Preuves efficaces qu'un nombre engagé appartient à un intervalle

Fabrice Boudot

Résumé. Alice veut prouver qu'elle est assez jeune pour emprunter de l'argent à sa banque, sans révéler son âge. Elle a donc besoin d'un outil pour prouver qu'un nombre engagé [1] appartient à un certain intervalle. Jusqu'à présent, de tels outils étaient soit inefficaces (trop de bits à calculer et transmettre), soit inexacts (i.e. démontraient l'appartenance à un intervalle beaucoup plus grand).
Cet article présente une nouvelle preuve, qui est à la fois *efficace* et *exacte*. Ici, "efficace" signifie qu'il y a moins de 20 exponentiations à effectuer et moins de 2 k-octets à transmettre. Les domaines d'application de cette preuve sont nombreux (monnaie électronique, signatures groupées, cryptage secret vérifiable publiquement, etc. ...).

1. Introduction

L'idée de vérifier si un nombre entier engagé appartient à un intervalle spécifique a été développée initialement dans [2]. Ces sortes de preuves sont intensivement utilisées dans divers domaines : les systèmes de monnaie électronique [7], les signatures groupées [11], les modèles de partage de secret vérifiables publiquement [17, 4], et d'autres protocoles à divulgation nulle (e.g. [13, 10]).

De nos jours, il existe deux méthodes pour démontrer qu'un nombre entier engagé est dans un intervalle particulier :

- la première (voir par exemple [17]) permet de démontrer que la longueur binaire du nombre entier engagé est inférieure ou égale à une valeur fixée k, qui appartient par conséquent à l'intervalle $[0, 2^k - 1]$.
  Malheureusement, cette méthode est très inefficace.
- la seconde méthode (voir par exemple [2, 8]) est beaucoup plus efficace, mais le prix à payer est que seule l'appartenance à un intervalle beaucoup plus grand peut être prouvée.

Dans cette article, nous donnons une nouvelle méthode pour prouver qu'un nombre engagé appartient à un intervalle, qui est plus efficace que la première méthode et qui prouve effectivement, contrairement à la seconde méthode, qu'un nombre engagé $x \in I$ appartient effectivement à I (et pas à un intervalle plus grand).

Tout au long de cet article, $\mathbb{Z}_n$ dénote l'anneau des classes résiduelles modulo n, et $\mathbb{Z}_n^*$ dénote le groupe multiplicatif des éléments inversibles dans $\mathbb{Z}_n$. $|.|$ dénote la longueur binaire , $a\|b$ est la concaténation des chaînes de caractères a et b. On dénote par $\sharp I$ le cardinal de l'ensemble I. Pour $g \in \mathbb{Z}_n^*$, et a dans le groupe engendré par g, on note $\log_g(a)$ le logarithme discret de a en base g modulo n, i.e. le nombre x tel que $a = g^x \bmod n$ qui appartient à $\{-\mathrm{ord}(g)/2, \ldots, \mathrm{ord}(g)/2 - 1\}$, où $\mathrm{ord}(g)$ est l'ordre de g dans $\mathbb{Z}_n^*$. On note $PK(x : \mathcal{R}(x))$ une preuve à divulgation nulle de la

Coordonnées de l'auteur : France Télécom - CNET, 42 rue des Coutures, B.P. 6243, 14066 CAEN CEDEX 4, fabrice.boudot@cnet.francetelecom.fr

Transcription en LaTeX du texte https://www.iacr.org/archive/eurocrypt2000/1807/18070437-new.pdf
Denise Vella-Chemla, décembre 2021.

1. *Note de la traductrice* : Un nombre engagé est un nombre que l'on ne souhaite pas révéler immédiatement, mais dont on engage qu'on ne changera pas la valeur qu'on a choisie pour lui le jour où on la révèlera.

connaissance d'un x telle que $\mathcal{R}(x)$ est vrai.

1.1. Définitions

Définition 1 : *Soit $E = BC(x)$ un engagement sur la valeur de x que $x \in [b_1, b_2]$. Une preuve de l'appartenance à un intervalle $[b_1, b_2]$ est une preuve de connaissance qui assure le vérificateur que le prouveur connaît x tel que $E = BC(x)$ et que x appartient à $[B_1, B_2]$, un intervalle qui contient $[b_1, b_2]$.*

Définition 2 : *En utilisant les notations de la définition 1, le niveau d'expansion d'une preuve d'appartenance à un intervalle est la quantité $\delta = (B_2 - B_1)/(b_2 - b_1)$. Cette quantité peut être ou ne pas être dépendante de $(b_2 - b_1)$.*

On évalue la qualité d'une preuve d'appartenance à un intervalle par la longueur de la preuve (qui doit être aussi courte que possible) et par son niveau d'expansion (qui doit être aussi faible que possible).

1.2. Résultats connus

Dans cette section, on présente trois preuves existantes de l'appartenance à un intervalle. Elles sont basées sur des preuves à divulgation nulle du fait de connaître le logarithme discret soit modulo un nombre premier (Schnorr [19]) soit modulo un nombre composé (Girault [16]).

1.2.1. Preuve classique [17]

Ce protocole prouve qu'un nombre engagé $x \in I = [0, b]$ appartient à $I = [0, 2^k - 1]$, où la longueur binaire de b est k.

Soit p un grand nombre premier, soit q tel que $q \mid p - 1$, et g et h des éléments d'ordre q dans $\mathbb{Z}_p^*$ tels que le logarithme discret de h en base g est inconnu d'Alice. On note $E(x, r) = g^x h^r \bmod p$ un engagement pour x, où r est choisi aléatoirement dans $\mathbb{Z}_p^*$. Soit $x = x_0 2^0 + x_1 2^1 + \ldots + x_{k-1} 2^{k-1}$ pour $x_i \in \{0, 1\}$ et $i = 0, 1, \ldots, k-1$ la représentation binaire de x. Alice définit $E(x_i, r_i)$ pour $i = 0, 1, \ldots, k-1$, où les r_i sont tels que $\sigma_{i=0,\ldots,k-1} r_i = r$, et prouve pour tout i que le nombre caché par $E(x_i, r_i)$ est soit 0 soit 1 en prouvant qu'elle connaît soit un logarithme discret de $E(x_i, r_i)$ en base h soit un logarithme discret de $E(x_i, r_i)/g$ en base h. Cela peut être fait en utilisant les preuves de connaissance d'un logarithme discret [19] et une preuve de connaissance d'un parmi deux [5]. Bob vérifie aussi que $\prod_{i=0,\ldots,k-1} E(x_i, r_i) = E(x, r)$.

