Complex Zero-Knowledge Proofs of Knowledge are Easy to Use

Sébastien Canard, Iwen Coisel, and Jacques Traoré

Orange Labs, 42 rue des Coutures, 14000 Caen, France
{sebastien.canard, iwen.coisel, jacques.traore}@orange-ftgroup.com

Abstract. Since 1985 and their introduction by Goldwasser, Micali and Rackoff, followed in 1988 by Feige, Fiat and Shamir, zero-knowledge proofs of knowledge have become a central tool in modern cryptography. Many articles use them as building blocks to construct more complex protocols, for which security is often hard to prove. The aim of this paper is to simplify analysis of many of these protocols, by providing the cryptographers with a theorem which will save them from stating explicit security proofs. Kiayias, Tsiounis and Yung made a first step in this direction at Eurocrypt'04, but they only addressed the case of so-called "triangular set of discrete-log relations". By generalizing their result to any set of discrete-log relations, we greatly extend the range of protocols it can be applied to.

1 Introduction

The main purpose of authentication is to know who is who. More precisely, Alice wants to be convinced that the entity she communicates with is the right one. When using cryptography, this is often achieved by proving knowledge of a particular secret without (provably) revealing it. In 1985, Goldwasser, Micali and Rackoff [19] introduced the concept of zero-knowledge interactive proofs (ZKIP). The idea of using it for purposes of authentication came one year later in the article by Fiat and Shamir [15], followed in 1988 by Feige, Fiat and Shamir [14], who introduced the zero-knowledge proofs of knowledge (ZKPK).

In modern cryptography, these protocols are not only used for authentication but also as building blocks to achieve more complex purposes, such as for example guaranteeing the anonymity of a user [1, 5, 9] or committing to a secret value without being able to change one's mind [16]. In these schemes, users typically have to compute some public data relying on secret and random values, then prove that these public data are well-formed by using these building blocks. The security of the global construction relies both on the computed data and protocols they are involved in, which consequently have to be proven as being ZKPK.

Appeared in W. Susilo, J. K. Liu, Y. Mu (Eds.): ProvSec 2007, LNCS 4784,pp. 122–137, 2007.

The aim of this paper is to simplify analysis of many of these protocols, by providing the cryptographers with a theorem which will save them from stating explicit security proofs. Kiayias, Tsiounis and Yung made a first step in this direction at Eurocrypt'04, but they only addressed the case of so-called "triangular set of discrete-log relations". By generalizing their result to any set of discrete-log relations, we greatly extend the range of protocols it can be applied to.

1.1 Related Work

Many ZKPK have been proposed since the article of Feige et al. in 1988 [14]. When based on discrete logarithms, they are often built over a cyclic group $\mathcal{G} = \langle g \rangle$ either of known prime order q (after Schnorr's article [22]) or of unknown order (but in the same range of magnitude as the order of G). In this paper, we will only consider discrete-logarithm based ZKPK in groups of unknown order, since this is the most difficult case. In this setting, the building block is the GPS authentication scheme [18], which allows to prove knowledge of a discrete logarithm in such groups.

The construction of complex cryptographic tools such as group signature schemes, credential schemes or e-cash systems, always requires more than a single proof of knowledge of a single discrete logarithm. Rather, it involves several secret values and several (discrete-log based) relations between these values. The GPS scheme has therefore to be extended in order to obtain first new building blocks as e.g. a proof of knowledge of a representation [16, 13], that involves two secret values and one relation, a proof of equality of two known representations [11, 7], which requires four secret values and two relations, or the proof that a committed value lies in an interval [4, 7, 10, 3], that necessitates several secret values and relations. Then, these various building blocks are used to construct still more elaborate protocols, the security of which must be demonstrated in detail for each of them, though the proofs are very similar to each other. As a consequence, it would be very useful to design a "general proof" which could apply to a wide range of such protocols, saving the designers from proving them secure.

Kiayias, Tsiounis and Yung [20] use such complex protocols in their construction of traceable signatures and, as an independent interest of the paper, make a first step towards designing such a general proof. They introduce the notion of *Discrete-Log Relation Set* (DLRS), that is a set of relations involving objects (as public keys and parameters) and free variables (as secret elements). For each free variable, there is a corresponding secret known by a prover $\mathcal{P}$. Then they propose a generic 3-move honest

Appeared in W. Susilo, J. K. Liu, Y. Mu (Eds.): ProvSec 2007, LNCS 4784,pp. 122–137, 2007.

verifier zero-knowledge proof that allows $\mathcal{P}$ to prove the knowledge of these values. They also show that their construction is a ZKPK in the particular case of a triangular discrete-log relation set, that is when each relation introduces at most one new free variable w.r.t. the previous ones. They thus solve the above problem only in part, since their security proof only addresses a particular case. The aim of our paper is to solve this problem in general, for any discrete-log relation set.

1.2 Our Contribution

In this paper, we prove the soundness of any discrete-log relation set (DLRS), as defined by Kiayas, Tsiounis and Yung [20], i.e. when G is a (large) subgroup of the multiplicative group of the ring of integers modulo a composite integer. We do not address the zero-knowledge property, since it happens that it can be derived from [20] in a straight-forward manner. Unlike in [20], we do not have any restrictions on the kind of DLRS we use.

All security proofs for a ZKPK in a group of unknown order use the trick of either solving the Flexible RSA problem or retrieving all secret values involved in the proof[1]. Another contribution of this paper is that, to the best of our knowledge, our proof is the first one where the instance of the Flexible RSA problem is clearly defined.

1.3 Organization of the Paper

We first give some preliminaries in the next section. Section 3 introduces the first results on DLRS. It also gives evidence that the model of Kiayias *et al.* does not cover all kind of DLRS. We then give our new theorem and its proof in Section 4, then conclude in Section 5.

2 Preliminaries

In the following, G will be typically a group $QR(n)$ of quadratic residues modulo n, where n is a safe RSA modulus, as defined in the next subsection. By definition, the group G is a group of possibly unknown order but where the size of the group order, denoted by l_G, is known.

[1] This is not the case for group of prime order.

2.1 Mathematical Background

A prime p is a safe prime when $p = 2p' + 1$ and p' is a prime. A safe RSA modulus n is an integer which is the product of two distinct safe primes $p = 2p' + 1$ and $q = 2q' + 1$, that is $n = pq$. The following technical lemma (see e.g. [17]) will be useful.

Lemma 1. *Let $n = pq$, where $p < q$, $p = 2p' + 1$, $q = 2q' + 1$, and p, q, p', q' are all prime numbers. Then,*

1. *The order of elements in $\mathbb{Z}_n^*$ is in $\{1, 2, p', q', 2p', 2q', p'q', 2p'q'\}$.*
2. *Given an element $w \in \mathbb{Z}_n^* \setminus \{-1, 1\}$ such that $ord(w) < p'q'$, then either $gcd(w-1, n)$ or $gcd(w+1, n)$ is a prime factor of n.*

As a consequence of the above lemma, any value found by a party that does not know (and cannot compute) the factorization of n must be of order at least $p'q'$ in $\mathbb{Z}_n^*$ (except for -1 and 1).

