves the problem of efficient signatures.

Blind Signatures. In 1982, Chaum [8] wanted to create an electronic version of money, with similar properties, namely anonymity. He claimed that a way to do it was to use the notion of electronic coins together with blind signatures. A blind signature involves two participants, a user and the bank. The user wants to get a coin signed by the bank in such a way that the bank cannot recognize later either the coin nor the signature. He proposed a variation of the RSA signature [41] and later Brands [5] proposed a variation of the Schnorr's one.

Unfortunately, none of those schemes admits any security proof. Excepted some theoretical propositions [9, 30, 22] which are totally impractical, we had to wait 1996 to see blind signature schemes [34] provably secure. They were based on the Okamoto [26] witness-indistinguishable protocols, and used the following functions, for which collisions are provably difficult to compute:

- *problem of representation = discrete logarithm*: $f_{p,g,h}(r,s) = g^r h^s \bmod p$.
  A collision reveals the discrete logarithm of h in basis g. Indeed,

$$f_{p,g,h}(r,s) = f_{p,g,h}(r',s') \Longrightarrow h = g^{(r'-r)/(s-s')} \bmod p.$$

- *RSA problem/factorization*: $f_{N,a,e}(r,s) = a^r s^e \bmod N$.
  For some well-chosen parameters, a collision reveals the e-th root of a modulo N. Indeed,

$$f_{N,a,e}(r,s) = f_{N,a,e}(r',s') \Longrightarrow a^{r'-r} = (s/s')^e \bmod N.$$

  For a large enough prime e, Bezout's equality provides the e-th root of a modulo N. Otherwise, if e is a power of two and N a Blum integer, we can get the factorization of N (*cf.* [28, 47]).

Later, another well-known witness-indistinguishable problem has been used [36], the *modular square root*: $f_N(x) = x^2 \bmod N$ for any $0 \leq x \leq N/2$, where

$$f_N(x) = f_N(y) \Longrightarrow \gcd(N, x - y) \in \{\text{factors of } N\}.$$

In those papers, it was claimed that the proposed blind signature schemes were provably secure against parallel attacks. This means that the bank is guaranteed that after having given 10 dollars to a user, this latter cannot withdraw more than 10 dollars.

However, the main drawback of all those schemes is a high computation cost, even if they are practical, in comparison with the schemes claimed secure in the standard model [9, 30, 22]. It is, by now, an important challenge for blind signatures: a provably secure scheme which is also efficient, and particularly from the signer point of view since he may have thousands of signatures to perform at the same time.

1.2 Outline of the Paper

In this paper, we investigate, for the first time, the witness-indistinguishable protocols provided by the discrete logarithm problem with a composite modulus.

We first recall the Girault's scheme [17] together with the recent security results of Poupard and Stern [38]. Unfortunately, as for the Schnorr's scheme [43], this scheme has been proven zero-knowledge only using fixed-size challenges. Then many iterations are required to achieve a high security level. Here, we prove the security of this scheme, even against active attacks, after only one iteration of the protocol, using the witness-indistinguishable property [13]. That is an important improvement for the practical security w.r.t. the previous results [38]. Furthermore, we formally prove the security even if we use small keys, and thus for a very efficient scheme, whereas it was only heuristic. As previously said, the security of the signature is therefore a straightforward corollary [37] and can be considered as folklore.

Thereafter, we consider a blind signature scheme based on this problem, with a formal proof of security relative to factorization. Besides the provable security, the main property of this new scheme is efficiency, since it requires only one multiplication (not a modular one), from the computational point of view of the bank.

2 The Discrete Logarithm Problem

As shown by Feige and Shamir [13], the witness-indistinguishability (and even witness-hiding property) of an identification scheme is enough to provide security against active attacks. Pointcheval and Stern [37] proved that this property further provides blind signature schemes secure against one-more forgeries under parallel attacks.

The composite discrete logarithm problem provides such protocols, using the function $f_{N,g}(x) = g^x \bmod N$ for well-chosen N and g. Let us first define some useful notions for the following before stating an important theorem.

Definition 1 (α-strong prime). A prime integer p is said *α-strong* if $p = 2r+1$ where r is a large integer whose prime factors are all greater than α.

Definition 2 (α-strong RSA modulus). An integer N is called an *α-strong RSA modulus* if $N = pq$ where p and q are both α-strong primes.

Definition 3 (asymmetric basis). Let $N = pq$ be an RSA modulus. A basis g in $\mathbb{Z}_N^\star$ is said *asymmetric* if the parities of $\mathtt{Ord}(\mathtt{g})$ are different in $\mathbb{Z}_p^\star$ and $\mathbb{Z}_q^\star$.

In other words, an asymmetric basis is a quadratic residue in only one of both subgroups $\mathbb{Z}_p^\star$ and $\mathbb{Z}_q^\star$.