Caractéristiques de cette preuve : pour $|p| = 1024$ bits, $|q| = 1023$ bits, $|b| = 512$ bits, et avec comme paramètre de sécurité de la preuve de Schnorr $t = 90$.

- *complétude* : la preuve réussit toujours.
- *robustesse* : un prouveur menteur peut réussir avec une probabilité inférieure à $1-(12^{-89})^{512} < 2^{-80}$.
- *divulgation nulle* : parfaitement à divulgation nulle dans le modèle de l'oracle aléatoire défini en [3].

- *ce qui est démontré* : $x \in [0, 2^k - 1]$.
- *niveau d'expansion* : $1 \leq \delta < 2$ (peut décroître jusqu'à 1 en prouvant qu'à la fois x et $b - x$ sont des nombres de k bits).
- *longueur de la preuve* : 1 612 800 bits = 196.9 kB.

1.2.2. Preuve BCDG [2]

Ce protocole prouve qu'un nombre engagé $x \in I$ appartient à J, où le niveau d'expansion $\sharp J/\sharp I$ est égal à 3. Nous donnons une présentation légèrement différente de celle de l'article original.

Soit t un paramètre de sécurité. Soit p un grand nombre premier, soit q tel que $q|p-1$, et g et h des éléments d'ordre q dans $\mathbb{Z}_p^*$, tels que le logarithme discret de h en base g est inconnu d'Alice. On note par $E = E(x, r) = g^x h^r \bmod p$ un engagement pour $x \in [0, b]$, où r est choisi aléatoirement dans $\mathbb{Z}_p^*$.

Pour simplifier, nous présentons une version interactive du protocole qui peut être aisément transformée en version non-interactive en utilisant l'heuristique de Fiat-Shamir [15].

Protocole : $PK_{[BCDG]}(x, r : E = E(x, r) \wedge x \in [-b, 2b])$.
Exécuter t fois en parallèle :

1. Alice choisit au hasard $\omega_1 \in_R [0, b]$ et initialise $\omega_2 = \omega_1 - b$. Elle choisit également aléatoirement $\eta_1 \in_R [0, q-1]$ et $\eta_2 \in_R [0.q-1]$, et envoie à Bob la paire non-ordonnée d'engagements $W_1 = g^{\omega_1} h^{\eta_1} \bmod p$ et $W_2 = g^{\omega_2} h^{\eta_2} \bmod p$.
2. Bob défie Alice par $c \in_R \{0, 1\}$.
3. Si $c = 0$, Alice envoie à Bob les valeurs de $\omega_1, \omega_2, \eta_1$ et η_2.
   Si $c = 1$, Alice envoie à Bob la valeur de $x + \omega_j, r + \eta_j$; car la valeur $j \in \{1, 2\}$ est telle que $x + \omega_j \in [0, b]$.
   Bob vérifie que $W_1 = g^{\omega_1} h^{\eta_1} \bmod p$ et $W_2 = g^{\omega_2} h^{\eta_2} \bmod p$ dans le premier cas et $W_j = g^{\omega_j} h^{\eta_j} \bmod p$, $x + \omega_j \in [0, b]$ dans le second cas.

Caractéristiques de cette preuve : Pour $|p| = 1024$ bits, $|q| = 1023$ bits, $|b| = 512$ bits, $t = 80$ et $l = 40$.

- *complétude* : la preuve réussit toujours si $r \in [0, b]$.
- *robustesse* : un prouveur menteur peut réussir avec une probabilité inférieure à $2 \times 2^{-t} = 2^{-79}$.
- *divulgation nulle* : preuve parfaitement à divulgation nulle dans le modèle de l'oracle aléatoire.
- *ce qui est démontré* : $x \in [-b, 2b]$.
- *niveau d'expansion* : $\delta = 3$.
- *longueur de la preuve (en moyenne)* : 225 320 bits = 27.5 kB.

1.2.3. Preuve CFT [8]

L'idée principale de cette preuve est essentiellement la même que celle de [2]. Soient t, l et s trois paramètres de sécurité. Ce protocole (dû à Chan, Frankel et Tsiounis [7], et corrigé dans [8], et également dû à [14] dans une autre forme) prouve qu'un nombre engagé $x \in I$ appartient à J, où le niveau d'expansion $\sharp J/\sharp I$ est égal à 2^{t+l+1}. Soit n un grand nombre composé dont la factorisation est

inconnue d'Alice et Bob, g un élément d'ordre élevé dans $\mathbb{Z}_n^*$, et h un élément du groupe engendré par g tel qu'à la fois le logarithme discret de g en base h et le logarithme discret de h en base g sont inconnus d'Alice. Soit H une fonction de hashage qui renvoie des chaînes de caractères de longueur $2t$ bits. Nous notons par $E = E(x, r) = g^x h^r \bmod n$ un engagement pour $x \in [0, b]$, où r est choisi aléatoirement dans $[-2^s n + 1, 2^s n - 1]$. Cet engagement, voir [13], ne révèle statistiquement aucune information sur x à Bob.