Lemma 2. *Let $n = pq$, where $p < q$, $p = 2p' + 1$, $q = 2q' + 1$, and p, q, p', q' are all prime numbers.*
If $\nu^2 = 1$ and $\nu \in QR(n)$ then $\nu = 1$.

Proof. As a safe modulus, n is also a Blum number (a product of two primes equal to $3 mod 4$). As a consequence, any element of $QR(n)$ has exactly one square root in $QR(n)$. Since 1 is in $QR(n)$, 1 is the only square root of 1 in $QR(n)$.

2.2 Number Theoretic Assumption

The security of discrete-logarithm based zero-knowledge proofs of knowledge in groups of unknown order relies on the Flexible RSA assumption (independently introduced by Barić and Pfitzmann [2] and by Fujisaki and Okamoto [16], also known as Strong RSA). This assumption can be stated as follows, restricted to safe modulus, as it is the case in our paper.

Assumption 1 (Flexible RSA) *Given a safe RSA modulus n and $\Gamma \in QR(n)$, it is infeasible to find $u \in \mathbb{Z}_n^*$ and $e \in \mathbb{Z}_{>1}$ such that $u^e = \Gamma \pmod{n}$, in time polynomial in $\lceil \log p'q' \rceil$ with a non-negligible probability.*

2.3 Zero-Knowledge Proofs of Knowledge

The notion of interactive zero-knowledge proof of knowledge has been formalized by Feige, Fiat and Shamir [14]. As in [20], we only consider honest verifier zero-knowledge since this is always the considered setting in studied complex constructions. Let us give the following (informal) definition.

Appeared in W. Susilo, J. K. Liu, Y. Mu (Eds.): ProvSec 2007, LNCS 4784,pp. 122–137, 2007.

Definition 1. *An interactive protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$, that takes on input $\mathcal{Y}$, is a zero-knowledge proof of knowledge of a secret x if the three following properties are verified.*

- *Completeness: given an honest prover $\mathcal{P}$ and an honest verifier $\mathcal{V}$, the protocol succeeds with overwhelming probability.*
- *Soundness: given a dishonest prover $\tilde{\mathcal{P}}$ that is accepted by a verifier $\mathcal{V}$ with non-negligible probability, it is possible to construct a probabilistic polynomial time Turing machine $\mathcal{M}$ that can find x by interacting with $\tilde{\mathcal{P}}$.*
- *(Honest verifier) zero-knowledge: it exists a probabilistic polynomial-time Turing machine that takes on input $\mathcal{Y}$ and which can simulate the communications between an honest prover $\mathcal{P}$ and an honest verifier $\mathcal{V}$ such that these simulated communications are indistinguishable from those between a real prover $\mathcal{P}$ and a real honest verifier $\mathcal{V}$.*

3 First Result on DLRS

Discrete-log relation sets (DLRS) were introduced by Kiayias *et al.* [20], and are useful when constructing complex proofs of knowledge for protocols operating over any group, even of unknown order. These constructions are quite useful in many complex cryptographic protocols [16, 1, 5, 9].

3.1 Introduction of the Concept of DLRS

The following definition of a DLRS has been proposed in [20]:

Definition 2. *(see [20]) Let G be a finite group. A discrete-log relation set R with z relations over r variables and m objects is a set of relations defined over the objects $A_1, \dots, A_m \in G$ and the free variables $\alpha_1, \dots, \alpha_r$ with the following specifications:*

1. *the i-th relation in the set R is specified by a tuple $\langle a_1^i, \dots, a_m^i \rangle$ so that each a_j^i is selected to be one of the free variables $\{\alpha_1 \dots, \alpha_r\}$ or an element of $\mathbb{Z}$. The relation is to be interpreted as $\prod_{j=1}^{m} A_j^{a_j^i} = 1$.*
2. *every free variable α_ω is assumed to take values in a finite integer range $]2^{l_\omega} - 2^{\mu_\omega}, 2^{l_\omega} + 2^{\mu_\omega}[$ where $l_\omega, \mu_\omega \geq 0$.*

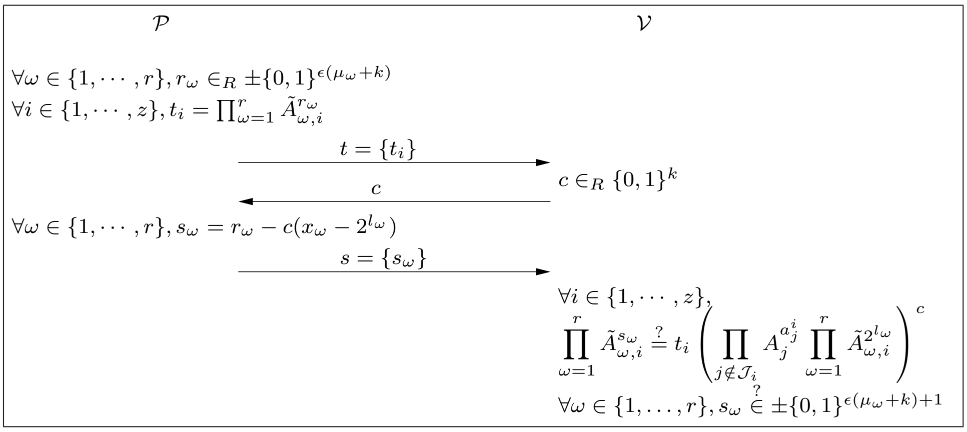
We will write $R(\alpha_1, \dots, \alpha_r)$ to denote the conjunction of all relations $\prod_{j=1}^{m} A_j^{a_j^i} = 1$ that are included in R.

Appeared in W. Susilo, J. K. Liu, Y. Mu (Eds.): ProvSec 2007, LNCS 4784,pp. 122–137, 2007.

Notation. The following notation will be used for the rest of the article. For the i-th relation, we define for each free variable α_ω ($\omega \in \{1, \ldots, r\}$) the set $\mathcal{J}_{\omega,i} \subseteq \{1, \ldots, m\}$ of the variable's locations in the tuple $\langle a_1^i, \ldots, a_m^i \rangle$. If a free variable α_ω is not contained in the relation i, the set $\mathcal{J}_{\omega,i}$ is empty. We also set $\mathcal{J}_i = \bigcup_{\omega=1}^{r} \mathcal{J}_{\omega,i}$. Note that $j \notin \mathcal{J}_i$ means $a_j^i \in \mathbb{Z}$. Finally, for all $\omega = 1, \ldots, r$, let us denote $\tilde{A}_{\omega,i} = \prod_{j \in \mathcal{J}_{\omega,i}} A_j$. Naturally, if $\mathcal{J}_{\omega,i} = \phi$ then $\tilde{A}_{\omega,i} = 1$. Consequently, the i-th relation verifies the following relation.

$$\prod_{j=1}^{m} A_j^{a_j^i} = 1 \ \Leftrightarrow \ \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{\alpha_\omega} \prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} = 1$$

Using these notations, a 3-move honest verifier zero-knowledge proof allows a prover that knows witnesses $x_1, \ldots, x_r$ such that $\forall \omega, x_\omega \in]2^{l_\omega} - 2^{\epsilon(\mu_\omega+k)+2}, 2^{l_\omega} + 2^{\epsilon(\mu_\omega+k)+2}[$ and $R(x_1, \ldots, x_r) = 1$ to prove knowledge of these values, is presented in [20] and shown in Figure 1, where ϵ and k are both security parameters such that $\epsilon > 1$ and $k \in \mathbb{N}$.