Theorem 4. *Let $N = pq$ be any α-strong RSA modulus, for some $\alpha > 2$, and g any asymmetric basis in $\mathbb{Z}_N^\star$, of order greater than α, then a collision of $f_{N,g}$, defined by $x \mapsto g^x \bmod N$, provides the factorization of N.*

Proof. Let us denote by 2ℓ the order of g in $\mathbb{Z}_N^\star$. One may remark that this order is necessarily even since it is even in at least, but also exactly, one of the subgroups, say $\mathbb{Z}_p^\star$. Furthermore, ℓ is odd and greater than α, since it should be greater than $\alpha/2 > 1$ and any prime factor of $(p-1)/2$ or $(q-1)/2$ is odd and greater than α. Therefore,

$$g^{2\ell} = 1 \bmod p \text{ and } g^{2\ell} = 1 \bmod q, \text{ but } g^{\ell} = -1 \bmod p \text{ and } g^{\ell} = 1 \bmod q.$$

Let us assume that we have a collision $x < y$ for $f_{N,g}$, $f_{N,g}(x) = f_{N,g}(y)$. If we note $L = y - x$, then $2\ell | L$. By extracting the odd part b of L, $L = 2^a b$, we get a multiple of ℓ. Then

$$g^{2b} = 1 \bmod p \text{ and } g^{2b} = 1 \bmod q, \text{ but } g^{b} = -1 \bmod p \text{ and } g^{b} = 1 \bmod q.$$

Therefore, g^b is a non-trivial square root of 1 in $\mathbb{Z}_N^\star$: $\gcd(g^b - 1, n) \in \{p, q\}$. □

Then, we have a difficult problem for which two distinct solutions provide the factorization of the modulus N.

3 Application to Cryptographic Protocols

We first consider the identification scheme, together with the derived signature. Then, we focus on a new blind signature scheme.

3.1 Identification

Presentation. Let us first recall the Girault's scheme [17] (see Figure 1).

- We have two security parameters k and k', where k represents the size of the challenge and k' is related to the information leak, and a bound S for the secret key. Then, we define $R = 2^{k+k'}S$. We use an RSA-modulus $N = pq$ and an element $g \in \mathbb{Z}_N^\star$ of high order. The prover chooses a random secret key $s \in \{0, \ldots, S-1\}$ and publishes $v = g^{-s} \bmod N$.

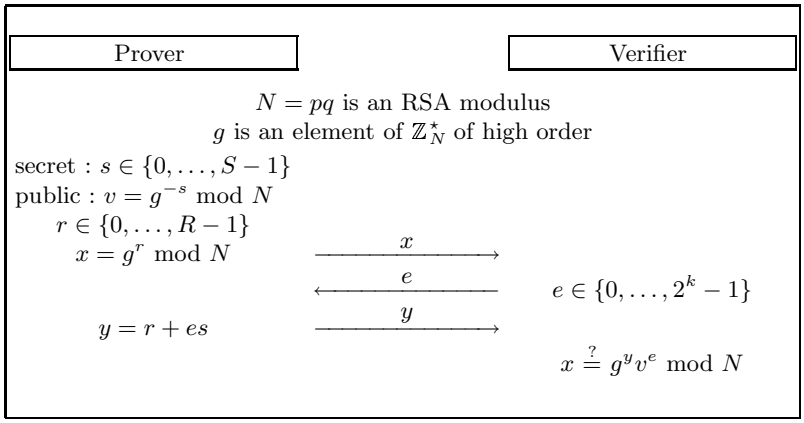

Fig. 1. Girault's Identification Scheme

- The prover initiates the protocol choosing a random $r \in \{0, \ldots, R-1\}$ and sending the "commitment" $x = g^r \bmod N$; The verifier randomly chooses a "challenge" $e \in \{0, \ldots, 2^k - 1\}$, and sends it to the prover; Finally, the prover computes and sends $y = r + es$;
- The verifier can check whether $x = g^y v^e \bmod N$, or not.

One cannot say this is a proof of knowledge of the discrete logarithm of v in basis g modulo N, but one can state the following theorem in the particular case where N is a 2^k-strong RSA modulus (which includes the strong-RSA moduli classically used in practice):

Theorem 5. *Let N be a 2^k-strong RSA modulus. If there exists an attacker $\mathcal{A}$, with running time bounded by T, that is able to be accepted with a probability ε greater than $2 \cdot 2^{-k}$, for a non-negligible fraction of v, then discrete logarithms in basis g modulo N can be computed within an expected time bounded by $4T/\varepsilon \times S/\mathtt{Ord}(\mathtt{g})$.*

Proof. Using the classical technique of extraction [14, 12, 37, 25], one can obtain, from two valid proofs with the same commitment x, a pair (α, β) such that $v^\alpha = g^\beta \bmod N$ with $0 < \alpha < 2^k$. Furthermore, this can be done in expected time bounded by $4T/\varepsilon$.

