Efficient Proofs that a Committed Number Lies in an Interval

Fabrice Boudot

France Télécom - CNET
42 rue des Coutures, B.P. 6243
14066 Caen CEDEX 4, France
fabrice.boudot@cnet.francetelecom.fr

Abstract. Alice wants to prove that she is young enough to borrow money from her bank, without revealing her age. She therefore needs a tool for proving that a committed number lies in a specific interval. Up to now, such tools were either inefficient (too many bits to compute and to transmit) or inexact (i.e. proved membership to a much larger interval). This paper presents a new proof, which is both *efficient* and *exact*. Here, "efficient" means that there are less than 20 exponentiations to perform and less than 2 Kbytes to transmit. The potential areas of application of this proof are numerous (electronic cash, group signatures, publicly verifiable secret encryption, etc ...).

1 Introduction

The idea of checking whether a committed integer lies in a specific interval was first developed in [2]. Such kind of proofs are intensively used in several schemes: electronic cash systems [7], group signatures [11], publicly verifiable secret sharing schemes [17,4], and other zero-knowledge protocols (e.g. [13,10]). Nowadays, there exist two methods to prove that a committed integer is in a specific interval:

- the first one (see e.g. [17]) allows to prove that the bit-length of the committed number is less or equal to a fixed value k, and hence belongs to $[0, 2^k - 1]$. Unfortunately, this method is very inefficient.
- the second one (see e.g. [2,8]) is much more efficient, but the price to pay is that only membership to a much larger interval can be proven.

In this paper, we give a new method to prove that a committed number belongs to an interval that is much more efficient than the first method and that effectively proves, unlike the second method, that a committed number $x \in I$ belongs to I (and not a larger interval).

Throughout this paper, $\mathbb{Z}_n$ denotes the residue class ring modulo n, and $\mathbb{Z}_n^*$ denotes the multiplicative group of invertible elements in $\mathbb{Z}_n$. $|\cdot|$ denotes binary

B. Preneel (Ed.): EUROCRYPT 2000, LNCS 1807, pp. 431–444, 2000.

length, $a \parallel b$ is the concatenation of the strings a and b. We denote by $\sharp I$ the cardinal of the set I. For $g \in \mathbb{Z}_n^*$ and a in the group generated by g, we denote by $\log_g(a)$ the discrete logarithm of a in base g modulo n, i.e. the number x such that $a = g^x \bmod n$ which belongs to $\{-\mathrm{ord}(g)/2, \ldots, \mathrm{ord}(g)/2 - 1\}$, where $\mathrm{ord}(g)$ is the order of g in $\mathbb{Z}_n^*$. We denote by $PK(x : \mathcal{R}(x))$ a zero-knowledge proof of knowledge of x such that $\mathcal{R}(x)$ is true.

1.1 Definitions

Definition 1 *Let $E = BC(x)$ be a commitment to a value $x \in [b_1, b_2]$. A* proof of membership to an interval $[b_1, b_2]$ *is a proof of knowledge that ensures the verifier that the prover knows x such that $E = BC(x)$ and that x belongs to $[B_1, B_2]$, an interval which contains $[b_1, b_2]$.*

Definition 2 *Following the notations of definition 1, the* expansion rate *of a proof of membership to an interval is the quantity $\delta = (B_2 - B_1)/(b_2 - b_1)$. This quantity may or not be dependent on $(b_2 - b_1)$.*

We evaluate the quality of a proof of membership to an interval by the length of the proof (which must be as short as possible) and by its expansion rate (which must be as low as possible).

1.2 Known Results

In this subsection, we present three existing proofs of membership to an interval. They are based on zero-knowledge proofs of knowledge of a discrete logarithm either modulo a prime (Schnorr [19]) or a composite number (Girault [16]).

1.2.1 Classical Proof [17]

This protocol proves that a committed number $x \in I = [0, b]$ belongs to $I = [0, 2^k - 1]$, where the binary length of b is k.

Let p be a large prime number, let q such that $q|p - 1$, and g and h be elements of order q in $\mathbb{Z}_p^*$ such that the discrete logarithm of h in base g is unknown by Alice. We denote by $E(x, r) = g^x h^r \bmod p$ a commitment to x, where r is randomly selected over $\mathbb{Z}_p^*$. Let $x = x_0 2^0 + x_1 2^1 + \cdots + x_{k-1} 2^{k-1}$ for $x_i \in \{0, 1\}$ and $i = 0, 1, \ldots, k - 1$ be the binary representation of x. Alice sets $E(x_i, r_i)$ for $i = 0, 1, \ldots, k-1$, where the r_i are such that $\sum_{i=0,\ldots,k-1} r_i = r$, and proves for all i that the number hidden by $E(x_i, r_i)$ is either 0 or 1 by proving that she knows either a discrete logarithm of $E(x_i, r_i)$ in base h or a discrete logarithm of $E(x_i, r_i)/g$ in base h. This can be done using proofs of knowledge of a discrete logarithm [19] and a proof of knowledge of one out of two secrets [5]. Bob also checks that $\prod_{i=0,\ldots,k-1} E(x_i, r_i) = E(x, r)$.

Characteristics of this proof: For $|p| = 1024$ bits, $|q| = 1023$ bits, $|b| = 512$ bits, and the Schnorr's proof security parameter $t = 90$.

- *completeness*: The proof always succeeds.
- *soundness*: A cheating prover can succeed with probability less than $1-(1-2^{-89})^{512} < 2^{-80}$.
- *zero-knowledge*: Perfectly zero-knowledge in the random-oracle model defined in [3].
- *what is proven*: $x \in [0, 2^k - 1]$.
- *expansion rate*: $1 \leq \delta < 2$ (can be decreased to 1 by proving that both x and $b - x$ are k-bit numbers).
- *length of the proof*: 1,612,800 bits = 196.9 kB.