$\mathcal{P}$
$\mathcal{V}$
$\forall \omega \in \{1, \cdots, r\}, r_\omega \in_R \pm\{0,1\}^{\epsilon(\mu_\omega+k)}$
$\forall i \in \{1, \cdots, z\}, t_i = \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{r_\omega}$
$t = \{t_i\}$
$c \in_R \{0,1\}^k$
c
$\forall \omega \in \{1, \cdots, r\}, s_\omega = r_\omega - c(x_\omega - 2^{l_\omega})$
$s = \{s_\omega\}$
$\forall i \in \{1, \cdots, z\},$
$\prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{s_\omega} \overset{?}{=} t_i \left(\prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{2^{l_\omega}} \right)^c$
$\forall \omega \in \{1, \ldots, r\}, s_\omega \overset{?}{\in} \pm\{0,1\}^{\epsilon(\mu_\omega+k)+1}$

Fig. 1. Discrete-log Relation Set R

Remark 1. Note that the proof of knowledge of Figure 1 only proves that a witness $x \in]2^l - 2^\mu, 2^l + 2^\mu[$ lies in $]2^l - 2^{\epsilon(\mu+k)+2}, 2^l + 2^{\epsilon(\mu+k)+2}[$. If needed, Boudot presents in [4] a scheme that provides a perfect proof but with less efficiency. If the interval is small, it is also possible to use a bit-by-bit solution, such as in [3, 8].

3.2 The Result of Kiayias, Tsiounis and Yung

In [20], the authors present a particular case of our result. They prove the security of the construction of DLRS R presented in Figure 1 w.r.t. Definition 1 (see Section 2.3) in the case the relation R is *triangular*, and when G is the group $QR(n)$ of quadratic residue modulo n where n is a safe RSA modulus. In the following, G will also be this group. In the next section, we will prove the security of this construction in the general case. A triangular DLRS is introduced in [20] by the following definition.

Definition 3. *(see [20]) A discrete-log relation set R is* triangular *if for each relation i containing the $b+1$ free variables $\alpha_\omega, \alpha_{\omega_1}, \ldots, \alpha_{\omega_b}$ it holds that $\{\alpha_{\omega_1}, \ldots, \alpha_{\omega_b}\}$ is a subset of the union of all the free variables involved in relations $1, \ldots, i-1$.*

In this context, Kiayias *et al.* prove that the construction in Figure 1 is secure, i.e. for any triangular discrete-log relation set R the 3-move protocol of figure 1 is complete, sound and honest-verifier zero-knowledge.

3.3 On the Use of Kiayias, Tsiounis and Yung Result

If a complex proof of knowledge can be represented by a triangular discrete-log relation set, the construction of [20] is suitable. This is for example the case in the group signature scheme proposed by Ateniese et al. [1], where the DLRS is composed of the 9 objects $T_1, T_2, T_3, A, a_0, a, y, g, h$, the 4 free-variables $\alpha, \beta, \gamma, \delta$ such that the 4 relations $a_0 = T_1^\alpha/(a^\beta y^\gamma) \wedge T_2 = g^\delta \wedge 1 = T_2^\alpha/g^\gamma \wedge T_3 = g^\alpha h^\delta)$ are verified in order to produce a signature.

But, in some cases, their approach cannot be applied. For example, the construction of [5] uses a DLRS with 8 objects $(C, C_1, C_2, C_3, g, h, 1/g, 1/h)$ and 11 variables $(\alpha, \beta, \gamma, \delta, \eta, \zeta, \phi, \psi, \theta, \sigma, \nu)$ verifying the following conjunction of the 7 relations

$$C = g^\alpha h^\phi \wedge g = \left(\frac{C}{g}\right)^\gamma h^\psi \wedge g = (gC)^\sigma h^\nu \wedge C_3 = g^\zeta h^\eta$$
$$\wedge C_1 = g^\alpha h^\theta \wedge v = C_2^\alpha \left(\frac{1}{h}\right)^\beta \wedge 1 = C_3^\alpha \left(\frac{1}{h}\right)^\delta \left(\frac{1}{g}\right)^\beta .$$

This DLRS clearly cannot be represented by a triangular discrete-log relation set.

This is also the case for [9] and more simply if Alice wants to commit to the value x using the Fujisaki-Okamoto construction [16], and that she knows the commited value. The latter can be done by computing

$PK(\alpha, \beta : C = g^{\alpha}h^{\beta})$, that is a DLRS R of 1 relation over 2 variables and 3 objects.

Consequently, there is sometimes more than one new free-variable at each new relation. More generally speaking, when a discrete-log relation set R is not triangular, then for each relation i containing the free variables $\alpha_{\tilde{\omega}_1}, \ldots, \alpha_{\tilde{\omega}_d}, \alpha_{\omega_1}, \ldots, \alpha_{\omega_b}$ it holds that the free variables $\alpha_{\omega_1}, \ldots, \alpha_{\omega_b}$ were contained in the union of all the free variables involved in relations $1, \ldots, i-1$. But that does not imply that the construction proposed in Figure 1 does not suit the general case. What lacks is a security proof for this construction in the general setting: the result of Kiayias *et al.* [20] cannot be used as it is in the general case.

4 Generalization of the DLRS Theorem

In the general setting, the proof of completeness and honest-verifier zero-knowledge are not different to the one described in [20]. They will consequently not be treated in this paper. On the contrary, the proof of soundness of [20] must be deeply modified to suit the model considering any kind of DLRS, not only the triangular ones. This adaptation is the actual contribution of this paper.

An interactive protocol between a prover $\mathcal{P}$ and a verifier $\mathcal{V}$ verifies the soundness property if a dishonest prover $\tilde{\mathcal{P}}$ can not be accepted by a verifier $\mathcal{V}$ with non-negligible probability. Generally, a probabilistic polynomial time Turing machine $\mathcal{M}$ that can find x by interacting with $\tilde{\mathcal{P}}$ is constructed to prove this property.

4.1 Our Result in a Nutshell

In this section, we briefly present our proof of soundness for all kinds of DLRS. The global structure of our proof is described in Figure 2.

In the first step, we assume that there exists $\tilde{\mathcal{P}}$ able to produce, with non-negligible probability, valid proofs of knowledge without knowing the secret values $X = \{x_1, \ldots, x_s\}$. Our aim is to construct a p.p.t. Turing machine $\mathcal{M}$ which, for each equation, is able to solve a given instance of the Flexible RSA problem (FRSA).