If one first runs this reduction with $v = g^\gamma \bmod N$, for a randomly chosen γ smaller than S, then one gets (α_1, β_1) such that

$$L = \alpha_1 \gamma - \beta_1 = 0 \bmod \mathtt{Ord}(\mathtt{g}),$$

which is nonzero with probability greater than $(S/\mathtt{Ord}(\mathtt{g}) - 1)^{-1}$.

Then, one runs this reduction with v whose discrete logarithm x is wanted and gets (α_2, β_2). Let us initialize ℓ_0 to the L obtained above. Thereafter, we recursively compute $\ell_{i+1} = \ell_i / \gcd(\alpha_2, \ell_i)$ until the gcd equals 1. The limit is denoted by ℓ. Since $\alpha_2 < 2^k$, which is smaller than all the odd prime factors of $\lambda(N)$, and then of $\mathtt{Ord}(\mathtt{g})$, 2ℓ is still a multiple of $\mathtt{Ord}(\mathtt{g})$. We then compute $y = \beta \alpha_2^{-1} \bmod \ell$, and one gets $x = y + c\ell \bmod \mathtt{Ord}(\mathtt{g})$, where $c \in \{0, 1\}$. One has just to check the right value for c.

On can remark that in the particular case where g is of maximal order $\lambda(N)$, a multiple of $\mathtt{Ord(g)} = \lambda(N)$ leads to the factorization of N [24]. □

Theorem 6. *This protocol is statistically zero-knowledge.*

Proof. The reader may refer to the Poupard-Stern's paper [38] or to the proof of witness-indistinguishability presented below. □

However, the zero-knowledge property of an interactive proof of knowledge is a too strong property for identification purpose, and the main drawback is the sequential iterations of the basic scheme to achieve a high security level. Witness-indistinguishability [13] is therefore enough to ensure security against active attacks and provides a much more efficient scheme.

Theorem 7. *This protocol is statistically witness-indistinguishable.*

Proof. We have to prove that the distribution of the communication tapes is independent of the secret key used by the prover, even with a dishonest verifier. Let $s_1 < s_2$ be two distinct secret keys in $\{0, \ldots, S-1\}$ such that

$$g^{-s_1} = g^{-s_2} = v \bmod N.$$

We can show that the following distributions, where r is uniformly chosen in $\{0, \ldots, R-1\}$ and $\mathcal{S}$ the strategy, possibly probabilistic, of the attacker to get the challenge e from x, are indistinguishable:

$$\begin{aligned} \delta_1 &= \{(x = g^r \bmod N, e, y) \mid y = r + s_1 e, e = \mathcal{S}(x)\} \\ \text{and } \delta_2 &= \{(x = g^r \bmod N, e, y) \mid y = r + s_2 e, e = \mathcal{S}(x)\}. \end{aligned}$$

Indeed, for any triple (α, β, γ) such that $\alpha = g^\gamma v^\beta \bmod N$, we can define

$$p_i(\alpha, \beta, \gamma) = \Pr_{(x,e,y)\in\delta_i}[(x, e, y) = (\alpha, \beta, \gamma)], \text{ for } i = 1, 2.$$

If we denote by $p_{\alpha,\beta}$ the probability for the strategy $\mathcal{S}$ to output β on the input α, and if δ is the boolean function defined by $\delta(\mathtt{true}) = 1$ and $\delta(\mathtt{false}) = 0$, then we get

$$\begin{aligned} p_i(\alpha, \beta, \gamma) &= \Pr_r[\alpha = g^r \bmod N, \beta = \mathcal{S}(\alpha), \gamma = r + s_i\beta] \\ &= \Pr_r[\alpha = g^r \bmod N] \cdot p_{\alpha,\beta} \cdot \Pr_r[\gamma = r + s_i\beta | \gamma = r + s_i\beta \bmod \mathtt{Ord(g)}] \\ &= \frac{1}{\mathtt{Ord(g)}} \cdot p_{\alpha,\beta} \cdot \delta(0 \le \gamma - s_i\beta < R) \cdot \frac{\mathtt{Ord(g)}}{R}. \end{aligned}$$

An easy simplification leads to $p_{\alpha,\beta}/R \times \delta(s_i\beta \le \gamma < R + s_i\beta)$. Therefore the distance between both distributions δ_1 and δ_2 is the sum over all the triples (α, β, γ) such that $\gamma = \log \alpha - s_1\beta \bmod \mathtt{Ord}(g)$:

$$\Delta = \sum_{\alpha,\beta} \frac{p_{\alpha,\beta}}{R} \cdot \frac{2(s_2 - s_1)\beta}{\mathtt{Ord}(g)} \le \frac{2S}{R \cdot \mathtt{Ord}(g)} \times \sum_{\alpha,\beta} \beta \cdot p_{\alpha,\beta}.$$

By definition of the probability $p_{\alpha,\beta}$, it is clear that for any α, $\sum_\beta p_{\alpha,\beta} = 1$, and therefore the sum over all possible α is equal to $\mathtt{Ord}(g)$. Since $\beta < 2^k$ and $R = 2^{k+k'}S$, we get

$$\Delta \leq \frac{2S \cdot 2^k}{R} = \frac{2}{2^{k'}}.$$

□

Thanks to this witness-indistinguishability, if we furthermore make g to be an *asymmetric basis* in $\mathbb{Z}_N^\star$, we get an efficient and secure identification scheme in only three flows.