1.2.2 BCDG Proof [2]

This protocol proves that a committed number $x \in I$ belongs to J, where the expansion rate $\sharp J/\sharp I$ is equal to 3. We give here a slightly different presentation from the one of the original paper.

Let t be a security parameter. Let p be a large prime number, let q such that $q|p-1$, and g and h be elements of order q in $\mathbb{Z}_p^*$ such that the discrete logarithm of h in base g is unknown by Alice. We denote by $E = E(x, r) = g^x h^r \bmod p$ a commitment to $x \in [0, b]$, where r is randomly selected over $\mathbb{Z}_p^*$.

For simplicity, we present an interactive version of the protocol which can be easily turned into a non-interactive one using the Fiat-Shamir heuristic [15].

Protocol: $PK_{[BCDG]}(x, r : E = E(x, r) \wedge x \in [-b, 2b])$.
Run t times in parallel:

1. Alice picks random $\omega_1 \in_R [0, b]$ and sets $\omega_2 = \omega_1 - b$. She also randomly selects $\eta_1 \in_R [0, q-1]$ and $\eta_2 \in_R [0, q-1]$, and sends to Bob the unordered pair of commitments $W_1 = g^{\omega_1} h^{\eta_1} \bmod p$ and $W_2 = g^{\omega_2} h^{\eta_2} \bmod p$.
2. Bob challenges Alice by $c \in_R \{0, 1\}$.
3. If $c = 0$, Alice sends to Bob the values of ω_1, ω_2, η_1 and η_2.
   If $c = 1$, Alice sends to Bob the value of $x+\omega_j$, $r+\eta_j$ for the value $j \in \{1, 2\}$ such that $x + \omega_j \in [0, b]$.
4. Bob checks that $W_1 = g^{\omega_1} h^{\eta_1} \bmod p$ and $W_2 = g^{\omega_2} h^{\eta_2} \bmod p$ in the former case and $W_j = g^{\omega_j} h^{\eta_j} \bmod p$, $x + \omega_j \in [0, b]$ in the latter case.

Characteristics of this proof: For $|p| = 1024$ bits, $|q| = 1023$ bits, $|b| = 512$ bits, $t = 80$ and $l = 40$.

- *completeness*: The proof always succeeds if $x \in [0, b]$
- *soundness*: A cheating prover can succeed with probability less than $2 \times 2^{-t} = 2^{-79}$.
- *zero-knowledge*: Perfectly zero-knowledge in the random-oracle model.
- *what is proven*: $x \in [-b, 2b]$.
- *expansion rate*: $\delta = 3$.
- *length of the proof (on average)*: 225,320 bits = 27.5 kB.

1.2.3 CFT Proof [8]

The main idea of this proof is roughly the same as the one of [2]. Let t, l and s be three security parameters. This protocol (due to Chan, Frankel and Tsiounis [7], and corrected in [8], and also due to [14] in another form) proves that a committed number $x \in I$ belongs to J, where the expansion rate $\sharp J/\sharp I$ is equal to 2^{t+l+1}. Let n be a large composite number whose factorization is unknown by Alice and Bob, g be an element of large order in $\mathbb{Z}_n^*$ and h be an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice. Let H be a hash-function which outputs $2t$-bit strings. We denote by $E = E(x, r) = g^x h^r \bmod n$ a commitment to $x \in [0, b]$, where r is randomly selected over $[-2^s n+1, 2^s n-1]$. This commitment, from [13], statistically reveals no information about x to Bob.

Protocol: $PK_{[CFT]}(x, r : E = E(x, r) \wedge x \in [-2^{t+l}b, 2^{t+l}b])$.

1. Alice picks random $\omega \in_R [0, 2^{t+l}b - 1]$ and $\eta \in_R [-2^{t+l+s}n + 1, 2^{t+l+s}n - 1]$, and then computes $W = g^\omega h^\eta \bmod n$.
2. Then, she computes $C = H(W)$ and $c = C \bmod 2^t$.
3. Finally, she computes $D_1 = \omega + xc$ and $D_2 = \eta + rc$ (in $\mathbb{Z}$). If $D_1 \in [cb, 2^{t+l}b - 1]$, she sends (C, D_1, D_2) to Bob, otherwise she starts again the protocol.
4. Bob checks that $D_1 \in [cb, 2^{t+l}b - 1]$ and that $C = H(g^{D_1} h^{D_2} E^{-c})$. This convinces Bob that $x \in [-2^{t+l}b, 2^{t+l}b]$.

Characteristics of this proof: For $|n| = 1024$ bits, $|b| = 512$ bits, $t = 80$, $l = 40$ and $s = 40$.

- *completeness*: The proof succeeds with probability greater than $1 - 2^l = 1 - 2^{-40}$ if $x \in [0, b]$.
- *soundness*: A cheating prover can succeed with probability less than 2^{-79}.
- *zero-knowledge*: Statistically zero-knowledge in the random-oracle model.
- *what is proven*: $x \in [-2^{t+l}b, 2^{t+l}b] = [-2^{120}b, 2^{120}b]$.
- *expansion rate*: $\delta = 2^{t+l+1} = 2^{121}$.
- *length of the proof*: 1,976 bits = 0.241 kB.

1.3 Our Results

The schemes we propose in this paper are much more efficient than the classical proof and the BCDG proof, and their expansion rates are $\delta = 1 + \varepsilon$ for the first one, and $\delta = 1$ for the other one, where ε is a negligible quantity with respect to 1 if the considered interval is large enough ($\varepsilon = 2^{-134}$ if the committed number lies in $[0, 2^{512} - 1]$).