We first give an instance $(n, \varGamma)$ of the Flexible RSA problem to $\mathcal{M}$. $\mathcal{M}$ generates a random DLRS R, function of this instance. We then ask $\tilde{\mathcal{P}}$ to produce a valid proof of knowledge until we obtain two valid conversations $\langle t, c, s\rangle, \langle t, c^*, s^*\rangle$, where $c \neq c^*, t = \{t_1, \ldots, t_z\}, s = \{s_1, \ldots, s_r\}, s^* = \{s_1^*, \ldots, s_r^*\}$. We also denote $\tilde{s}_i = s_i - s_i^*$ for all i, $\tilde{S} = \{\tilde{s}_1, \ldots, \tilde{s}_r\}$ and

$\tilde{c} = c - c^*$.

From these relations, $\mathcal{M}$ then computes for each of the z relations an independent equation only depending on c, c^*, s and s^*. Each couple (s_i, s_i^*) is related to a free variable, and thus to a secret. Our aim is then to retrieve the value of all secrets.

In a similar way to [20], the machine $\mathcal{M}$ always operates as follows.

1. For each of the z relations, it first pushes aside the couples (s_i, s_i^*) for which the secret has already been retrieved. This step is not done for the first relation.
2. It then calculates the number of secrets that are unknown in the relation. Depending on it, there are three cases.
   (a) There is only one unknown secret. This is the case that has been studied in [20]. In fact, if, for each relation, there is only one unknown secret, the DLRS is then triangular. The conclusion is that either we can compute all secret or we can solve the instance $(n, \mathit{\Gamma})$ of the Flexible RSA problem.
   (b) There are two unknown secrets. This case corresponds to the ZKPK of a representation. In a group of unknown order, the case has been studied in [13], using the Root assumption. We thus adapt it by using the Flexible RSA assumption. The conclusion is that either we can compute all secrets or we can solve the instance $(n, \mathit{\Gamma})$ of the Flexible RSA problem.
   (c) The general case (up to three but the cases 1 and 2 can also be seen as particular cases) is the one we study in this paper. The relation can thus be denoted as $\tilde{A}_1^{\tilde{s}_1} \dots \tilde{A}_d^{\tilde{s}_d} = \mathit{\Psi}_i^{\tilde{c}}$. $\tilde{A}_1, \dots, \tilde{A}_d$ correspond to the objects defined after the DLRS definition (see Section 3) and $\mathit{\Psi}_i$ is the product of a constant element and possibly some objects $\tilde{\mathcal{A}}_j$ raised to the power of secret values already compute. $\tilde{c}, \tilde{S}$ are dependant of c, c^*, S, S^*.
   We then study two cases. In the first one, $\mathcal{M}$ retrieves all secrets involved in this relation. The second case is also divided into two possible cases.
      i. $\mathcal{M}$ can solve the instance $(n, \mathit{\Gamma})$ of the FRSA problem.
      ii. We prove that the second case only happens with probability less than 1/2.

   If $\mathcal{M}$ is able to find all the secret values, $\tilde{\mathcal{P}}$ can also do it. So, under the assumption that $\tilde{\mathcal{P}}$ does not know these values, we conclude that $\mathcal{M}$ solves the given instance of the Flexible RSA problem.

In all papers where there is a ZKPK in the group of unknown order $QR(n)$, such as in the paper of Kiayias, Tsiounis and Yung [20] but also

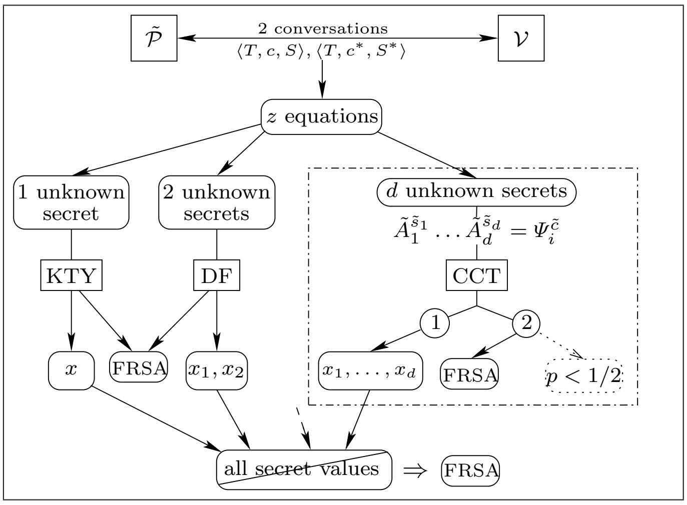


Fig. 2. Sketch of proof

e.g. in [1, 6], a p.p.t. Turing machine $\mathcal{M}$ is constructed so as to solve with a non-negligible probability an instance of the Flexible RSA problem. However, this instance is never specified so that it could possibly be an easy instance of the problem.

More precisely, the solved instance corresponds to the modular multiplication of public parameters (the A_i's) but nothing is said about the difficulty of solving the Flexible RSA on one A_i nor on the modular multiplication of some of them. It seems better, and that's what we do in our proof, to introduce a challenger $\mathcal{C}$ which gives to $\mathcal{M}$ a random instance of the Flexible RSA problem at the beginning of the proof.

Nevertheless, as we will see in our proof, $\mathcal{M}$ will need to interact possibly with several dishonest provers $\tilde{\mathcal{P}}$, depending on the objects $A_1, \dots, A_m$ the machine $\mathcal{M}$ has to use to solve the Flexible RSA instance. The number z of relations and the number r of free variables can be unchanged between all the interactions. This consequently implies the use of an attacker $\tilde{\mathcal{P}}$ being able to break the soundness of a DLRS for a polynomial number of tuples $A_1, \dots, A_m$.

4.2 The New Theorem

We can then introduce our new theorem and prove the security of the construction in Figure 1 in the case of any discrete-log relation set.

Theorem 1. *Let $G = QR(n)$ where $n(= (2p' + 1)(2q' + 1))$ is safe. For any discrete-log relation set R the 3-move protocol of Figure 1 is a honest-verifier zero-knowledge proof of knowledge that can be used by a first party (prover) knowing a witness for R to prove knowledge of the witness to a second party (verifier).*

Proof. We have to prove that the protocol of Figure 1 verifies the three properties of completeness, soundness and honest verifier zero-knowledge. The proof of completeness and honest verifier zero-knowledge can be found in [20]. They will not be treated in this proof. The proof of soundness of [20] must be modified to suit our model (all kinds of DLRS, not only the triangular ones).

Assume it exists a dishonest prover $\tilde{\mathcal{P}}$ attacking the soundness of the protocol presented in Figure 1. It means that $\tilde{\mathcal{P}}$ is able to produce valid conversations for this protocol with non-negligible probability, and without knowing all the involved secrets. We define a p.p.t. Turing machine $\mathcal{M}$ which solves a given instance of the Flexible RSA problem, using $\tilde{\mathcal{P}}$ as an oracle. Let $\mathcal{C}$ be the challenger who gives the instance (n, Γ) of the Flexible RSA problem to $\mathcal{M}$. The Turing machine $\mathcal{M}$:

- takes on input the instance (n, Γ) of the FRSA problem given by $\mathcal{C}$,
- generates a random DLRS R,
- interacts with $\tilde{\mathcal{P}}$,
- solves the given instance using $\tilde{\mathcal{P}}$'s outputs.