Theorem 8. *Let N be a 2^k-strong RSA modulus and g an asymmetric basis of high order in $\mathbb{Z}_N^\star$. If $S \geq 2 \cdot \mathtt{Ord}(\mathtt{g})$, this protocol is secure against active attacks relative to the factorization of N.*

Proof. In order to prove the security of the identification scheme against active attacks, we choose a random secret key $s < S$. We let the attacker verify some interactions. Then, we assume that she succeeds in her impersonation with probability ε. Using the first step of the proof of the Theorem 5, we get a multiple L of the order of g with probability greater than one half. Then, as in the proof of the Theorem 4, since g is an asymmetric basis, one gets the factorization of N. □

Remark 9. It is important to remark that we have only proven that an impersonation under an active attack is harder than the factorization, whereas the security of the iterated protocol has already been proven relative to the composite discrete logarithm, using the zero-knowledge property.

Nevertheless, when we have the factorization of N, the remaining security is the same as in the Schnorr's identification scheme [43, 44]: heuristically, the discrete logarithm in subgroups of prime orders, which is still hard to solve.

Furthermore, the security result remains even if the challenge grows in order to get a high security level. Which is not the case for the zero-knowledge property.

Reduction Costs. Let us compare the reduction costs to obtain two answers from the impersonator. With the Poupard and Stern's proof [38], this leads with some more computations to the discrete logarithm of v, with our proof, this immediately leads to the factorization of N.

Poupard and Stern's Reduction. We assume that we use a k-bit challenge, and there exists an impersonator who succeeds with probability $\varepsilon \geq 2 \cdot 2^{-k}$. Then, one can easily show [25, 37] that after less than $4/\varepsilon$ iterations, we get two valid answers with probability greater than $1/2$. As a consequence, a passive impersonation, with probability ε greater than $2 \cdot 2^{-k}$ within time T, can be used to find two distinct answers for a same commitment within an expected time bound $4T/\varepsilon$. On the other hand, an impersonation, with probability ε greater than $2 \cdot 2^{-k}$ after ℓ active attacks, within time T, can be used to find two distinct answers for a same commitment within a time bound $(4/\varepsilon + \ell \times 2^k) \cdot T$. because of the simulation which requires many resets. It is almost equal to $2^k \ell T$.

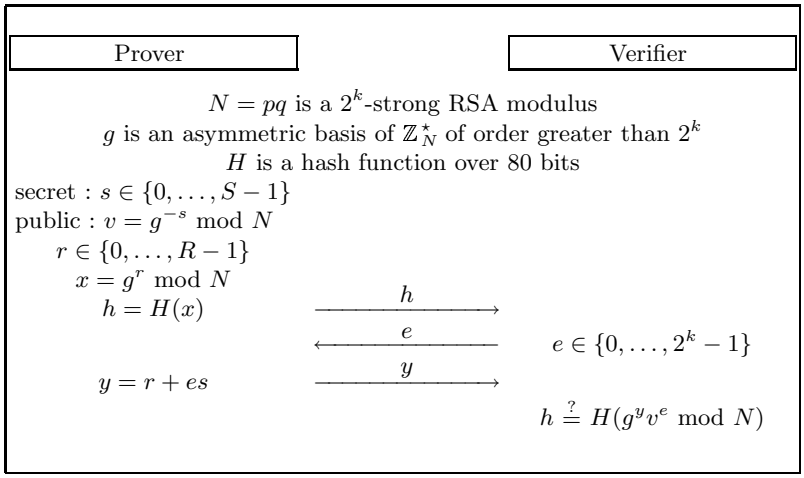

Fig. 2. Optimized Identification Scheme

Our Reduction. Using the witness-indistinguishable property, the reduction using a passive impersonation has the same complexity. On the other hand, an impersonation with probability ε greater than $2 \cdot 2^{-k}$ after ℓ active attacks within time T can be used to find two distinct answers for a same commitment within an expected time bound $4T/\varepsilon$, since no simulation is required.