We briefly describe our algorithms: first note that it is sufficient to know how to prove that a number is positive to prove that a number belongs to an interval. Indeed, to prove that x belongs to $[a, b]$, it is sufficient to prove that $x - a \geq 0$ and $b - x \geq 0$.

Consider the following commitment scheme: to hide an integer x, Alice computes $E(x,r) = g^x h^r \bmod n$, where n is a composite number whose factorization is unknown by both Alice and Bob, g is an element of large order in $\mathbb{Z}_n^*$, h is an element of large order of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice, r is randomly selected over $[-2^s n + 1, 2^s n - 1]$ and s is a security parameter. This commitment has been introduced in [13], and statistically reveals no information of x to Bob (see section 2.1). Note that this commitment is homomorphic, i.e. $E(x+y, r+s) = E(x,r) \times E(y,s) \bmod n$.

Assume that Alice commits herself to a positive integer x by $E = E(x,r)$ and wants to prove that $x \in [a,b]$.

In our first scheme, Alice writes the positive integer $x - a$ as the sum of x_1^2, the greatest square less than x and of ρ, a positive number less than $2\sqrt{x-a}$ (and therefore less than $2\sqrt{b-a}$). Then, she randomly selects r_1, r_2 in $[0, 2^s n - 1]$ such that $r_1 + r_2 = r$ and computes $E_1 = E(x_1^2, r_1)$ and $E_2 = E(\rho, r_2)$. Then, she proves to Bob that E_1 hides a square in $\mathbb{Z}$ and that E_2 hides a number whose absolute value is less than $2^{t+l+1}\sqrt{b-a}$ by a CFT proof. Finally, she applies the same method to $b - x$. This leads to a proof that $x \in [a - 2^{t+l+1}\sqrt{b-a}, b + 2^{t+l+1}\sqrt{b-a}]$. The expansion rate of this proof is equal to $1 + (2^{t+l+2}/\sqrt{b-a})$, which becomes close to 1 when $b - a$ is large.

In our second scheme, we artificially enlarge the size of x by setting $x' = 2^T x$. By using the first scheme, we prove that $x' \in [2^T a - 2^{t+l+T/2+1}\sqrt{b-a}, 2^T b + 2^{t+l+T/2+1}\sqrt{b-a}]$, and if T is large enough (i.e. T is such that $2^{t+l+T/2+1}\sqrt{b-a} < 2^T$), Bob is convinced that $x' \in [2^T a - 2^T + 1, 2^T b + 2^T - 1]$, so that $x \in [a - \varepsilon, b + \varepsilon]$ where $0 \leq \varepsilon < 1$. So, as x is an integer, Bob is convinced that $x \in [a,b]$.

1.4 Organization of the Paper

In Section 2, we describe some building blocks used in our protocols: a proof that two commitments hide the same secret, and a proof that a committed number is a square. In Section 3, we describe our two schemes: a proof of membership to an interval with tolerance and a proof of membership without tolerance. Then, we extend our results to various commitments. In Section 4, we give an application of our schemes. Finally, we conclude in Section 5.

2 Building Blocks

The schemes we present in this section are based on the following assumption, introduced e.g. in [13]:

Strong RSA Assumption: There exist an efficient algorithm that on input $|n|$ outputs an RSA-modulus n and an element $z \in \mathbb{Z}_n^*$ such that it is infeasible to find integers $e \notin \{-1, 1\}$ and u such that $z = u^e \bmod n$.

2.1 The Fujisaki-Okamoto Commitment Scheme

In this subsection, we briefly describe the commitment scheme we use throughout this paper.

Let s be a security parameter. Let n be a large composite number whose factorization is unknown by Alice and Bob, g be an element of large order in $\mathbb{Z}_n^*$ and h be an element of large order of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice.

We denote by $E = E(x, r) = g^x h^r \bmod n$ a commitment to x in base (g, h), where r is randomly selected over $\{-2^s n + 1, ..., 2^s n - 1\}$.

This commitment has first appeared in [13].

Proposition 1 *$E(x, r)$ is a statistically secure commitment scheme, i.e.:*

- *Alice is unable to commit herself to two values x_1 and x_2 such that $x_1 \neq x_2$ (in $\mathbb{Z}$) by the same commitment unless she can factor n or solve the discrete logarithm of g in base h or the discrete logarithm of h in base g. In other words, under the factoring assumption, it is computationally infeasible to compute x_1, x_2, r_1, r_2 where $x_1 \neq x_2$ such that $E(x_1, r_1) = E(x_2, r_2)$.*
- *$E(x, r)$ statistically reveals no information to Bob. More formally, there exists a simulator which outputs simulated commitments to x which are statistically indistinguishable from true ones.*

As Alice only knows one couple of numbers (x, r) such that $E = g^x h^r \bmod n$, we say that x is the value committed by (or hidden by) E, and that E hides the secret x.

2.2 Proof that Two Commitments Hide the Same Secret

Let t, l, s_1 and s_2 be four security parameters. Let n be a large composite number whose factorization is unknown by Alice and Bob, g_1 be an element of large order in $\mathbb{Z}_n^*$ and g_2, h_1, h_2 be elements of the group generated by g_1 such that the discrete logarithm of g_1 in base h_1, the discrete logarithm of h_1 in base g_1, the discrete logarithm of g_2 in base h_2 and the discrete logarithm of h_2 in base g_2 are unknown by Alice. Let H be a hash-function which outputs $2t$-bit strings. We denote by $E_1(x, r_1) = g_1^x h_1^{r_1} \bmod n$ a commitment to x in base (g_1, h_1) where r_1 is randomly selected over $[2^{s_1} n + 1, 2^{s_1} n - 1]$, and $E_2(x, r_2) = g_2^x h_2^{r_2} \bmod n$ a commitment to x in base (g_2, h_2) where r_2 is randomly selected over $[-2^{s_2} n + 1, 2^{s_2} n - 1]$.