In order to define R, $\mathcal{M}$ randomly chooses integers $\gamma_\omega \in \{1, \ldots, n^2\}$ and computes $A_\omega = \Gamma^{\gamma_\omega}$, for $\omega \in \{1, \ldots, m\}$. Under the factorisation assumption, the order of Γ is $\phi(n)/4$ and consequently, the A_ω are distributed over $QR(n)$. $\mathcal{M}$ sends R to the dishonest prover $\tilde{\mathcal{P}}$. Let $\langle t_1, \ldots, t_z, c, s_1, \ldots, s_r\rangle$ and $\langle t_1, \ldots, t_z, c^*, s_1^*, \ldots, s_r^*\rangle$, with $c \neq c^*$, be two accepted protocols for R between $\tilde{\mathcal{P}}$ and an (honest) verifier. As these protocols are valid, both following relations are true for all $i \in \{1, \ldots, z\}$:

$$\prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{s_\omega} = t_i \left(\prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{2^{l_\omega}} \right)^{c} \quad \text{and} \quad \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{s_\omega^*} = t_i \left(\prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{2^{l_\omega}} \right)^{c^*}$$

$$\Rightarrow \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{s_\omega - s_\omega^*} = \left(\prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} \prod_{\omega=1}^{r} \tilde{A}_{\omega,i}^{2^{l_\omega}} \right)^{c-c^*} . \qquad (1)$$

The proof consists now in proving that using relations (1) for all $i \in \{1, \ldots, z\}$, $\mathcal{M}$ is able to solve the given instance of the Flexible RSA problem. First, we introduce the notations we will use in the following of the proof. For $\omega \in \{1,\ldots,r\}$: $\tilde{s}_\omega := s_\omega - s^*_\omega$, and $\tilde{c} := c - c^*$. We also introduce the sets of distinct integers $\Omega_i = \{\omega_{i,1},\ldots,\omega_{i,d}\}$, for each relation i (i.e. for i from 1 to z), such that the free variables $\alpha_{\omega_{i,1}},\ldots,\alpha_{\omega_{i,d}}$ are the ones involved in the i-th relation. Using these notations, for $i \in \{1,\ldots,z\}$, the relation (1) can be written:

$$\prod_{\omega\in\Omega_i} \tilde{A}_{\omega,i}^{\tilde{s}_\omega} = \left(\prod_{j\notin\mathcal{J}_i} A_j^{a_j^i} \prod_{\omega\in\Omega_i} \tilde{A}_{\omega,i}^{2^{l_\omega}}\right)^{\tilde{c}} . \tag{2}$$

Relation 1. Considering the first relation, there are two cases:

- $\tilde{c}$ divides all the integers $\tilde{s}_\omega$

  The particular case where $d = 1$ (as in [20]) is included in the general case. So we restrict our proof to the general case, where $d \geq 1$. It holds that the first relationship in R involves d free variables denoted by α_ω for $\omega \in \Omega_1 = \{\omega_{1,1},\ldots,\omega_{1,d}\}$. In this case, we have the following relation, where $\tilde{A}_\omega$ stands for $\tilde{A}_{\omega,1}$:

$$\prod_{\omega\in\Omega_1} \tilde{A}_\omega^{\tilde{s}_\omega} = \left(\prod_{\omega\in\Omega_1} \tilde{A}_\omega^{2^{l_\omega}} \prod_{j\notin\mathcal{J}_1} A_j^{a_j^1}\right)^{\tilde{c}} .$$

  As $\tilde{c}$ divides $\tilde{s}_\omega$, for all $\omega \in \Omega_1$, the previous relation becomes (see remark below):

$$\prod_{\omega\in\Omega_1} \tilde{A}_\omega^{\frac{-\tilde{s}_\omega}{\tilde{c}}+2^{l_\omega}} \prod_{j\notin\mathcal{J}_1} A_j^{a_j^1} = 1. \tag{3}$$

  Remark 2. In fact, we have the following equivalence :

$$\prod_{\omega\in\Omega_1} \tilde{A}_\omega^{\tilde{s}_\omega} = \left(\prod_{\omega\in\Omega_1} \tilde{A}_\omega^{2^{l_\omega}} \prod_{j\notin\mathcal{J}_1} A_j^{a_j^1}\right)^{\tilde{c}} \Leftrightarrow \prod_{\omega\in\Omega_1} \tilde{A}_\omega^{\frac{\tilde{s}_\omega}{\tilde{c}}} = \nu \prod_{\omega\in\Omega_1} \tilde{A}_\omega^{2^{l_\omega}} \prod_{j\notin\mathcal{J}_1} A_j^{a_j^1},$$

  with $\nu^c = 1$. Indeed, by definition $\tilde{c} < 2^k$ and thus $\tilde{c} < min(p,q)$. By Lemma 1, we can then affirm that the order of ν can only be equal to 1 or 2 and by lemma 2, that ν can only be equal to 1. We will not repeat this remark later, even when it holds.

The equality 3 implies that we have constructed the d witnesses for each ω-th variable $\tilde{x}_\omega = \frac{\tilde{s}_\omega}{\tilde{c}} + 2^{l_\omega} = \frac{s_\omega - s^*_\omega}{c - c^*} + 2^{l_\omega}$ where $\omega \in \Omega_1$.
We verify that these values are in the right interval. For $\omega \in \Omega_1$, $\tilde{s}_\omega \in \pm\{0,1\}^{\epsilon(\mu_\omega + k)+2}$ (since $s_\omega, s^*_\omega \in \pm\{0,1\}^{\epsilon(\mu_\omega+k)+1}$, it implies that $s^*_\omega - s_\omega \in \pm\{0,1\}^{\epsilon(\mu_\omega+k)+2}$) it follows that $\frac{\tilde{s}_\omega}{\tilde{c}} \in \pm\{0,1\}^{\epsilon(\mu_\omega+k)+2}$ and as a result $\tilde{x}_\omega \in]2^{l_\omega} - 2^{\epsilon(\mu_\omega+k)+2}, 2^{l_\omega} + 2^{\epsilon(\mu_\omega+k)+2}[$. Consequently, $\mathcal{M}$ finds the secrets $\{\tilde{x}_\omega\}\ for\ \omega \in \Omega_1$ in polynomial time, $\tilde{\mathcal{P}}$ can also find it. So we can assume that $\tilde{\mathcal{P}}$ already knows it.

- It exists at least one integer $\omega \in \Omega_1$ such that $\tilde{c}$ does not divide $\tilde{s}_\omega$.