Summary. An impersonation with probability ε, greater than 2×2^{-k}, after $\ell > 0$ active attacks can help to compute discrete logarithms within a time $2^k \ell T$ (thanks to the zero-knowledge property) or to factor N within a time $4T/\varepsilon$ (thanks to the witness-indistinguishable property). This latter is much smaller than the former. Therefore, a high security level against active attacks can only be related to factorization: for example, with $k = 30$ and $\ell = 2^{40}$, the reduction cost is less than 2^{30} from factorization, against 2^{70} from discrete logarithm, which has no practical meaning!

Communication Load. With the presented proof, S can be chosen over very few hundreds of bits, provided $S \geq 2 \cdot \mathtt{Ord}(\mathsf{g})$ (namely 160 bits to avoid baby steps–giant steps attacks [46]). Furthermore, the communication load can be optimized using the Girault and Stern's technique [18] as it is presented on Figure 2. Indeed, a hash function that returns 80-bit digests requires 2^{64} computations to expect a 5-collision. Then, with a $k + 3$-bit challenge, the security level remains 2^{-k}. Both remarks lead to very efficient and low-cost protocols (see Figure 2).

3.2 Signature

We can of course derive this identification scheme into a signature scheme Σ (see Figure 3), using a hash function to generate the random challenge. The security against existential forgeries under no-message attacks of the signature scheme is clear in the random oracle model [12, 26, 25, 37]. Because of the witness-indistinguishable property, we need not any simulation for the security against

Initialisation
$N = pq$ is a 2^k-strong RSA modulus g is an asymmetric basis of $\mathbb{Z}_N^\star$ of order greater than 2^k
Key Generation
secret key : $s \in \{0, \ldots, S-1\}$ public key: $v = g^{-s} \bmod N$
Signature of m
choose $r \in \{0, \ldots, R-1\}$ and compute $x = g^r \bmod N$ get $e = H(m, x)$ and compute $y = r + es$ $\mathbf{\Sigma(m) = (e, y)}$
Verification of (m, e, y): $e \stackrel{?}{=} H(m, g^y v^e \bmod N)$

Fig. 3. Signature Scheme

adaptive chosen-message attacks. In fact, we can use a real signer with a secret key s_1 and use the forking lemma [37], or the ID reduction lemma [25], to extract a second one from the attacker. As previously seen for the identification scheme, if $S \geq 2 \cdot \mathtt{Ord}(\mathtt{g})$, with high probability, we get the factorization of the modulus N.

Theorem 10. *With $S \geq 2 \cdot \mathtt{Ord}(\mathtt{g})$, an existential forgery under an adaptive chosen-message attack of this scheme is harder than the factorization.*

3.3 Blind Signature

Now, we focus on a new blind signature scheme based on the previously seen problem. The construction of the blind signature is not straightforward because the initialization of this scheme requires the security parameters to be carefully chosen. However, the resulting scheme is very interesting from the bank point of view. Indeed, its computational load is minimal.

Presentation. Because of the witness-indistinguishable property seen above, we hope to get a blind signature scheme at least more secure than factorization. Let first present this scheme (see Figure 4), where k is the security parameter and k' the information leak parameter: we define $R = 2^{k+k'}S$ and $M = 2^{k+2k'}S$, where $S \geq 2 \cdot \mathtt{Ord}(\mathtt{g})$ defines the range set of the secret key.

Security. First, we have to prove that this scheme is really blind, *i.e.* even a dishonest bank cannot link later a user and a message/signature pair. This is a fundamental property required by anonymous protocols (electronic cash, electronic voting). We want the bank not to be able to recognize a user even with the message and the signature.

Theorem 11. *This scheme is a statistically blind signature scheme.*

Proof. The output of this protocol is a signature which has been considered in the previous section and proven secure. Then, we only have to prove that the protocol is "blind".