Alice secretly holds $x \in [0, b]$. Let $E = E_1(x, r_1)$ and $F = E_2(x, r_2)$ be two commitments to x. She wants to prove to Bob that she knows x, r_1, r_2 such that $E = E_1(x, r_1)$ and $F = E_2(x, r_2)$, i.e. that E and F hide the same secret x.

This protocol is derived from proofs of equality of two discrete logarithms from [6,12,1], combined with a proof of knowledge of a discrete logarithm modulo n [16].

Protocol: $PK(x, r_1, r_2 : E = E_1(x, r_1) \wedge F = E_2(x, r_2))$.

1. Alice picks random $\omega \in [1, 2^{l+t}b-1]$, $\eta_1 \in [1, 2^{l+t+s_1}n-1]$, $\eta_2 \in [1, 2^{l+t+s_2}n-1]$. Then, she computes $W_1 = g_1^{\omega} h_1^{\eta_1} \bmod n$ and $W_2 = g_2^{\omega} h_2^{\eta_2} \bmod n$.
2. Alice computes $c = H(W_1 \parallel W_2)$.
3. She computes $D = \omega + cx$, $D_1 = \eta_1 + cr_1$, $D_2 = \eta_2 + cr_2$ (in $\mathbb{Z}$) and sends (c, D, D_1, D_2) to Bob.
4. Bob checks whether $c = H(g_1^D h_1^{D_1} E^{-c} \bmod n \parallel g_2^D h_2^{D_2} F^{-c} \bmod n)$.

It is shown in [9] that a successful execution of this protocol convinces Bob that the numbers hidden in E and F are equal provided the Strong RSA problem is infeasible.

Characteristics of this proof: For $|n| = 1024$ bits, $|b| = 512$ bits, $t = 80$, $l = 40$, $s_1 = 40$ and $s_2 = 552$.

- *completeness*: The proof always succeeds.
- *soundness*: Under the strong RSA assumption, a cheating prover can succeed with probability less than $2 \times 2^{-t} = 2^{-79}$.
- *zero-knowledge*: Statistically zero-knowledge in the random-oracle model if $1/l$ is negligible.
- *length of the proof*: $2,648 + 2|x|$ bits $= 3672$ bits $= 0.448$ kB.

2.3 Proof that a Committed Number is a Square

Let t, l, and s be three security parameters. Let n be a large composite number whose factorization is unknown by Alice and Bob, g be an element of large order in $\mathbb{Z}_n^*$ and h be an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice. Let H be a hash-function which outputs $2t$-bit strings. We denote by $E(x, r) = g^x h^r \bmod n$ a commitment to x in base (g, h) where r is randomly selected over $[-2^s n + 1, 2^s n - 1]$.

Alice secretly holds $x \in [0, b]$. Let $E = E(x^2, r_1)$ be a commitment to the square of x (in $\mathbb{Z}$). She wants to prove to Bob that she knows x and r_1 such that $E = E(x^2, r_1)$, i.e. that E hides the square x^2.

The first proof that a committed number is a square has appeared in [13].

Protocol: $PK(x, r_1 : E = E(x^2, r_1))$.

1. Alice picks random $r_2 \in [-2^s n + 1, 2^s n - 1]$ and computes $F = E(x, r_2)$.
2. Then, Alice computes $r_3 = r_1 - r_2 x$ (in $\mathbb{Z}$). Note that $r_3 \in [-2^s bn + 1, 2^s bn - 1]$. Then, $E = F^x h^{r_3} \bmod n$.
3. As E is a commitment to x in base (F, h) and F is a commitment to x in base (g, h), Alice can run $PK(x, r_2, r_3 : F = g^x h^{r_2} \bmod n \wedge E = F^x h^{r_3} \bmod n)$, the proof that two commitments hide the same secret described in section 2.2. She gets (c, D, D_1, D_2).
4. She sends (F, c, D, D_1, D_2) to Bob.

5. Bob checks that $PK(x, r_2, r_3 : F = g^x h^{r_2} \bmod n \wedge E = F^x h^{r_3} \bmod n)$ is valid.

The soundness of this protocol is clear: if Alice is able to compute F and a proof that E and F are commitments to the same number $\tilde{x}$ resp. in base (F, h) and (g, h), then Alice knows $\tilde{x}$, $\tilde{r}_2$ and $\tilde{r}_3$ such that $E = F^{\tilde{x}} h^{\tilde{r}_3} = g^{\tilde{x}^2} h^{\tilde{x}\tilde{r}_2 + \tilde{r}_3} = g^{\tilde{x}^2} h^{\tilde{r}_1} \bmod n$. Then, this proof shows that Alice knows $\tilde{x}^2$, a square which is hidden in the commitment E. In other words, a successful execution of this protocol convinces Bob that the value hidden in the commitment E is a square in $\mathbb{Z}$.

Technical proofs of the soundness and the zero-knowledgeness of this protocol are easily obtained from the properties of the previous protocol.

Characteristics of this proof: For $|n| = 1024$ bits, $|b| = 512$ bits, $t = 80$, $l = 40$ and $s = 40$.

- *completeness*: The proof always succeeds.
- *soundness*: Under the strong RSA assumption, a cheating prover can succeed with probability less than $2 \times 2^{-t} = 2^{-79}$.
- *zero-knowledge*: Statistically zero-knowledge in the random-oracle model if $1/l$ is negligible.
- *length of the proof*: $3,672 + 2|x|$ bits $= 4696$ bits $= 0.573$ kB.