Now, we prove that $\mathcal{M}$ solves the given instance (n, Γ) of the FRSA problem on G. Let

$$T_1 = \left(\prod_{\omega \in \Omega_1} \tilde{A}_\omega^{2^{l_\omega}} \prod_{j \notin \mathcal{J}_1} A_j^{a_j^1} \right).$$

For all j in $\{1, \ldots, d\}$, $A_j = \Gamma^{\gamma_j}$, and for all $\omega \in \Omega_1$, we have $\tilde{A}_\omega = \prod_{j \in \mathcal{J}_{\omega,1}} A_j = \prod_{j \in \mathcal{J}_{\omega,1}} \Gamma^{\gamma_j} = \Gamma^{\sum_{j \in \mathcal{J}_{\omega,1}} \gamma_j}$. We define $\theta_\omega = \sum_{j \in \mathcal{J}_{\omega,1}} \gamma_j \pmod{n^2}$ for all $\omega \in \Omega_1$. Consequently, with those notations relation (2) becomes:

$$\prod_{\omega \in \Omega_1} \left(\Gamma^{\sum_{j \in \mathcal{J}_{\omega,1}} \gamma_j} \right)^{\tilde{s}_\omega} = T_1^{\tilde{c}} \quad \Leftrightarrow \quad \Gamma^{\sum_{\omega \in \Omega_1} \theta_\omega \tilde{s}_\omega} = T_1^{\tilde{c}}. \tag{4}$$

Without loss of generality, we assume that integers $\tilde{s}_{1,1}, \ldots, \tilde{s}_{1,d_1}$ are divisible by $\tilde{c}$, as opposed to integers $\tilde{s}_{1,d_1+1}, \ldots, \tilde{s}_{1,d_2}$, with $1 \leq d_1 < d_2 = d$. If $d_2 = 1$, because we assumed that $\tilde{c}$ does not divide all the $\tilde{s}_\omega$, then $d_1 = 0$.
Then there are two cases:

1. If $\tilde{c}$ does not divide $\sum_{\omega \in \Omega_1} \theta_\omega \tilde{s}_\omega$, $\mathcal{M}$ can solve the given instance of the Flexible RSA problem as follows. Let δ be the greatest common divisor of $\tilde{c}$ and $\sum_{\omega \in \Omega_1} \theta_\omega \tilde{s}_\omega$. There exist α and β in $\mathbb{Z}$ such that $\alpha\tilde{c} + \beta\big(\sum_{\omega \in \Omega_1} \theta_\omega \tilde{s}_\omega\big) = \delta$. It follows that

$$\Gamma = \Gamma^{\left(\alpha\tilde{c} + \beta(\sum_{\omega \in \Omega_1} \theta_\omega \tilde{s}_\omega)\right)/\delta} = (\Gamma^\alpha T_1^\beta)^{\tilde{c}/\delta}.$$

By assumption, $\delta < \tilde{c}$ and so, we can set $e = \tilde{c}/\delta$ and $u = \Gamma^\alpha T_1^\beta$, which is a solution of the Flexible RSA problem on G relatively to the instance (n, Γ).

Remark 3. This part of the proof works with any values of the integer $d_1 < d_2$.

2. If $\tilde{c}$ divides $\sum_{\omega\in\Omega_1}\theta_\omega\tilde{s}_\omega$, we prove that, as $\tilde{\mathcal{P}}$ does not have complete information about the θ_ω's, this case only happens with probability less or equal to 1/2. Consequently, case (1) happens with probability greater than 1/2 and the probability to break the Flexible RSA assumption is greater than 1/2. The strategy consists in choosing the θ_ω's until we get back on case (1). This quickly happens in a bounded time with non-negligible probability.
   Let f be a prime factor of $\tilde{c}$ and e an integer such that:
   - f^e is the greatest power of f that divides $\tilde{c}$,
   - at least one of the $\tilde{s}_\omega$ is non-zero modulo f^e.

   This value must exist since $\tilde{c}$ does not divide at least one of the $\tilde{s}_\omega$, even if $d_2 = 1$. For all $\omega\in\Omega_1$, we define $b_\omega = \theta_\omega \pmod{\operatorname{ord}(G)}$ and h_ω such that $\theta_\omega = b_\omega + h_\omega\operatorname{ord}(G)$. Note that the $\tilde{A}_{\omega,1}$'s represent all the information the machine $\tilde{\mathcal{P}}$ knows about the θ_ω's and the b_ω's are uniquely determined from the $\tilde{A}_{\omega,1}$'s, whereas the h_ω's are completely unknown. As f^e divides $\sum_{\omega\in\Omega_1}\theta_\omega\tilde{s}_\omega$ (since $\tilde{c}$ does), it follows that

   $$\sum_{\omega\in\Omega_1}\theta_\omega\tilde{s}_\omega = 0 \pmod{f^e} \text{ and } \sum_{j=1}^{d_2}\theta_{\omega_{1,j}}\tilde{s}_{\omega_{1,j}} = 0 \pmod{f^e}.$$

   We know that for j from 1 to d_1, $\tilde{s}_{\omega_{1,j}} \equiv 0 \pmod{f^e}$ as they are divisible by $\tilde{c}$, consequently, $\sum_{j=1}^{d_1}\theta_{\omega_{1,j}}\tilde{s}_{\omega_{1,j}} \equiv 0 \pmod{f^e}$.

   $$\sum_{j=d_1+1}^{d_2} b_{\omega_{1,j}}\tilde{s}_{\omega_{1,j}} + \operatorname{ord}(G)\sum_{j=d_1+1}^{d_2} h_{\omega_{1,j}}\tilde{s}_{\omega_{1,j}} = 0 \pmod{f^e}. \quad (5)$$

   Since $f^e \le 2^k \le min(p', q'$, we have $|G| \ne 0 \pmod{f}$. $\tilde{\mathcal{P}}$ does not know anything about the h_ω's except that they follow the uniform distribution and that they satisfy equation (5). Let $\tilde{\omega}$ be one of the indexes such that $\tilde{s}_{\tilde{\omega}}$ is not divisible by f^e. If $d_2 = 1$, it is evident that $\tilde{\omega} = 1$. If we fix the h_ω's for $\omega\in\Omega_1/\{\tilde{\omega}\}$, then the number of solutions modulo f^e of the equation (5) is at most $gcd(|G|\tilde{s}_{\tilde{\omega}}, f^e)$. This number is necessarily a power of f, since f^e does not divide $|G|\tilde{s}_{\tilde{\omega}}$, and at most f^{e-1}. Since for all $\omega\in\Omega_1$, θ_ω has been chosen from a large interval, the distribution of b_ω is statistically indistinguishable from the uniform distribution on $\mathbb{Z}_{p'q'}$. Moreover the distribution of h_ω is statistically indistinguishable from the uniform distribution on $\{0,\ldots,M\}$, where $M = \lfloor n^2/p'q' \rfloor$. Thus, there are nearly M^{d_2} possible tuples $\langle h_1,\ldots,h_{d_2}\rangle$ uniformly distributed [12].

Let $\mathsf{w} \in \mathbb{R}$ such that $M = \mathsf{w}f^e$. The number of solutions of the equation is at most $[\mathsf{w}f^{e-1}]M^{d_2-1}$, hence the probability that the h_ω's verify the equation is at most

$$\frac{[\mathsf{w}f^{e-1}]M^{d_2-1}}{M^{d_2}} \leq \frac{\mathsf{w}f^{e-1}}{M} \leq \frac{\mathsf{w}f^{e-1}}{\mathsf{w}f^e} \leq \frac{1}{f} \leq \frac{1}{2}$$

We can then solve the instance of the Flexible RSA problem with non-negligible probability.