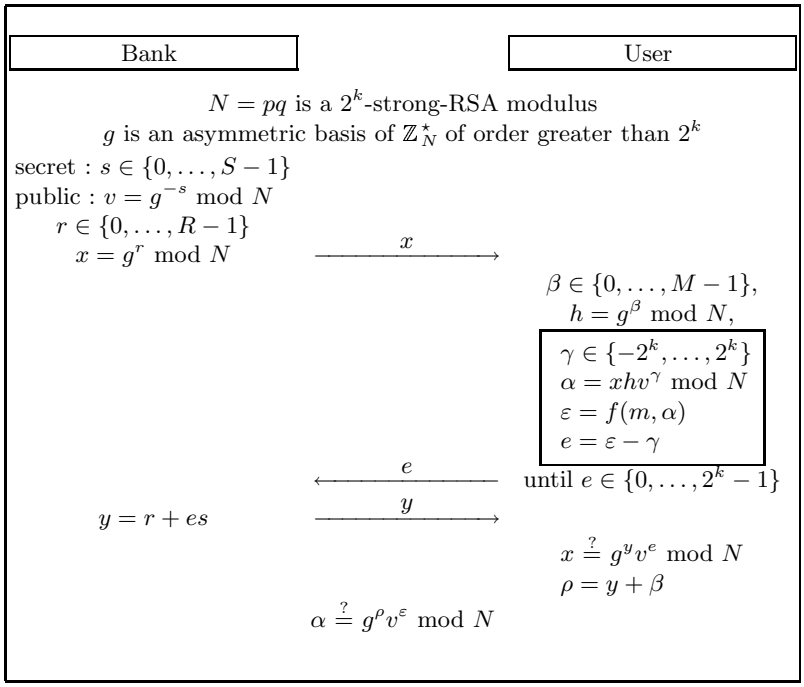

Fig. 4. Blind Signature Scheme

Let $(m, \alpha, \varepsilon, \rho)$ be a valid signature obtained from an execution of the "blind signature scheme" after one of both interactions (x_1, e_1, y_1) and (x_2, e_2, y_2). Is it possible to know, with non-negligible advantage, from which one it comes? To know that, we have to study the following probabilities for $i = 1, 2$:

$$p_i(\alpha, \varepsilon, \rho) = \Pr_{\beta,\gamma}[\alpha = x_i g^\beta v^\gamma, \varepsilon = e_i + \gamma \text{ and } \rho = y_i + \beta \,|\, 0 \leq \varepsilon - \gamma \leq 2^k - 1].$$

For both values of i,

$$\begin{aligned} p_i(\alpha, \varepsilon, \rho) &= \Pr_{\beta,\gamma}[\gamma = \varepsilon - e_i \text{ and } \beta = \rho - y_i \,|\, 0 \leq \varepsilon - \gamma \leq 2^k - 1] \\ &= \frac{\delta(0 \leq \rho - y_i \leq M - 1)}{M} \times 2^{-k} = \delta(y_i \leq \rho \leq M + y_i - 1)/2^k M. \end{aligned}$$

Then, the distance between both distributions is equal to

$$\Delta = \sum_\varepsilon \frac{2|y_2 - y_1|}{2^k M} \leq 2 \times \sum_\varepsilon \frac{2^k S(1 + 2^{k'})}{2^k M} \leq 2 \times \frac{1 + 2^{k'}}{2^{2k'}} \leq \frac{3}{2^{k'}}.$$

This distance is therefore negligible into the information leak parameter k'. □

Now, we also claim the following security result:

Theorem 12. *A "one-more" forgery under a parallel attack against this blind signature scheme is harder than the factorization of N, in the random oracle model.*

Proof. The proof uses the same technique as [37], since it just takes advantage of the witness-indistinguishability. We therefore refer the reader to this paper. □

Scheme	Identification	Signature	Blind Signature
Modulus	$\|N\| = 1024$ bits with $\|p\| = \|q\| = 512$ bits		
$\mathtt{Ord}(\mathtt{g})$	160 bits		
Security parameter	$k = 24$	$k = 128$	
Information leak parameter	$k' = 64$		
$\|S\|$ $(> \|\mathtt{Ord}(\mathtt{g})\|)$	168 bits		
$\|R\|$ $(= \|S\| + k + k')$	256 bits	360 bits	
$\|M\|$ $(= \|S\| + k + 2k')$			424 bits
Online Cost (prover)	$\mathtt{Mult}(24,168)$ + $\mathtt{Add}(256,192)$	$\mathtt{Mult}(128,168)$ + $\mathtt{Add}(360,296)$	
Communication	360 bits (45 bytes)		
Signature Size		488 bits (61 bytes)	552 bits (69 bytes)

Fig. 5. Efficiency of the Proposed Schemes

4 Security and Efficiency

For practical purpose, it seems to be convenient to choose a 1024-bit modulus N and an asymmetric basis g of 160-bit long order. The information leak parameter k' can be fixed to 64, and the security parameter to 24 or 128 depending on the situation (see Figure 5).

Therefore, the security provably relies on the factorization of the 1024-bit modulus (which is assumed to be infeasible). In case of discovery of a new and efficient algorithm to factor large numbers, the security collapses at the same level as the Schnorr schemes: the discrete logarithms in subgroups of prime order (unproven for identification, but provable for signatures).

From the prover point of view, these protocols are very efficient. Indeed, if we only take in account the computation he has to do in real-time, it only consists of one multiplication and one addition over the natural integers $\mathbb{N}$. Furthermore, the used numbers are very small.

As one can remark, since the commitment can be precomputed, the prover has only one multiplication and one addition to perform during a proof (identification/signature/blind signature). For the recommended parameters, for a blind signature (the most costly scheme), the bank has just to multiply a 128-bit integer by a 168-bit one and to add the result to a 360-bit integer. The important gain versus the Schnorr schemes is the suppression of the modular reduction.

Then, at the cost of a little storage, the bank can blindly sign millions of messages per second, which can be required in a huge electronic cash application or electronic vote. Furthermore, thanks to the security result, parallel withdrawals can be performed securely.