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

1. Alice choisit aléatoirement $\omega \in_R [0, 2^{t+l}b - 1]$ et $\eta \in_R [-2^{t+l+s}n + 1, 2^{t+l+s}n - 1]$, et calcule alors $W = g^\omega h^\eta \bmod n$.
2. Alors, elle calcule $C = H(W)$ et $c = C \bmod 2^t$.
3. Finalement, elle calcule $D_1 = \omega + xc$ et $D_2 = \eta + rc$ (dans $\mathbb{Z}$). Si $D_1 \in [cb, 2^{t+l}b - 1]$, elle envoie (C, D_1, D_2) à Bob, sinon, elle recommence le protocole.
4. Bob vérifie que $D_1 \in [cb, 2^{t+l}b - 1]$ et que $C = H(g^{D_1} h^{D_2} E^{-c})$. Cela convainc Bob que $x \in [-2^{t+l}b, 2^{t+l}b]$.

Caractéristiques de la preuve : Pour $|n| = 1024$ bits, $|b| = 512$ bits, $t = 80, l = 40$ et $s = 40$.

- *complétude* : la preuve réussit avec une probabilité supérieure à $1 - 2^l = 1 - 2^{-40}$ si $x \in [0, b]$.
- *robustesse* : un prouveur menteur peut réussir avec une probabilité moindre que 2^{-79}.
- *divulgation nulle* : statistiquement à divulgation nulle dans le modèle de l'oracle aléatoire.
- *ce qui est démontré* : $x \in [-2^{t+l}b, 2^{t+l}b] = [-2^{120}b, 2^{120}b]$.
- *niveau d'expansion* : $\delta = 2^{t+l+1} = 2^{121}$.
- *longueur de la preuve* : 1 976 bits $= 0.241$ kB.

1.3. Nos résultats

Les modèles que nous proposons dans cet article sont beaucoup plus efficaces que la preuve classique et la preuve BCDG, et leur niveau d'expansion sont $\delta = 1 + \varepsilon$ pour le premier modèle, et $\delta = 1$ pour l'autre, où ε est une quantité négligeable par rapport à 1 si l'intervalle considéré est suffisamment grand ($\varepsilon = 2^{-134}$ si le nombre engagé est dans l'intervalle $[0, 2^{512} - 1]$).

Décrivons brièvement nos algorithmes : d'abord notons qu'il suffit de savoir comment prouver qu'un nombre est positif pour prouver qu'un nombre appartient à un certain intervalle. En effet, pour prouver que x appartient à $[a, b]$, il suffit de démontrer que $x - a \geq 0$ et $b - x \geq 0$.

Considérons le modèle d'engagement suivant : pour cacher un entier x, Alice calcule $E(x, r) = g^x h^r \bmod n$, où n est un nombre composé dont la factorisation est inconnue à la fois d'Alice et de Bob, g est un élément d'ordre élevé dans $\mathbb{Z}_n^*$, h est un élément d'ordre élevé du groupe engendré par g tel qu'à la fois le logarithme discret de g en base h et le logarithme discret de h en base g sont inconnus d'Alice, r est choisi aléatoirement dans $[-2^s n + 1, 2^s n - 1]$ et s est un paramètre de sécurité. Cet engagement a été introduit dans [13], et ne révèle statistiquement aucune information sur x à Bob (voir le paragraphe 2.1). Notons que cet engagement est holomorphe, i.e. $E(x + y, r + s) = E(x, r) \times E(y, s) \bmod n$.

Supposons qu'Alice s'engage elle-même sur un entier positif x par $E = E(x, r)$ et qu'elle veut dé-

montrer que $x \in [a, b]$.

Dans notre premier modèle, Alice écrit l'entier positif $x - a$ comme la somme de x_1^2, le plus grand carré inférieur à x et de ρ, un nombre positif inférieur à $2\sqrt{x-a}$ (et par conséquent inférieur à $2\sqrt{b-a}$. Alors, elle choisit aléatoirement r_1, r_2 dans $[0, 2^s n - 1]$ tel que $r_1 + r_2 = r$ et elle calcule $E_1 = E(x_1^2, r_1)$ et $E_2 = E(\rho, r_2)$. Alors, elle prouve à Bob que E_1 cache un carré dans $\mathbb{Z}$ et que E_2 cache un nombre dont la valeur absolue est inférieure à $2^{t+l+1}\sqrt{b-a}$ par une preuve CFT. Finalement, elle applique la même méthode à $b - x$. Cela amène à une preuve que $x \in [a - 2^{t+l+1}\sqrt{b-a}, b + 2^{t+l+1}\sqrt{b-a}]$. Le niveau d'expansion de cette preuve est égal à $1 + (2^{t+l+2}/\sqrt{b-a})$, qui devient proche de 1 quand $b - a$ est grand.

Dans notre second modèle, nous agrandissons artificiellement la taille de x en posant $x' = 2^T x$. En utilisant le premier modèle, nous prouvons que $x' \in [2^T a - 2^{t+l+T/2+1}\sqrt{b-a}, 2^T b + 2^{t+l+T/2+1}\sqrt{b-a}]$, et si T est suffisamment grand (i.e. T est tel que $2^{t+l+T/2+1}\sqrt{b-a} < 2^T$), Bob est convaincu que $x' \in [2^T a - 2^T + 1, 2^T b + 2^T - 1]$, de telle façon que $x \in [a - \varepsilon, b + \varepsilon]$ où $0 \leq \varepsilon < 1$. Ainsi, comme x est un entier, Bob est convaincu que $x \in [a, b]$.

1.4. Organisation de l'article

Dans le paragraphe 2, nous décrivons quelques blocs de construction utilisés dans nos protocoles : une preuve que deux engagements cachent le même secret, et une preuve qu'un nombre engagé est un carré. Dans le paragraphe 3, nous décrivons nos deux modèles : une preuve d'appartenance à un intervalle avec tolérance et une preuve d'appartenance sans tolérance. Alors, nous étendons nos résultats à divers engagements. Au paragraphe 4, nous fournissons une application de nos modèles. Finalement, nous concluons au paragraphe 5.