If $\tilde{\mathcal{P}}$ outputs integers $\tilde{c}, \tilde{s}_1, \ldots, \tilde{s}_r$ such that relation (4) is verified and at least one of the $\tilde{s}_\omega$ is not divisible by $\tilde{c}$, for $\omega \in \Omega_1$, then $\mathcal{M}$ solves the given instance of the Flexible RSA problem.

Relation *i*. Now, we assume that we have processed all the relations with index less than i and $\mathcal{M}$ did not already solve the instance of the FRSA problem. We process the i-th relation which involves variables α_ω, for all $\omega \in \Omega_i (= \{\omega_{i,1}, \ldots, \omega_{i,d}\})$. As we have processed all the relations with index less than i, some of these variables are already known. We split Ω_i in two sets of integers $\Omega_{i,1} = \{\omega_{i,1}, \ldots, \omega_{i,d_2}\}$ and $\Omega_{i,2} = \{\omega_{i,d_2+1}, \ldots, \omega_{i,d}\}$ so that the variables α_ω, for $\omega \in \Omega_{i,2}$ are already contained in previous relations. We assume that these variables are known by $\mathcal{M}$ and then by $\tilde{\mathcal{P}}$. By an inductive argument, we construct witnesses for the free-variables $\tilde{x}_\omega = \frac{-\tilde{s}_\omega}{\tilde{c}} + 2^{l_\omega} = \frac{s^*_\omega - s_\omega}{c - c^*} + 2^{l_\omega}$, and $\tilde{c}$ divides $\tilde{s}_\omega$, for all $\omega \in \Omega_{i,2}$. There are again two cases:

- $\tilde{c}$ divides $\tilde{s}_\omega$, for all $\omega \in \Omega_{i,1}$
  First, we study the particular case where $d_2 = 1$ (see also [20]): the i-th relation in R involves variables $\alpha_{\omega_{i,1}}, \ldots, \alpha_{\omega_{i,d}}$, where $\alpha_{\omega_{i,1}}$ is the only one for which the witness associated is not yet constructed. Using relation (2), the i-th relation becomes, where $\tilde{A}_\omega$ stands for $\tilde{A}_{\omega,i}$:

$$\tilde{A}_{\omega_{i,1}}^{\tilde{s}_{\omega_{i,1}}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{\tilde{s}_\omega} = \left(\tilde{A}_{\omega_{i,1}}^{2^{l_{\omega_{i,1}}}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{2^{l_\omega}} \prod_{j \notin \mathcal{J}_i} A_j^{a^i_j} \right)^{\tilde{c}}$$

$$\tilde{A}_{\omega_{i,1}}^{\tilde{s}_{\omega_{i,1}}} = \left(\tilde{A}_{\omega_{i,1}}^{2^{l_{\omega_{i,1}}}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{\tilde{x}_\omega} \prod_{j \notin \mathcal{J}_i} A_j^{a^i_j} \right)^{\tilde{c}}.$$

  As $\tilde{c}$ divides $s_{\omega_{i,1}}$ we obtain the following relation :

$$\tilde{A}_{\omega_{i,1}}^{\frac{-\tilde{s}_{\omega_{i,1}} + 2^{l_{\omega_{i,1}}}}{\tilde{c}}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{x_\omega} \prod_{j \notin \mathcal{J}_i} A_j^{a^i_j} = 1.$$

The above equality implies that we have constructed the witness for the variables $\tilde{x}_{\omega_{i,1}} = \frac{-\tilde{s}_{\omega_{i,1}}}{\tilde{c}} + 2^{l_{\omega_{i,1}}} = \frac{s^*_{\omega_{i,1}} - s_{\omega_{i,1}}}{c-c^*} + 2^{l_{\omega_{i,1}}}$. As previously, it is possible to show that this witness is in the right interval, i.e. $\tilde{x}_{\omega_{i,1}} \in]2^{l_{\omega_{i,1}}} - 2^{\epsilon(\mu_{\omega_{i,1}}+k)+2}, 2^{l_{\omega_{i,1}}} + 2^{\epsilon(\mu_{\omega_{i,1}}+k)+2}[$. We can also assume in this case that $\tilde{\mathcal{P}}$ already knows this witness.

Now, we study the general case where $d_2 \neq 1$: the i-th relation in R involves variables $\alpha_{\omega_1}, \ldots, \alpha_{\omega_d}$ so that variables $\alpha_{\omega_{d_2+1}}, \ldots, \alpha_{\omega_d}$ were already contained in previous relations. So the associated witnesses are known by $\tilde{\mathcal{P}}$. Using relation (2), the i-th relation becomes:

$$\prod_{\omega \in \Omega_{i,1}} \tilde{A}_\omega^{\tilde{s}_\omega} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{\tilde{s}_\omega} = \left(\prod_{\omega \in \Omega_{i,1}} \tilde{A}_\omega^{2^{l_\omega}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{2^{l_\omega}} \prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} \right)^{\tilde{c}} \tag{6}$$

$$\prod_{\omega \in \Omega_{i,1}} \tilde{A}_\omega^{\tilde{s}_\omega} = \left(\prod_{\omega \in \Omega_{i,1}} \tilde{A}_\omega^{2^{l_\omega}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{\tilde{x}_\omega} \prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} \right)^{\tilde{c}} . \tag{7}$$

As $\tilde{c}$ divides s_ω for all $\omega \in \Omega_{i,1}$ we obtain the following relation:

$$\prod_{\omega \in \Omega_{i,1}} \tilde{A}_\omega^{\frac{-\tilde{s}_\omega + 2^{l_\omega}}{\tilde{c}}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{x_\omega} \prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} = 1.$$

The above equality implies that we have constructed d_2 witnesses for each ω-th variable $\tilde{x}_\omega = \frac{-\tilde{s}_\omega}{\tilde{c}} + 2^{l_\omega} = \frac{s^*_\omega - s_\omega}{c-c^*} + 2^{l_\omega}$, for all $\omega \in \Omega_{i,1}$. As previously, it is possible to show that these witnesses are in the right intervals, i.e. $\tilde{x}_\omega \in]2^{l_\omega} - 2^{\epsilon(\mu_\omega+k)+2}, 2^{l_\omega} + 2^{\epsilon(\mu_\omega+k)+2}[$, for all $\omega \in \Omega_{i,1}$. We can also assume in this case that $\tilde{\mathcal{P}}$ already knows those witnesses.