3 Our Schemes

3.1 Proof that a committed number belongs to an interval

Let t, l and s be three security parameters. Let n be a large composite number whose factorization is unknown by Alice and Bob, g be an element of large order in $\mathbb{Z}_n^*$ and h be an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice. We denote by $E(x, r) = g^x h^r \bmod n$ a commitment to x in base (g, h) where r is randomly selected over $[-2^s n + 1, 2^s n - 1]$.

3.1.1 Proof with Tolerance: $\delta = 1 + \varepsilon$.

The above protocol allows Alice to prove to Bob that the committed number $x \in [a, b]$ belongs to $[a - \theta, b + \theta]$, where $\theta = 2^{t+l+1}\sqrt{b-a}$.

Protocol: $PK_{[WithTol.]}(x, r : E = E(x, r) \wedge x \in [a - \theta, b + \theta])$.

1. [Knowledge of x]
   Alice executes with Bob:
   $PK(x, r : E = E(x, r))$
2. [Setting]
   Both Alice and Bob compute $\tilde{E} = E/g^a \bmod n$ and $\bar{E} = g^b/E \bmod n$. Alice sets $\tilde{x} = x - a$ and $\bar{x} = b - x$. Now, Alice must prove to Bob that both $\tilde{E}$ and $\bar{E}$ hide secrets which are greater than $-\theta$.

3. [Decomposition of $\tilde{x}$ and $\bar{x}$]
   Alice computes:
   $\tilde{x}_1 = \lfloor\sqrt{x-a}\rfloor$, $\tilde{x}_2 = \tilde{x} - \tilde{x}_1^2$,
   $\bar{x}_1 = \lfloor\sqrt{b-x}\rfloor$, $\bar{x}_2 = \bar{x} - \bar{x}_1^2$.
   Then, $\tilde{x} = \tilde{x}_1^2 + \tilde{x}_2$ and $\bar{x} = \bar{x}_1^2 + \bar{x}_2$, where $0 \leq \tilde{x}_2 \leq 2\sqrt{b-a}$ and $0 \leq \bar{x}_2 \leq 2\sqrt{b-a}$.
4. [Choice of random values for new commitments]
   Alice randomly selects $\tilde{r}_1$ and $\tilde{r}_2$ in $[-2^s n+1, ..., 2^s n-1]$ such that $\tilde{r}_1+\tilde{r}_2 = r$, and $\bar{r}_1$ and $\bar{r}_2$ such that $\bar{r}_1 + \bar{r}_2 = -r$.
5. [Computation of new commitments]
   Alice computes:
   $\tilde{E}_1 = E(\tilde{x}_1^2, \tilde{r}_1)$, $\tilde{E}_2 = E(\tilde{x}_2, \tilde{r}_2)$,
   $\bar{E}_1 = E(\bar{x}_1^2, \bar{r}_1)$, $\bar{E}_2 = E(\bar{x}_2, \bar{r}_2)$.
6. [Sending of the new commitments]
   Alice sends $\tilde{E}_1$ and $\bar{E}_1$ to Bob. Bob computes $\tilde{E}_2 = \tilde{E}/\tilde{E}_1$ and $\bar{E}_2 = \bar{E}/\bar{E}_1$
7. [Validity of the commitments to a square]
   Alice executes with Bob
   $PK(\tilde{x}_1, \tilde{r}_1 : \tilde{E}_1 = E(\tilde{x}_1^2, \tilde{r}_1))$,
   $PK(\bar{x}_1, \bar{r}_1 : \bar{E}_1 = E(\bar{x}_1^2, \bar{r}_1))$.
   which prove that both $\tilde{E}_1$ and $\bar{E}_1$ hide a square.
8. [Validity of the commitments to a small value]
   Let $\theta = 2^{t+l+1}\sqrt{b-a}$. Alice executes with Bob the two following CFT proofs:
   $PK_{[CFT]}(\tilde{x}_2, \tilde{r}_2 : \tilde{E}_2 = E(\tilde{x}_2, \tilde{r}_2) \wedge \tilde{x}_2 \in [-\theta, \theta])$,
   $PK_{[CFT]}(\bar{x}_2, \bar{r}_2 : \bar{E}_2 = E(\bar{x}_2, \bar{r}_2) \wedge \bar{x}_2 \in [-\theta, \theta])$.
   which prove that both $\tilde{E}_2$ and $\bar{E}_2$ hide numbers which belong to $[-\theta, \theta]$, where $\theta = 2^{t+l+1}\sqrt{b-a}$, instead of proving that they belong to $[0, 2\sqrt{b-a}]$.

Sketch of Analysis:

After a successful execution of this protocol, Bob is convinced that :

- $\tilde{E}_1$ and $\bar{E}_1$ hide numbers which are positive integers, as they are squares (Step 7).
- $\tilde{E}_2$ and $\bar{E}_2$ hide numbers which are greater than $-\theta$ (Step 8).
- Alice knows the values hidden by $\tilde{E}$ and $\bar{E}$ (Step 1 and 2).
- The number hidden in $\tilde{E}$ is the sum of the number hidden in $\tilde{E}_1$ and of the number hidden in $\tilde{E}_2$, and so are $\bar{E}$, $\bar{E}_1$ and $\bar{E}_2$ (Step 6).

So, Bob is convinced that $\tilde{E}$ and $\bar{E}$ hide numbers which are greater than $-\theta$, as they are the sum of a positive number and a number greater than $-\theta$.

Let x be the number known by Alice (from step 1) and hidden by E. Bob is convinced that $x - a$ is the value hidden by $\tilde{E}$ and $b - x$ is the value hidden by $\bar{E}$. So, Bob is convinced that $x - a \geq -\theta$ and $b - x \geq -\theta$, i.e. that x belongs to $[a - \theta, b + \theta]$, where $\theta = 2^{t+l+1}\sqrt{b-a}$.