2. Blocs de construction

Les modèles que nous présentons dans ce paragraphe sont basés sur l'hypothèse suivante, introduite par exemple dans [13] :

Hypothèse RSA forte : Il existe un algorithme efficace qui avec l'entrée $|n|$ renvoie un module RSA n et un élément $z \in \mathbb{Z}_n^*$, tel qu'il est impossible de trouver des entiers $e \notin \{-1, 1\}$ et u tels que $z = u^e \bmod n$.

2.1. Le modèle d'engagement de Fujisaki-Okamoto

Dans ce paragraphe, nous décrivons brièvement le modèle d'engagement que nous utilisons tout au long de cet article.

Soit s un paramètre de sécurité. Soit n un grand nombre composé dont la factorisation est inconnue d'Alice et Bob, g un élément d'ordre élevé dans $\mathbb{Z}_n^*$ et h un élément d'ordre élevé du groupe engendré par g tel qu'à la fois le logarithme discret de g en base h et le logarithme discret de h en base g sont inconnus d'Alice.

On note $E = E(x, r) = g^x h^r \mod n$ un engagement pour x en base (g, h), où r est choisi aléatoirement dans $\{-2^s n + 1, \ldots, 2^s n - 1\}$.

Cet engagement est apparu pour la première fois dans [13].

Proposition 1 : *$E(x, r)$ est un schéma d'engagement statistiquement sûr, i.e.* :

- Alice est incapable de s'engager elle-même sur deux valeurs x_1 et x_2 tels que $x_1 \neq x_2$ (dans $\mathbb{Z}$) par le même engagement à moins qu'elle ne puisse factoriser n ou trouver le logarithme discret de g en base h ou bien le logarithme discret de h en base g. En d'autres termes, sous l'hypothèse de factorisation, il est infaisable de calculer x_1, x_2, r_1, r_2 où $x_1 \neq x_2$ sont tels que $E(x_1, r_1) = E(x_2, r_2)$.
- $E(x, r)$ ne divulgue statistiquement aucune information à Bob. Plus formellement, il existe un simulateur qui renvoie des engagements simulés pour x qui sont statistiquement indistingables des valeurs réelles.

Comme Alice connaît seulement un couple de nombres (x, r) tels que $E = g^x h^r \mod n$, on dit que x est la valeur engagée par (ou cachée par) E, et que E cache le secret x.

2.2. Preuve que deux engagements cachent le même secret

Soient t, l, s_1 et s_2 quatre paramètres de sécurité. Soit n un grand nombre composé dont la factorisation est inconnue d'Alice et de Bob, g_1 un élément d'ordre élevé dans Z_n^*, et g_2, h_1, h_2 des éléments du groupe engendré par g_1 tels que le logarithme discret de g_1 en base h_1, le logarithme discret de h_1 en base g_1, le logarithme discret de g_2 en base h_2 et le logarithme discret de h_2 en base g_2 sont inconnus d'Alice. Soit H une fonction de hashage qui renvoie des chaînes de caractères de longueur $2t$ bits. On note par $E_1(x, r_1) = g_1^x h_1^{r_1} \mod n$ un engagement pour x en base (g_1, h_1) où r_1 est choisi aléatoirement dans $[2^{s_1} n + 1, 2^{s_1} n - 1]$, et $E_2(x, r_2) = g_2^x h_2^{r_2} \mod n$ un engagement pour x en base (g_2, h_2) où r_2 est choisi aléatoirement dans $[-2^{s_2} n + 1, 2^{s_2} n - 1]$.

Alice garde secret $x \in [0, b]$. Soit $E = E_1(x, r_1)$ et $F = E_2(x, r_2)$ deux engagements pour x. Elle veut prouver à Bob qu'elle connaît x, r_1, r_2 tels que $E = E_1(x, r_1)$ et $F = E_2(x, r_2)$, i.e. que E et F cachent le même secret x.

Ce protocole est dérivé de preuves de l'égalité de deux logarithmes discrets des articles [6, 12, 1], combinés avec une preuve de la connaissance du logarithme discret modulo n [16].

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

1. Alice choisit aléatoirement $\omega \in [1, 2^{l+t} b - 1], \eta_1 \in [1, 2^{l+t+s_1} n - 1], \eta_2 \in [1, 2^{l+t+s_2} n - 1]$. Alors, elle calcule $W_1 = g_1^\omega h_1^{\eta_1} \mod n$ et $W_2 = g_2^\omega h_2^{\eta_2} \mod n$.
2. Alice calcule $c = H(W_1 \parallel W_2)$.
3. Elle calcule $D = \omega + cx, D_1 = \eta_1 + cr_1, D_2 = \eta_2 + cr_2$ (dans $\mathbb{Z}$) et elle envoie (c, D, D_1, D_2) à Bob.
4. Bob vérifie si $c = H(g_1^D h_1^{D_1} E^{-c} \mod n \parallel g_2^D h_2^{D_2} F^{-c} \mod n)$.

Il est démontré dans [9] qu'une exécution qui réussit de ce protocole convainc Bob que les nombres

cachés E et F sont égaux sous l'hypothèse que le problème RSA difficile est infaisable.

Caractéristiques de cette preuve : Pour $|n| = 1024$ bits, $|b| = 512$ bits, $t = 80, l = 40$, $s_1 = 40$ et $s_2 = 552$.

- *complétude* : la preuve réussit toujours.
- *robustesse* : sous l'hypothèse de RSA difficile, un prouveur menteur peut réussir avec une probabilité moindre que $2 \times 2^{-t} = 2^{-79}$
- *divulgation nulle* : la divulgation est nulle dans le modèle de l'orable aléatoire si $1/l$ est négligeable.
- *longueur de la preuve* : $2\,648 + 2|x|$ bits $=$ 3672 bits $=$ 0.448 kB.