5 Conclusion

In this paper, we have presented many schemes based on the composite discrete logarithm problem. From identification to blind signature, we have proven efficient schemes to be at least as secure as factorization.

The main contributions of this paper, vs. the Poupard and Stern's one [38], are the possible use of small secret keys and the security proof of the three-pass identification scheme even with large challenges, thanks to the witness-indistinguishability of the protocol. Both properties lead to the most efficient identification scheme known for the moment, with provable security (namely related to factorization). The non-interactive version, using a hash function [12], thus provides a very efficient signature scheme more secure than factorization, outputting very short signatures (approximatively 60 bytes).

Furthermore we provide a new blind signature scheme really efficient from the bank point of view. Indeed, the security result allows parallel withdrawals and the low computational load of the bank provides a very high rate. Therefore, this scheme is very well suited for very huge scale applications with thousands of users.

References

1. M. Bellare and P. Rogaway. Random Oracles Are Practical: a Paradigm for Designing Efficient Protocols. In *Proc. of the 1st CCS*, pages 62–73. ACM Press, New York, 1993.
2. M. Bellare and P. Rogaway. Optimal Asymmetric Encryption – How to Encrypt with RSA. In *Eurocrypt '94*, LNCS 950, pages 92–111. Springer-Verlag, Berlin, 1995.
3. 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, Berlin, 1996.
4. S. A. Brands. An Efficient Off-Line Electronic Cash System Based on the Representation Problem. Technical Report CS-R9323, CWI, Amsterdam, 1993.
5. S. A. Brands. Untraceable Off-Line Cash in Wallets with Observers. In *Crypto '93*, LNCS 773, pages 302–318. Springer-Verlag, Berlin, 1994.
6. E. F. Brickell and K. S. McCurley. An Interactive Identification Scheme Based on Discrete Logarithms and Factoring. *Journal of Cryptology*, 5:29–39, 1992.
7. R. Canetti, O. Goldreich, and S. Halevi. The Random Oracles Methodology, Revisited. In *Proc. of the 30th STOC*, pages 209–218. ACM Press, New York, 1998.
8. D. Chaum. Blind Signatures for Untraceable Payments. In *Crypto '82*, pages 199–203. Plenum, New York, 1983.
9. I. B. Damgård. Payment Systems and Credential Mechanisms with Provable Security against Abuse by Individuals. In *Crypto '88*, LNCS 403, pages 328–335. Springer-Verlag, Berlin, 1989.
10. P. de Rooij. On the Security of the Schnorr Scheme Using Preprocessing. In *Eurocrypt '91*, LNCS 547, pages 71–80. Springer-Verlag, Berlin, 1992.
11. P. de Rooij. On Schnorr's Preprocessing for Digital Signature Schemes. *Journal of Cryptology*, 10:1–16, 1997.
12. U. Feige, A. Fiat, and A. Shamir. Zero-Knowledge Proofs of Identity. *Journal of Cryptology*, 1:77–95, 1988.
13. U. Feige and A. Shamir. Witness Indistinguishable and Witness Hiding Protocols. In *Proc. of the 22nd STOC*, pages 416–426. ACM Press, New York, 1990.
14. 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, Berlin, 1987.
15. E. Fujisaki and T. Okamoto. How to Enhance the Security of Public-Key Encryption at Minimum Cost. In *PKC '99*, LNCS 1560, pages 53–68. Springer-Verlag, Berlin, 1999.
16. E. Fujisaki and T. Okamoto. Secure Integration of Asymmetric and Symmetric Encryption Schemes. In *Crypto '99*, LNCS 1666, pages 537–554. Springer-Verlag, Berlin, 1999.
17. M. Girault. Self-Certified Public Keys. In *Eurocrypt '91*, LNCS 547, pages 490–497. Springer-Verlag, Berlin, 1992.