Expansion Rate: Following Definition 2, the expansion rate is equal to :

$$\delta = \frac{(b+\theta) - (a-\theta)}{b-a} = 1 + \frac{2\theta}{b-a} = 1 + \varepsilon$$

where:

$$\varepsilon = \frac{2\theta}{b-a} = \frac{2^{t+l+2}}{\sqrt{b-a}} \leq 2^{t+l+2-\lfloor \frac{|b-a|}{2} \rfloor}$$

ε is negligible if and only if $|b-a| \geq 2t+2l+2z+4$, where z is a security parameter. If it is the case, the expansion rate is equal to $\delta = 1+2^{-z}$.

Characteristics of this proof: for $|n| = 1024$ bits, $|b-a| = 512$ bits $t = 80$, $l = 40$ and $s = 40$.

- *length of the proof*: 13860 bits = 1.692 kB.
- *expansion rate*: $\delta = 1+\varepsilon$, where $\varepsilon \leq 2^{t+l+2-\lfloor \frac{|b-a|}{2} \rfloor} = 2^{-134}$.

3.1.2 Proof without Tolerance: $\delta = 1$.

The above protocol allows Alice to prove to Bob that the committed number $x \in [a,b]$ belongs to the desired interval $[a,b]$.

To achieve a proof of membership without tolerance, we artificially enlarge the size of x by setting $x' = 2^T x$, where $T = 2(t+l+1)+|b-a|$. Let $E' = E^{2^T}$. E' is a Fujisaki-Okamoto commitment to $x' = 2^T x$ that Alice can open.

By using the first scheme, Alice proves to Bob that she knows the value x' hidden by E' is such that $x' \in [2^T a - 2^{t+l+T/2+1}\sqrt{b-a}, 2^T b + 2^{t+l+T/2+1}\sqrt{b-a}]$ by a CFT proof (instead of proving that $x' \in [2^T a, 2^T b]$).

As $T = 2(t+l+1)+|b-a|$, we have:

$$\begin{aligned}\theta' = 2^{t+l+T/2+1}\sqrt{b-a} &< 2^{t+l+T/2+1} \times 2^{\lceil (|b-a|-1)/2 \rceil} \\ &< 2^{T/2} \times 2^{t+l+1} \times 2^{\lceil (|b-a|-1)/2 \rceil} \\ &< 2^{T/2} \times 2^{T/2} \\ &< 2^T\end{aligned}$$

Then, if Bob is convinced that $x' \in [2^T a - \theta', 2^T b + \theta']$, he is also convinced that $x' \in]2^T a - 2^T, 2^T b + 2^T[$.

Provided Alice does not know the factorization of n, she is unable to know two different values in $\mathbb{Z}$ hidden by E'. So, necessarily, $x' = 2^T x$. The proof convinces Bob that $2^T x \in]2^T a - 2^T, 2^T b + 2^T[$, and so that $x \in]a-1, b+1[$. Finally, as x is an integer, Bob is convinced that $x \in [a,b]$.

Protocol: $PK(x, r : E = E(x,r) \wedge x \in [a,b])$.

1. [Setting]
   Both Alice and Bob compute $E' = E^{2^T}$, where $T = 2(t+l+1)+|b-a|$.
2. [Proof]
   Alice executes with Bob:
   $PK_{[WithTol.]}(x', r' : E' = E(x', r') \wedge x' \in [2^T a - 2^{t+l+T/2+1}\sqrt{b-a}, 2^T b + 2^{t+l+T/2+1}\sqrt{b-a}]$.

Characteristics of this proof: for $|n| = 1024$ bits, $|b-a| = 512$ bits, $t = 80$, $l = 40$ and $s = 40$.

- *length of the proof*: 16176 bits = 1.975 kB.
- *expansion rate*: $\delta = 1$.

3.2 Extensions

The above protocols can be used to prove that:

- a discrete logarithm modulo a composite number n whose factorization is unknown to Alice belongs to an interval. Let g be an element of large order in $\mathbb{Z}_n^*$ and h be an element of the group generated by g such that both the discrete logarithm of g in base h and the discrete logarithm of h in base g are unknown by Alice. Let x be such that $y = g^x \bmod n$. Alice randomly selects r and computes $y' = h^r \bmod n$. She proves to Bob that she knows a discrete logarithm of y' in base h, and then that $yy' = g^x h^r \bmod n$ is a commitment to a value which belongs to the given interval.
- a discrete logarithm modulo p (a prime number or a composite number whose factorization is known to Alice) belongs to an interval. Let x be such that $Y = G^x \bmod p$. Alice randomly selects r and computes $E = E(x, r) = g^x h^r \bmod n$, a commitment to x. Then, she executes with Bob $PK(x, r : Y = G^x \bmod p \wedge E = g^x h^r \bmod n)$ (see Appendix A) and $PK(x, r : E = g^x h^r \bmod n \wedge x \in [a, b])$.
- a third root (or, more generally, a e-th root) modulo N belongs to an interval. Let x be such that $Y = x^3 \bmod N$. Alice randomly selects r and computes $E = E(x, r) = g^x h^r \bmod n$, a commitment to x. Then, she executes with Bob $PK(x, r : Y = x^3 \bmod N \wedge E = g^x h^r \bmod n)$ (see Appendix B) and $PK(x, r : E = g^x h^r \bmod n \wedge x \in [a, b])$.

Note: to prove that a committed number x lies in $I \cup J$, Alice proves that x lies in I or x lies in J by using a proof of "or" by [5].

4 Application to Verifiable Encryption

As one of the several applications of proofs of membership to an interval, we present in this section an efficient (publicly) verifiable encryption scheme.