2.3. Preuve qu'un nombre engagé est un carré

Soient t, l, et s trois paramètres de sécurité. Soit n un grand nombre composé dont la factorisation est inconnue d'Alice et Bob, g un élément d'ordre élevé dans $\mathbb{Z}_n^*$, et h un élément du groupe engendré par g tels qu'à la fois le logarithme discret de g en base h et le logarithme discret de h en base g sont inconnus d'Alice. Soit H une fonction de hashage qui renvoie des chaînes de caractères de longueur $2t$ bits. On note par $E(x, r) = g^x h^r \bmod n$ un engagement pour x en base (g, h) où r est choisi aléatoirement dans $[-2^s n + 1, 2^s n - 1]$.

Alice garde secret $x \in [0, b]$. Soit $E = E(x^2, r_1)$ un engagement sur le carré de x (dans $\mathbb{Z}$). Elle veut prouver à Bob qu'elle connaît x et r_1 tels que $E = E(x^2, r_1)$, i.e. que E cache un carré x^2.

La première preuve qu'un nombre engagé est un carré est apparue dans l'article [13].

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

1. Alice choisit aléatoirement $r_2 \in [-2^s n + 1, 2^s n - 1]$ et elle calcule $F = E(x, r_2)$.
2. Alors, Alice calcule $r_3 = r_1 - r_2$ (dans $\mathbb{Z}$). Noter que $r_3 \in [-2^s bn + 1, 2^s bn - 1]$. Alors, $E = F^x h^{r_3} \bmod n$.
3. Puisque E est un engagement pour x en base (F, h) et F est un engagement pour x en base (g, h), Alice peut faire tourner $PK(x, r_2, r_3 : F = g^x h^{r_2} \bmod n \wedge E = F^x h^{r_3} \bmod n)$, la preuve que deux engagements cachent le même secret décrite au paragraphe 2.2. Elle obtient (c, D, D_1, D_2).
4. Elle envoie (F, c, D, D_1, D_2) à Bob.
5. Bob vérifie que $PK(x, r_2, r_3 : F = g^x h^{r_2} \bmod n \wedge E = F^x h^{r_3} \bmod n)$ est valide.

La robustesse de ce protocole est claire : si Alice est capable de calculer F et de fournir une preuve que E et F sont des engagements au même nombre $\tilde{x}$ resp. en base (F, h) et (g, h), alors Alice connaît $\tilde{x}, \tilde{r}_2$ et $\tilde{r}_3$ tels que $E = F^{\tilde{x}} h^{\tilde{r}_3} = g^{\tilde{x}^2} h^{\tilde{x}\tilde{r}_2 + \tilde{r}_3} = g^{\tilde{x}^2} h^{\tilde{r}_1} \bmod n$. Alors, cette preuve montre qu'Alice connaît $\tilde{x}^2$, un carré qui est caché dans l'engagement E. En d'autres termes, une exécution qui réussit de ce protocole convainc Bob que la valeur cachée dans l'engagement E est un carré dans $\mathbb{Z}$.

Les preuves techniques de la robustesse et de la divulgation nulle de ce protocole sont facilement déduites des propriétés du protocole précédent.

Caractéristique de cette preuve : pour $|n| = 1024$ bits, $|b| = 512$ bits, $t = 80, l = 40$ et $s = 40$.

- *complétude* : la preuve réussit toujours.
- *robustesse* : sous l'hypothèse RSA forte, un prouveur menteur peut réussir avec une probabilité inférieure à $2 \times 2^{-t} = 2^{-79}$.
- *divulgation nulle* : la divulgation est statistiquement nulle dans le modèle de l'oracle aléatoire si $1/l$ est négligeable.
- *longueur de la preuve* : $3\,672 + 2|x|$ bits $=$ 4696 bits $=$ 0.573 kB.

3. Nos modèles

3.1. Preuve qu'un nombre engagé appartient à un certain intervalle

Soient t, l et s trois paramètres de sécurité. Soit n un grand nombre composé dont la factorisation est inconnue d'Alice et Bob, g un élément d'ordre élevé dans $\mathbb{Z}_n^*$, et h un élément du groupe engendré par g tels qu'à la fois le logarithme discret de g en base h et le logarithme de h en base g sont inconnus d'Alice. On note par $E(x, r) = g^x h^r \bmod n$ un engagement pour x en base (g, h) où r est choisi aléatoirement dans $[-2^s n + 1, 2^s n - 1]$.

3.1.1. Preuve avec tolérance : $\delta = 1 + \varepsilon$

Le protocole ci-dessus permet à Alice de prouver à Bob que le nombre engagé $x \in [a, b]$ appartient à $[a - \theta, b + \theta]$, où $\theta = 2^{t+l+1}\sqrt{b-a}$.

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

1. [Connaissance de x]
   Alice exécute avec Bob :
   $PK(x, r : E = E(x, r))$
2. [Initialisation]
   Alice et Bob calculent tous les deux $\tilde{E} = E/g^a \bmod n$ et $\overline{E} = g^b/E \bmod n$. Alice initialise $\tilde{x} = x - a$ et $\overline{x} = b - x$. Maintenant, Alice doit prouver à Bob qu'à la fois $\tilde{E}$ et $\overline{E}$ cachent des secrets qui sont plus grands que $-\theta$.
3. [Décomposition de $\tilde{x}$ et $\overline{x}$]
   Alice calcule :
   $\tilde{x}_1 = \lfloor\sqrt{x-a}\rfloor, \tilde{x}_2 = \tilde{x} - \tilde{x}_1^2,$
   $\overline{x}_1 = \lfloor\sqrt{b-x}\rfloor, \overline{x}_2 = \overline{x} - \overline{x}_1^2.$
   Alors, $\tilde{x} = \tilde{x}_1^2 + \tilde{w}_2$ et $\overline{x} = \overline{x}_1^2 + \overline{x}_2$, où $0 \leq \overline{x}_2 \leq 2\sqrt{b-a}$ et $0 \leq \overline{x}_2 \leq 2\sqrt{b-a}$.
4. [Choix de valeurs aléatoires pour les nouveaux engagements]
   Alice choisit au hasard $\tilde{r}_1$ et $\tilde{r}_2$ dans $[-2^s n + 1, \ldots, 2^s n - 1]$ tels que $\tilde{r}_1 + \tilde{r}_2 = r$, et $\overline{r}_1$ et $\overline{r}_2$ tels que $\overline{r}_1 + \overline{r}_2 = -r$.
5. [Calcul des nouveaux engagements]
   Alice calcule :
   $\tilde{E}_1 = E(\tilde{x}_1^2, \tilde{r}_1), \tilde{E}_2 = E(\tilde{x}_2^2, \tilde{r}_2)$
   $\overline{E}_1 = E(\overline{x}_1^2, \overline{r}_1), \overline{E}_2 = E(\overline{x}_2^2, \overline{r}_2).$