18. M. Girault and J. Stern. On the Length of Cryptographic Hash-Values used in Identification Schemes. In *Crypto '94*, LNCS 839, pages 202–215. Springer-Verlag, Berlin, 1994.
19. S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. In *Proc. of the 17th STOC*, pages 291–304. ACM Press, New York, 1985.
20. 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, Berlin, 1988.
21. L. C. Guillou and J.-J. Quisquater. A "Paradoxal" Identity-Based Signature Scheme Resulting from Zero-Knowledge. In *Crypto '88*, LNCS 403, pages 216–231. Springer-Verlag, Berlin, 1989.
22. A. Juels, M. Luby, and R. Ostrovsky. Security of Blind Digital Signatures. In *Crypto '97*, LNCS 1294, pages 150–164. Springer-Verlag, Berlin, 1997.
23. SET Secure Electronic Transaction LLC. SET Secure Electronic Transaction Specification – Book 3: Formal Protocol Definition, may 1997.
Available from `http://www.setco.org/`.
24. G. Miller. Riemann's Hypothesis and Tests for Primality. *Journal of Computer and System Sciences*, 13:300–317, 1976.
25. K. Ohta and T. Okamoto. On Concrete Security Treatment of Signatures Derived from Identification. In *Crypto '98*, LNCS 1462, pages 354–369. Springer-Verlag, Berlin, 1998.
26. T. Okamoto. Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes. In *Crypto '92*, LNCS 740, pages 31–53. Springer-Verlag, Berlin, 1992.
27. T. Okamoto, S. Uchiyama, and E. Fujisaki. EPOC: Efficient Probabilistic Public-Key Encryption. Submission to IEEE P1363a. November 1998.
Available from `http://grouper.ieee.org/groups/1363/addendum.html`.
28. H. Ong and C.P. Schnorr. Fast Signature Generation with a Fiat-Shamir-Like Scheme. In *Eurocrypt '90*, LNCS 473, pages 432–440. Springer-Verlag, Berlin, 1991.
29. P. Paillier and D. Pointcheval. Efficient Public-Key Cryptosystems Provably Secure against Active Adversaries. In *Asiacrypt '99*, LNCS 1716. Springer-Verlag, Berlin, 1999.
30. B. Pfitzmann and M. Waidner. How to Break and Repair a "Provably Secure" Untraceable Payment System. In *Crypto '91*, LNCS 576, pages 338–350. Springer-Verlag, Berlin, 1992.
31. D. Pointcheval. A New Identification Scheme Based on the Perceptrons Problem. In *Eurocrypt '95*, LNCS 921, pages 319–328. Springer-Verlag, Berlin, 1995.
32. D. Pointcheval. New Public Key Cryptosystems based on the Dependent-RSA Problems. In *Eurocrypt '99*, LNCS 1592, pages 239–254. Springer-Verlag, Berlin, 1999.
33. D. Pointcheval. Chosen-Ciphertext Security for any One-Way Cryptosystem. In *PKC '00*, LNCS. Springer-Verlag, Berlin, 2000.
34. D. Pointcheval and J. Stern. Provably Secure Blind Signature Schemes. In *Asiacrypt '96*, LNCS 1163, pages 252–265. Springer-Verlag, Berlin, 1996.
35. D. Pointcheval and J. Stern. Security Proofs for Signature Schemes. In *Eurocrypt '96*, LNCS 1070, pages 387–398. Springer-Verlag, Berlin, 1996.
36. D. Pointcheval and J. Stern. New Blind Signatures Equivalent to Factorization. In *Proc. of the 4th CCS*, pages 92–99. ACM Press, New York, 1997.
37. D. Pointcheval and J. Stern. Security Arguments for Digital Signatures and Blind Signatures. *Journal of Cryptology*, 1999.
Available from `http://www.di.ens.fr/~pointche`.
38. G. Poupard and J. Stern. Security Analysis of a Practical "on the fly" Authentication and Signature Generation. In *Eurocrypt '98*, LNCS 1403, pages 422–436. Springer-Verlag, Berlin, 1998.
39. G. Poupard and J. Stern. On The Fly Signatures based on Factoring. In *Proc. of the 6th CCS*. ACM Press, New York, 1999.
40. G. Poupard and J. Stern. Short Proofs of Knowledge for Factoring. In *PKC '00*, LNCS. Springer-Verlag, Berlin, 2000.
41. 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.
42. RSA Data Security, Inc. Public Key Cryptography Standards – PKCS.
Available from `http://www.rsa.com/rsalabs/pubs/PKCS/`.
43. C. P. Schnorr. Efficient Identification and Signatures for Smart Cards. In *Crypto '89*, LNCS 435, pages 235–251. Springer-Verlag, Berlin, 1990.
44. C. P. Schnorr. Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, 4(3):161–174, 1991.
45. A. Shamir. An Efficient Identification Scheme Based on Permuted Kernels. In *Crypto '89*, LNCS 435, pages 606–609. Springer-Verlag, Berlin, 1990.

46. D. Shanks. Class number, a theory of factorization, and genera. In *Proceedings of the symposium on Pure Mathematics*, volume 20, pages 415–440. AMS, 1971.
47. V. Shoup. On The Security of a Practical Identification Scheme. In *Eurocrypt '96*, LNCS 1070, pages 344–353. Springer-Verlag, Berlin, 1996.
48. V. Shoup and R. Gennaro. Securing Threshold Cryptosystems against Chosen Ciphertext Attack. In *Eurocrypt '98*, LNCS 1403, pages 1–16. Springer-Verlag, Berlin, 1998.
49. J. Stern. A New Identification Scheme Based on Syndrome Decoding. In *Crypto '93*, LNCS 773, pages 13–21. Springer-Verlag, Berlin, 1994.
50. J. Stern. Designing Identification Schemes with Keys of Short Size. In *Crypto '94*, LNCS 839, pages 164–173. Springer-Verlag, Berlin, 1994.