Alice has sent two encrypted messages to Charlie and Deborah, and wants to prove to Bob that the two ciphertexts encrypt the same message.

Charlie and Deborah use the Okamoto-Uchiyama [18] cryptosystem, i.e. Charlie holds a composite number $n_C = p_C^2 q_C$ ($|p_C| = |q_C| = k$), an element $g_C \in \mathbb{Z}_{n_C}^*$ such that the order of $g_C^{p_C - 1} \bmod p_C^2$ is p_C, and Deborah holds a composite number $n_D = p_D^2 q_D$ ($|p_D| = |q_D| = k$), an element $g_D \in \mathbb{Z}_{n_D}^*$ such that the order of $g_D^{p_D - 1} \bmod p_D^2$ is p_D.

We denote by $h_C = g_C^{n_C} \bmod n_C$ and $h_D = g_D^{n_D} \bmod n_D$.

To encrypt a message m such that $0 \leq m \leq 2^{k-1}$ intended to Charlie, Alice computes $E_C = g_C^m h_C^{r_C} \bmod n_C$, where r_C is randomly selected over $\mathbb{Z}_{n_C}^*$. In the same way, she encrypts the same message m intended to Deborah by computing $E_D = g_D^m h_D^{r_D} \bmod n_D$.

Now, Alice wants to prove to Bob that the two ciphertexts E_C and E_D encrypt the same message.

First, she executes with Bob $PK(m, r_C, r_D : E_C = g_C^m h_C^{r_C} \bmod n_C \wedge E_D = g_D^m h_D^{r_D} \bmod n_D)$, a proof of equality of two committed numbers with respect to different moduli (see Appendix A). This only proves that she knows an integer m such that $m \bmod p_C$ and $m \bmod p_D$ are respectively the messages decrypted by Charlie and Deborah. Note that if m is greater than p_C and p_D, then $m \bmod p_C \neq m \bmod p_D$. So it is necessary that Alice also proves to Bob that m is less than p_C and p_D. Alice uses the proof of membership to an interval without tolerance presented in section 3.1.2: $PK(m, r_C : E_C = g_C^m h_C^{r_C} \bmod n_C \wedge m \in [0; 2^{k-1}])$. Then, necessarily, $m \bmod p_C = m \bmod p_D$: Bob is convinced that Alice has secretly sent the same messages to Charlie and to Deborah.

5 Conclusion

We have presented in this paper efficient proofs that a committed number belongs to an interval and give examples of applications, more particularly an efficient verifiable encryption scheme. By their efficiency, they are well suited to be used in various cryptographic protocols.

Acknowledgements

We would like to thank Marc Girault for helpful discussions and comments.

References

1. Bao, F.: An Efficient Verifiable Encryption Scheme for Encryption of Discrete Logarithms. Proceedings of CARDIS'98 (1998)
2. Brickell, E., Chaum, D., Damgård, I., Van de Graaf, J.: Gradual and Verifiable Release of a Secret. Proceedings of CRYPTO'87, LNCS **293** (1988) 156–166
3. Bellare, M., Rogaway, P.: Random Oracles are Practical: a Paradigm for Designing Efficient Protocols. Proceedings of the First Annual Conference and Communications Security (1993) 62–73
4. Boudot, F., Traoré, J.: Efficient Publicly Verifiable Secret Sharing Schemes with Fast or Delayed Recovery. Proceedings of the Second International Conference on Information and Communication Security, LNCS **1726** (1999) 87–102
5. Cramer, R., Damgård, I., Schoenmakers, B.: Proofs of Partial Knowledge and Simplified Design of Witness Hiding Protocols. Proceedings of CRYPTO'94, LNCS **839** (1997) 174–187
6. Chaum, D., Evertse, J.-H., Van de Graaf, J.: An Improved Protocol for Demonstrating Possession of Discrete Logarithm and Some Generalizations. Proceedings of EUROCRYPT'87, LNCS **304** (1998) 127–141
7. Chan, A., Frankel, Y., Tsiounis, Y,: Easy Come - Easy Go Divisible Cash. Proceedings of EUROCRYPT'98, LNCS **1403** (1998) 561–575
8. Chan, A., Frankel, Y., Tsiounis, Y,: Easy Come - Easy Go Divisible Cash. Updated version with corrections, GTE Tech. Rep. (1998), available at `http://www.ccs.neu.edu/home/yiannis/`

9. Camenisch, J., Michels, M.: A Group Signature Scheme Based on an RSA-Variant. Tech. Rep. **RS-98-27**, BRICS, Dept. of Comp. Sci., University of Aarhus, available at `http://www.zurich.ibm.com/~jca/` (1998)
10. Camenisch, J., Michels, M.: Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes. Proceedings of EUROCRYPT'99, LNCS **1592** (1999) 106–121
11. Camenisch, J., Michels, M.: Separability and Efficiency for Generic Group Signature Schemes. Proceedings of CRYPTO'99, LNCS **1666** (1999) 413–430
12. Chaum, D., Pedersen, T.-P.: Wallet Databases with Observers. Proceedings of CRYPTO'92, LNCS **740** (1992) 89–105
13. Fujisaki, E., Okamoto, T.: Statistical Zero Knowledge Protocols to Prove Modular Polynomial Relations. Proceedings of CRYPTO'97, LNCS **1294** (1997) 16–30
14. Fujisaki, E., Okamoto, T.: A Practical and Provably Secure Scheme for Publicly Verifiable Secret Sharing and Its Applications, Proceedings of EUROCRYPT'98, LNCS **1403** (1998) 32–46
15. Fiat, A., Shamir, A.: How to Prove Yourself: Practical Solutions to Identification and Signature Problems. Proceedings of CRYPTO'86, LNCS **263** (1986) 186–194
16. Girault, M.: Self-Certified Public Keys. Proceedings of EUROCRYPT'91, LNCS **547** (1991) 490–497
17. Mao, W.: Guaranteed Correct Sharing of Integer Factorization with Off-line Shareholders. Proceedings of Public Key Cryptography 98, (1998) 27–42
18. Okamoto, T., Uchiyama, S.: A New Public-Key Cryptosystem as Secure as Factoring. Proceedings of EUROCRYPT'98, LNCS **1403** (1998) 308–318
19. Schnorr, C.-P.: Efficient Signature Generation for Smart Cards Journal of Cryptology, (**4:3**) (1991) 239–252

A Proof of Equality of Two Committed Numbers in Different Moduli

This proof originally appeared in[4] and independently in [10] in a more general form.