6. [Envoi des nouveaux engagements]
   Alice envoie $\tilde{E}_1$ et $\overline{E}_1$ à Bob. Bob calcule $\tilde{E}_2 = \tilde{E}/\tilde{E}_1$ et $\overline{E}_2 = \overline{E}/\overline{E}_1$
7. [Validité des engagements à un carré]
   Alice exécute avec Bob.
   $PK(\tilde{x}_1, \tilde{r}_1 : \tilde{E}_1 = E(\tilde{x}_1^2, \tilde{r}_1))$,
   $PK(\overline{x}_1, \overline{r}_1 : \overline{E}_1 = E(\overline{x}_1^2, \overline{r}_1))$.
   qui prouve qu'à la fois $\tilde{E}_1$ et $\overline{E}_1$ cachent un carré.
8. [Validité de l'engagement à une petite valeur]
   Soit $\theta = 2^{t+l+1}\sqrt{b-a}$. Alice exécute avec Bob les deux preuves CFT suivantes :
   $PK_{[CFT]}(\tilde{x}_2, \tilde{r}_2 : \tilde{E}_2 = E(\tilde{x}_2, \tilde{r}_2) \wedge \tilde{x}_2 \in [-\theta, \theta])$,
   $PK_{[CFT]}(\overline{x}_2, \overline{r}_2 : \overline{E}_2 = E(\overline{x}_2, \overline{r}_2) \wedge \overline{x}_2 \in [-\theta, \theta])$.
   qui prouvent qu'à la fois $\tilde{E}_2$ et $\overline{E}_2$ cachent des nombres qui appartiennent à $[-\theta, \theta]$, où $\theta = 2^{t+l+1}\sqrt{b-a}$, plutôt que de démontrer qu'ils appartiennent à $[0, 2\sqrt{b-a}]$.

Esquisse de l'analyse :
Après une exécution qui réussit de ce protocole, Bob est convaincu que :
- $\tilde{E}_1$ et $\overline{E}_1$ cachent des nombres qui sont des entiers positifs, puisque ce sont des carrés (étape 7).
- $\tilde{E}_2$ et $\overline{E}_2$ cachent des nombres qui sont plus grands que $-\theta$ (étape 8).
- Alice connaît les valeurs cachées par $\tilde{E}$ et $\overline{E}$ (étapes 1 et 2).
- le nombre caché dans $\tilde{E}$ est la somme du nombre caché dans $\tilde{E}_1$ et du nombre caché dans $\tilde{E}_2$, et il en est de même pour $\overline{E}, \overline{E}_1$, et $\overline{E}_2$ (étape 6).

Ainsi, Bob est convaincu que $\tilde{E}$ et $\overline{E}$ cachent des nombres qui sont plus grands que $-\theta$ puisqu'ils sont somme d'un nombre positif et d'un nombre supérieur à $-\theta$.

Soit x le nombre connu d'Alice (de l'étape 1) et caché par E. Bob est convaincu que $x - a$ est la valeur cachée par $\tilde{E}$ et $b - x$ est la valeur cachée par $\overline{E}$. Ainsi, Bob est convaincu que $x - a \geq -\theta$ et $b - x \geq -\theta$, i.e. que x appartient à $[a - \theta, b + \theta]$, où $\theta = 2^{t+l+1}\sqrt{b-a}$.

Niveau d'expansion : en suivant la définition 2, le niveau d'expansion est égal à :

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

où :

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

ε est négligeable si et seulement si $|b-a| \geq 2t + 2l + 2z + 4$, où z est un paramètre de sécurité. Si c'est le cas, le niveau d'expansion est égal à $\delta = 1 + 2^{-z}$.

Caratéristiques de la preuve : pour $|n| = 1024$ bits, $|b - al = 512$ bits $t = 80, l = 40$ et $s = 40$.
- *longueur de la preuve* : 13860 bits = 1.692 kB.
- *niveau d'expansion* : $\delta = -1 + \varepsilon$, où $\varepsilon \leq 2^{t+l+2-\lfloor \frac{|b-a|}{2} \rfloor} = 2^{-134}$

3.1.2. Preuve sans tolérance : $\delta = 1$

Le protocole ci-dessus permet à Alice de prouver à Bob que le nombre engagé $x \in [a, b]$ appartient à l'intervalle souhaité $[a, b]$.

Pour obtenir une preuve d'appartenance sans tolérance, nous agrandissons artificiellement la taille de x en initialisant $x' = 2^T x$, où $T = 2(t + l + 1) + |b - a|$. Soit $E' = E^{2^T}$, E' est un engagement de Fujisaki-Okamoto pour $x' = 2^T x$ qu'Alice peut ouvrir.

En utilisant le premier modèle, Alice prouve à Bob qu'elle sait que la valeur x' cachée par E' est telle que $x' \in [2^T a - 2^{t+l+1/2+1}\sqrt{b-a}, 2^T b + 2^{t+l+1/2+1}\sqrt{b-a}]$ par une preuve CFT (plutôt que de démontrer que $x' \in [2^T a, 2^T b]$).

Puisque $T = 2(t + l + 1) + |b - a|$, on a :

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

Alors, si Bob est convaincu que $x' \in [2^T a - \theta', 2^T b + \theta']$, il est également convaincu que $x' \in]2^T a - 2^T, 2^T b + 2^T]$.