- It exists at least one integer $\omega \in \Omega_{i,1}$ such that $\tilde{c}$ does not divide $\tilde{s}_\omega$. Like in part (4.2), we have to prove that $\mathcal{M}$ can solve the given instance (n, Γ) of the Flexible RSA problem on G. As in the previous part, the relation (7) is true. Let $T_i = \left(\prod_{\omega \in \Omega_{i,1}} \tilde{A}_\omega^{2^{l_\omega}} \prod_{\omega \in \Omega_{i,2}} \tilde{A}_\omega^{\tilde{x}_\omega} \prod_{j \notin \mathcal{J}_i} A_j^{a_j^i} \right)$.
  As in part (4.2), we have, for all $\omega \in \Omega_{i,1}$, $\tilde{A}_\omega = \Gamma^{\sum_{j \in \mathcal{J}_{\omega,i}} \gamma_j}$, and we define $\theta_\omega = \sum_{j \in \mathcal{J}_{\omega,i}} \gamma_j$, for all $\omega \in \Omega_{i,1}$. With those notations, relation (7) becomes $\Gamma^{\sum_{\omega \in \Omega_{i,1}} \theta_\omega \tilde{s}_\omega} = T_i^{\tilde{c}}$. This relation has exactly the same form than relation (4). Then, it is possible to conclude similarly that $\mathcal{M}$ solves the given instance of the Flexible RSA problem on G with a non-negligible probability.

In conclusion, $\mathcal{M}$ will not be able to solve the given instance (n, Γ) of the Flexible RSA problem only if $\tilde{c}$ divides all integers $\tilde{s}_1, \ldots, \tilde{s}_r$. But in this case, it is necessary that $\tilde{\mathcal{P}}$ knows all the witnesses involved in the protocol, which is infeasible by assumption. Consequently, $\mathcal{M}$ necessarily solves the given instance (n, Γ) if it obtains as input two valid conversations from $\tilde{\mathcal{P}}$. Since the machine $\mathcal{M}$ interacts a polynomial number of times with $\tilde{\mathcal{P}}$ which runs in polynomial time, $\mathcal{M}$ solves the random instance of the Flexible RSA problem in polynomial time. Thus, under the Flexible RSA assumption, $\tilde{\mathcal{P}}$ cannot product valid conversations for the protocol of Figure 1, then the soundness of the DLRS is proved.

5 Conclusion

We have proved that many complex discrete-logarithm protocols in groups of unknown order are ZKPK under the Flexible RSA assumption. A result by Kiayias, Tsiounis and Yung appears as a particular case of our construction. It is possible to extend the work done in this paper to signature schemes using the Fiat-Shamir heuristic [15]. The security of the construction can then be proven by using the result of [21].

There is still some work to do since complex cryptographic constructions can also use ZKPK of secret values verifying some different properties not studied in this paper such as *e.g.* the proof of the "or" statement and the proof of equality of two discrete logarithms in different groups.

Acknowledgements

We are grateful to Marc Girault for his suggestions of improvement, and to anonymous referees for their valuable comments. This work has been partially financially supported by the European Commission through the IST Program under Contract IST-2002-507932 ECRYPT.

References

1. G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-Resistant Group Signature Scheme. Crypto'2000, volume 1880 of LNCS, pages 255-270. Springer-Verlag, 2000.
2. N. Barić and B. Pfitzmann. Collision-Free Accumulators and Fail-Stop Signature Schemes Without Trees, Eurocrypt'97, volume 1233 of LNCS, pages 480-484. Springer-Verlag, 1997.
3. M. Bellare and S. Goldwasser. Verifiable Partial Key Escrow. ACM CCS'97, pages 78-91. ACM Press, 1997.
4. F. Boudot. Efficient Proofs that a Committed Number Lies in an Interval. Eurocrypt 2000, volume 1807 of LNCS, pages 431-444. Springer-Verlag, 2000.

Appeared in W. Susilo, J. K. Liu, Y. Mu (Eds.): ProvSec 2007, LNCS 4784,pp. 122–137, 2007.

5. J. Camenisch and A. Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. Crypto 2002, volume 2442 of LNCS, pages 61-76. Springer-Verlag, 2002.
6. J. Camenisch and M. Michels. A Group Signature Scheme Based on an RSA-Variant. Asiacrypt'98, volume 1514 of LNCS, pages 160-174. Springer-Verlag, 1998.
7. J. Camenisch and M. Michels. Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. Eurocrypt'99, volume 1592 of LNCS, pages 107-122. Springer-Verlag, 1999.
8. S. Canard, A. Gouget, and E. Hufschmitt. A Handy Muti-Coupon System. ACNS 2006, volume 3089 of LNCS, pages 66-81. Springer-Verlag, 2006.
9. S. Canard and J. Traoré. On Fair E-cash Systems based on Group Signature Schemes. ACISP 2003, volume 2727 of LNCS, pages 237-248. Springer-Verlag, 2003.
10. A.H. Chan, Y. Frankel, and Y. Tsiounis. Easy Come - Easy Go Divisible Cash. Eurocrypt'98, volume 1403 of LNCS, pages 561-575. Springer-Verlag, 1998.
11. D. Chaum and T. Pedersen. Transferred Cash Grows in Size. Eurocrypt'92, volume 658 of LNCS, pages 390-407. Springer-Verlag, 1993.
12. R. Cramer and V. Shoup. Signature Schemes Based on the Strong RSA Assumption, ACM TISSEC 3(3), pages 161-185. ACM Press, 2000.
13. I. Damgård and E. Fujisaki, A Statistically-Hiding Integer Commitment Scheme Based on Groups with Hidden Order, Asiacrypt 2002, volume 2501 of LNCS, pages 143-159. Springer-Verlag, 2002.
14. U. Feige, A. Fiat, and A. Shamir. Zero-knowledge Proofs of Identity. Journal of Cryptology, 1(2), pages 77-94. 1988.
15. A. Fiat and A. Shamir. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. Crypto'86, volume 263 of LNCS, pages 186-194. Springer-Verlag, 1987.
16. E. Fujisaki and T. Okamoto. Statistical Zero-Knowledge Protocols Solution to Identification and Signature Problems. Crypto'97, volume 1294 of LNCS, pages 16-30. Springer-Verlag, 1997.
17. R. Gennaro, T. Rabin, and H. Krawczyk. RSA-Based Undeniable Signatures, Journal of Cryptology, 13(4), pages 397-416. 2000.
18. M. Girault, G. Poupard, and J. Stern. On the Fly Authentication and Signature Schemes Based on Groups of Unknown Order. Journal of Cryptology, 19(4), pages 463-487. 2006.
19. S. Goldwasser, S. Micali, and C.W. Rackoff. The Knowledge Complexity of Interactive Proof Systems. SIAM Journal of Computing, vol. 18(1), pages 186-208. 1989.
20. A. Kiayias, Y. Tsiounis, and M. Yung. Traceable Signatures. Eurocrypt'04, volume 3027 of LNCS, pages 571-589. Springer-Verlag, 2004. Extended version at e-print cryptology archive report 2004/007, http://eprint.iacr.org/.
21. D. Pointcheval and J. Stern. Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 13(3), pages 361-396. 2000.
22. C. P. Schnorr. Efficient Signature Generation for Smart Cards. Journal of Cryptology, 4(3), pages 239-252. 1991.

Appeared in W. Susilo, J. K. Liu, Y. Mu (Eds.): ProvSec 2007, LNCS 4784,pp. 122–137, 2007.