Let t, l and s be three security parameters. Let n_1 be a large composite number whose factorization is unknown by Alice and Bob, and n_2 be another large number, prime or composite whose factorization is known or unknown by Alice. Let g_1 be an element of large order in $\mathbb{Z}^*_{n_1}$ and h_1 be an element of the group generated by g_1 such that both the discrete logarithm of g_1 in base h_1 and the discrete logarithm of h_1 in base g_1 are unknown by Alice. Let g_2 be an element of large order in $\mathbb{Z}^*_{n_2}$ and h_2 be an element of the group generated by g_2 such that both the discrete logarithm of g_2 in base h_2 and the discrete logarithm of h_2 in base g_2 are unknown by Alice. Let H be a hash-function which outputs $2t$-bit strings. We denote by $E_1(x, r_1) = g_1^x h_1^{r_1} \bmod n_1$ a commitment to x in base (g_1, h_1) where r_1 is randomly selected over $\{-2^s n + 1, ..., 2^s n - 1\}$, and $E_2(x, r_2) = g_2^x h_2^{r_2} \bmod n_2$ a commitment to x in base (g_2, h_2) where r_2 is randomly selected over $\{-2^s n + 1, ..., 2^s n - 1\}$.

Alice secretly holds $x \in \{0, \ldots, b\}$. Let $E = E_1(x, r_1)$ and $F = E_2(x, r_2)$ be two commitments to x. She wants to prove to Bob that she knows x, r_1, r_2 such that $E = E_1(x, r_1)$ and $F = E_2(x, r_2)$, i.e. that E and F hide the same secret x.

Protocol: $PK(x, r_1, r_2 : E = E_1(x, r_1) \bmod n_1 \wedge F = E_2(x, r_2) \bmod n_2)$.

1. Alice picks random $\omega \in \{1, \ldots, 2^{l+t}b - 1\}$, $\eta_1 \in \{1, \ldots, 2^{l+t+s}n - 1\}$, $\eta_2 \in \{1, \ldots, 2^{l+t+s}n - 1\}$. Then, she computes $W_1 = g_1^{\omega} h_1^{\eta_1} \bmod n_1$ and $W_2 = g_2^{\omega} h_2^{\eta_2} \bmod n_2$.
2. Alice computes $c = H(W_1 \parallel W_2)$.
3. She computes $D = \omega + cx$, $D_1 = \eta_1 + cr_1$, $D_2 = \eta_2 + cr_2$ (in $\mathbb{Z}$) and sends (c, D, D_1, D_2) to Bob.
4. Bob checks whether $c = H(g_1^D h_1^{D_1} E^{-c} \bmod n_1 \parallel g_2^D h_2^{D_2} F^{-c} \bmod n_2)$.

Note that this protocol can be used to prove the equality of more than two committed numbers, or to prove the equality of a committed number modulo n_1 and a discrete logarithm modulo n_2 by setting r_2, η_2 and D_2 to zero.

B Proof of Equality of a Third Root and a Committed Number

This proof is derived from [14].

Let n_1 be a large composite number whose factorization is unknown by Alice and Bob, and n_2 be another large composite number whose factorization is known or unknown by Alice. Let g_1 be an element of large order in $\mathbb{Z}_{n_1}^*$ and h_1 be an element of the group generated by g_1 such that both the discrete logarithm of g_1 in base h_1 and the discrete logarithm of h_1 in base g_1 are unknown by Alice. We denote by $E_1(x, r_1) = g_1^x h_1^{r_1} \bmod n_1$ a commitment to x in base (g_1, h_1) where r_1 is randomly selected over $\{-2^s n + 1, ..., 2^s n - 1\}$. We also denote by $E_2(x) = x^3 \bmod n_2$ a RSA$(n_2, 3)$ encryption of x.

Alice secretly holds $x \in \{0, \ldots, b\}$. Let $E = E_1(x, r_1)$ and $F = E_2(x) = x^3 \bmod n_2$ be a commitment to x and a RSA encryption to x. She wants to prove to Bob that she knows x and r_1 such that $E = E_1(x, r_1)$ and $F = E_2(x)$, i.e. that E and F hide the same secret x.

Protocol: $PK(x, r_1, r_2 : E = E_1(x, r_1) \bmod n_1 \wedge F = E_2(x) \bmod n_2)$.

1. Alice computes $\alpha = \frac{F - x^3}{n_2}$ (in $\mathbb{Z}$), $G_2 = E_1(x^2, r_2)$, $G_3 = E_1(x^3, r_3)$ and $Z = E_1(\alpha n_2, -r_3)$.
2. Alice proves to Bob that E, G_2 and G_3 are commitments to the same value respectively in bases (g_1, h_1), (E, h_1) and (G_1, h_1), and that she knows which value is committed by Z in base $(g_1^{n_2}, h_1)$.
3. Bob checks these proofs, computes $T = g_1^F \bmod n_1$ and checks that $T = G_3 Z \bmod n_1$.