En supposant qu'Alice ne connaît pas la factorisation de n, elle est incapable de connaître deux valeurs différentes dans $\mathbb{Z}$ cachées par E'. Donc, nécessairement $x' = 2^T x$. La preuve convainc Bob que $2^T \in]2^T a - 2^T, 2^T b + 2^T[$, et ainsi que $x \in]a - 1, b + 1[$. Finalement, puisque x est un nombre entier, Bob est convaincu que $x \in [a, b]$.

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

1. [Initialisation]
   Alice et Bob calculent tous les deux $E' = E^{2^T}$, avec $T = 2(t + l + 1) + |b - a|$.
2. [Preuve]
   Alice exécute avec Bob :
   $PK_{[Avec\ Tol.]}(x', r' : E' = E(x', r') \wedge x' \in [2^T a - 2^{t+l+T/2+1}\sqrt{b-a}, 2^T b + 2^{t+l+T/2+1}\sqrt{b-a}]$.

Caractéristiques de cette preuve : pour $|n| = 1024$ bits, $|b - a| = 512$ bits, $t = 80, l = 40$ et $s = 40$.

- *longueur de la preuve* : 16176 bits = 1.975 kB.
- *niveau d'expansion* : $\delta = 1$.

3.2. Extensions

Les protocoles ci-dessus peuvent être utilisés pour prouver que :

- un logarithme discret modulo un nombre composé n dont la factorisation est inconnue d'Alice appartient à un intervalle. Soit g un élément d'ordre élevé dans $\mathbb{Z}_n^*$, et h un élément du groupe engendré par g tel qu'à la fois le logarithme discret de g en base h et le logarithme discret de h en base g sont inconnus d'Alice. Soit x tel que $y = g^x \bmod n$. Alice choisit aléatoirement

r et calcule $y' = h^r \bmod n$. Elle prouve à Bob qu'elle connaît un logarithme discret de y' en base h, et alors que $yy' = g^x h^r \bmod n$ est un engagement pour une valeur qui appartient à l'intervalle donné.

- un logarithme discret modulo p (un nombre premier ou un nombre composé dont la factorisation est connue d'Alice) appartient à un intervalle. Soit x tel que $Y = G^x \bmod p$. Alice choisit aléatoirement r et calcule $E = E(x, r) = g^x h^r \bmod n$, un engagement pour x. Alors, elle exécute avec Bob $PK(x, r : Y = G^x \bmod p \wedge E = g^x h^r \bmod n)$ (voir l'appendice A) et $PK(x, r : E = g^x h^r \bmod n \wedge x \in [a, b])$.
- une troisième racine (ou, plus généralement, une e-ième racine) modulo N appartient à un intervalle. Soit x tel que $Y = x^3 \ mod N$. Alice choisit aléatoirement r et calcule $E = E(x, r) = g^x h^r \bmod n$, un engagement pour x. Alors, elle exécute avec Bob $PK(x, r : Y = x^3 \bmod N \wedge E = g^x h^r \bmod n)$ (voir l'appendice B) et $PK(x, r : E = g^x h^r \bmod n \wedge x \in [a, b])$.

Note : pour prouver qu'un nombre engagé x appartient à $I \cup J$, Alice prouve que x appartient à I ou que x appartient à J en utilisant une preuve de "ou" comme dans [5].

4. Application au cryptage vérifiable

Comme exemple d'application parmi les multiples applications possibles de l'appartenance à un intervalle, nous présentons dans ce paragraphe un modèle de cryptage public efficace vérifiable.

Alice a envoyé deux messages cryptés à Charlie et Deborah, et veut prouver à Bob que les deux textes cryptés codent le même message.

Charlie et Deborah utilisent le système de cryptage d'Okamoto-Uchiyama [18], i.e. Charlie garde un nombre composé $n_C = p_C^2 q_C$ ($|p_C| = |q_C| = k$), un élément $g_C \in \mathbb{Z}_{n_C}^*$ tel que l'ordre de $g_C^{m p_C - 1} \bmod p_C$ est p_C, et Deborah garde un nombre composé $n_D = p_D^2 q_D$ ($|p_D| = |q_D| = k$), un élément $g_D \in Z_{n_D}^*$, tel que l'ordre de $g_D^{p_D - 1} \bmod p_D^2$ est p_D.

On note par $h_C = g\text{ç}C^{n_C} \bmod n_C$ et $h_D = g_D^{n_D} \bmod n_D$.

Pour crypter un message m tel que $0 \leq m \leq 2^{k-1}$ destiné à Charlie, Alice calcule $E_C = g_C^m h_C^{r_C} \bmod n_C$, où r_C est choisi aléatoirement dans $\mathbb{Z}_{n_C}^*$. De la même façon, elle crypte le même message m destiné à Deborah en calculant $E_D = g_D^m h_D^{r_D} \bmod n_D$.

Maintenant, Alice veut prouver à Bob que les deux textes chiffrés E_C et E_D codent le même message.

D'abord, elle exécute avec Bob $PK(m, r_C, r_D : E_C = g_C^m h_C^{r_C} \bmod n_C \wedge E_D g_D^m h_D^{r_D} \bmod n_D)$, une preuve d'égalité de deux nombres engagés selon différents modules (voir l'appendice A). Cela prouve seulement qu'elle connaît un entier m tel que $m \bmod p_C$ et $m \bmod p_D$ sont respectivement les messages cryptés par Charlie et Deborah. Notons que si m est plus grand que p_C et p_D, alors $m \bmod p_C \neq m \bmod p_D$. Donc il est nécessaire qu'Alice prouve aussi à Bob que m est inférieur à p_C et p_D. Alice utilise la preuve d'appartenance à un intervalle sans tolérance présentée au paragraphe 3.1.2 : $PK(m, r_C : E_C = g_C^m h_C^{r_C} \bmod n_C \wedge m \in [0; 2^{k-1}])$. Alors, nécessairement, $m \bmod p_C = m \bmod p_D$: Bob est convaincu qu'Alice a secrètement envoyé le même message à Charlie et à Deborah.

5. Conclusion

Nous avons présenté dans cet article des preuves efficaces qu'un nombre engagé appartient à un intervalle et fourni des exemples d'applications, plus particulièrement un modèle efficace et vérifiable de cryptage. Par leur efficacité, ces preuves sont bien adaptées pour être utilisées dans des protocoles de cryptographie variés.

Remerciements

Nous souhaiterions remercier Marc Girault pour des discussions et commentaires fructueux.

Références

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), consultable ici 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, consultable ici 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 Share holders. 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. Preuve de l'égalité de deux nombres engagés selon différents modules

Cette preuve est apparue initialement dans [4] et indépendamment dans [10] sous une forme plus générale.

Soient t, l et s trois paramètres de sécurité. Soit n_1 un grand nombre composé dont la factorisation est inconnue d'Alice et Bob, et n_2 un autre grand nombre, premier ou composé dont la factorisation est connue ou inconnue par Alice. Soit g_1 un élément d'ordre élevé dans $\mathbb{Z}^*_{n_1}$, et h_1 un élément du groupe engendré par g_1 tel qu'à la fois le logarithme discret de g_1 en base h_1 et le logarithme discret de h_1 en base g_1 sont inconnus d'Alice. Soit g_2 un élément d'ordre élevé dans $\mathbb{Z}^*_{n_2}$, et h_2 un élément

du groupe engendré par g_2 tel qu'à la fois le logarithme discret de g_2 en base h_2 et le logarithme discret de h_2 en base g_2 sont inconnus d'Alice. Soit H une fonction de hashage qui renvoie des chaînes de caractères de longueur $2t$ bits. On note $E_1(x, r_1) = g_1^x h_1^{r_1} \bmod n_1$ un engagement pour x en base (g_1, h_1) où r_1 est choisi au hasard dans $\{-2^s n + 1, ..., 2^s n - 1\}$, et $E_2(x.r_2) = g_2^x h_2^{r_2} \bmod n_2$ un engagement pour x en base (g_2, h_2) où r_2 est choisi au hasard dans $\{-2^s n + 1, \ldots, 2^s n - 1\}$.

Alice maintient secrètement $x \in \{0, ..., b\}$. Soit $E = E_1(x, r_1)$ et $F = E_2(x, r_2)$ deux engagements pour x. Elle veut prouver à Bob qu'elle connaît x, r_1, r_2 tels que $E = E_1(x, r_1)$ et $F = E_2(x, r_2)$, i.e. que E et F cachent le même x secret.

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

1. Alice choisit au hasard $\omega \in \{1, \ldots, 2^{l+t}b - 1\}, \eta_1 \in \{1, \ldots, 2^{l+t+s}n - 1\}, \eta_2 \in \{1, \ldots, 2^{l+t+s}n - 1\}$. Alors, elle calcule $W_1 = g_1^{\omega} h_1^{\eta_1} \bmod \eta_1$ et $W_2 = g_2^{\omega} h_2^{\eta_2} \bmod n_2$.
2. Alice calcule $c = H(W_1 \parallel W_2)$.
3. Elle calcule $D = \omega + cx, D_1 = \eta_1 + cr_1, D_2 = \eta_2 + cr_2$ (dans $\mathbb{Z}$) et envoie (c, D, D_1, D_2) à Bob.
4. Bob vérifie si $c = H(g_1^D h_1^{D_1} E^{-c} \bmod n_1 \parallel g_2^D h_2^{D_2} F^{-c} \bmod n_2)$.

Notons que ce protocole peut être utilisé pour prouver l'égalité de plus de deux nombres engagés, ou pour prouver l'égalité d'un nombre engagé modulo n_1 et d'un logarithme discret modulo n_2 en initialisant r_2, η_2 et D_2 à zéro.

B. Preuve de l'égalité d'une troisième racine et d'un nombre engagé

Cette preuve est dérivée de [14].

Soit n_1 un grand nombre composé dont la factorisation n'est pas connue d'Alice et Bob, et n_2 un autre grand nombre composé dont la factorisation est connue ou inconnue d'Alice. Soit g_1 un élément d'ordre élevé dans $\mathbb{Z}_{n_1}^*$, et h_1 un élément du groupe engendré par g_1 tels qu'à la fois le logarithme discret de g_1 en base h_1 et le logarithme discret de h_1 en base g_1 sont inconnus d'Alice. On dénote par $E_1(x, r_1) = g_1^x h_1^{r_1} \bmod n_1$ un engagement pour x en base (g_1, h_1) où r_1 est choisi au hasard dans $\{-2^s n + 1, \ldots, 2^s n - 1\}$. On dénote également par $E_2(x) = x^3 \bmod n_2$ un codage crypté RSA$(n_2, 3)$ de x.

Alice garde secret $x \in \{0, \ldots, b\}$. Soient $E = E_1(x, r_1)$ et $F = E_2(x) = x^3 \bmod n_2$ un engagement pour x et un codage crypté RSA pour x. Elle veut prouver à Bob qu'elle connaît x et r_1 tels que $E = E_1(x, r_1)$ et $F = E_2(x)$, i.e. que E et F cachent le même x secret.

Protocole : $PK(x, r_1, r_2 : E = E_1(x, r_1) \bmod n_1 \wedge F = E_2(x^2, r_2) \bmod n_2)$.

1. Alice calcule $\alpha = \dfrac{F - x^3}{n_2}$ (dans $\mathbb{Z}$).
2. Alice prouve à Bob que E, G_2 et G_3 sont des engagements pour la même valeur respectivement dans les bases $(g_1, h_1), (E, h_1)$ et (G_1, h_1), et qu'elle sait quelle valeur est engagée par Z en base $(g_1^{n_2}, h_1)$.
3. Bob vérifie ces preuves, calcule $T = g_1^F \bmod n_1$ et vérifie que $T = G_3 Z \bmod n_1$.