GQ2
une preuve zero-knowledge de connaissance de la factorisation complément essentiel à RSA

Sophie Boutiton[1], François Daudé[2], and Louis Guillou[3]

[1] Doctorante à France Télécom R&D
[2] Ingénieur de recherche à France Télécom R&D
[3] Expert Emérite à France Télécom R&D,
4 rue du Clos de Courtel
35 512 Cesson Sévigné, France

Résumé Nous présentons un protocole d'authentification et de signature électronique inventé par L. Guillou et J.J. Quisquater et appelé GQ2. Nous caractérisons de manière riguoureuse les conditions suffisantes pour que le protocole GQ2 soit une preuve zero-knowledge de connaissance de la factorisation et complétons les éléments de preuve apportés dans [8]. Nous évaluons alors ses performances en le comparant aux principaux protocoles d'authentification existants.
Nous montrons ainsi qu'il offre le meilleur compromis actuel en terme de sécurité et de performance. En particulier, nous montrons qu'à sécurité égale (c'est à dire pour un même module RSA-1024), l'authentification GQ2 est 40 fois plus rapide que l'authentification RSA.

1 Introduction

La découverte, faite en 1977 par Rivest Shamir et Adleman, de l'algorithme RSA [15] a révolutionné le monde de la sécurité, en proposant une réponse efficace au problème de l'authentification. Il faut attendre 1985 pour voir Golwasser, Micali et Rackoff [3] introduire le concept de « zero-knowledge » et apporter une réponse nouvelle au problème de l'authentification. Depuis, de nombreux algorithmes de type « zero-knowledge » ont été proposés dans la litterature scientifique, et dans le but de les comparer, deux critères de base peuvent être pris en considération :

- **la sécurité :** Dans ce cas, on cherche à établir une relation logique entre la sécurité de l'algorithme et la difficulté pour résoudre un certain problème mathématique. Cela suppose au préalable de disposer d'une formalisation mathématique précise de la notion de sécurité de l'algorithme.
- **La performance :** Dans ce cas, on peut la décliner par l'intermédiaire de différentes caractéristiques : le temps de calcul des différentes ressources, le nombre de bits échangés entre les différentes ressources, ou encore la taille mémoire utilisée par chaque ressource.

Dans ce papier, nous nous proposons d'étudier la sécurité et les performances du mécanisme zero-knowledge GQ2 et de montrer qu'il réalise le meilleur compromis actuel de ces deux critères.

1.1 Résultats précédents

En 1987, A.Fiat et A.Shamir [2] propose le premier schéma d'authentification zero-knowledge. Sa sécurité est basée sur le problème de la factorisation, plus précisément le problème du calcul d'une racine carrée modulo n (où n désigne un entier de Blum). D'un point de vue performance, sa faiblesse réside dans le fait que le protocole exige un très grand nombre de bits échangés entre le prouveur et le vérifieur.

En 1988, L.Guillou et JJ.Quisquater [6] propose un protocole appelé GQ1. Ce protocole réduit considérablement le volume de données échangées. Ce protocole est prouvée zero-knowledge, mais sa sécurité n'est plus directement liée à la factorisation mais seulement au problème RSA.

En 1990, H.Ong et C.P.Schnorr [12] proposent un protocole qui, comme GQ1, réduit le volume de données échangées. Sa sécurité est basée sur le problème difficile du calcul des racines carrées successives. Cependant, bien que prouvé sûr contre les attaques actives dans le cas des entiers de Blum [18] puis dans le cas d'un module quelconque [17], il n'est pas « zero-knowledge » dans le sens donnée par [3].

En 2001, L.Guillou et JJ.Quisquater [8] présentent un nouveau protocole GQ2. Il accroit les performances du schéma de Ong-Schnorr et de GQ1. Quand à sa sécurité, des éléments de preuve sont apportés concernant son caractère « zero-knowledge » et sa relation avec le problème de la factorisation.

En parallèle, grâce en particulier aux travaux de O.Goldreich [20], une formalisation mathématique précise du concept de protocole « zero-knowledge » a été effectuée. Cette formalisation fournit le matériel mathématique nécessaire pour établir les preuves de sécurité des protocoles zero-knowledge.

1.2 Nos résultats

En se basant sur le formalisme mathématique introduit par [20] et précisé par [14], nous caractérisons rigoureusement les conditions suffisantes pour que le protocole GQ2 soit une preuve zero-knowledge de connaissance de la factorisation au sens de [3].

En particulier, nous montrons que s'il existe une attaque permettant de tromper le vérifieur avec une probabilité non négligeable, alors il existe un algorithme de factorisation en temps polynomial.

Par ailleurs, nous comparons les performances du protocole GQ2 avec différents protocoles de sécurité selon plusieurs critères : la complexité de calcul du prouveur puis du vérifieur, la taille mémoire nécessaire au prouveur pour le stockage de sa clé privée et le volume des données qui transitent entre le prouveur et le

vérifieur. Nous montrons ainsi que GQ2 offre des performances bien supérieures aux principaux mécanismes d'authentification, exception faite du volume de stockage de la clé privée. En particulier, nous établissons que pour un même module RSA-1024, l'authentification GQ2 est 40 fois plus rapide que celle obtenue à partir du RSA.

2 Présentation du protocole d'authentification GQ2

2.1 Elaboration des bi-clés GQ2

Cette description est conforme aux spécifications de GQ2 présentes dans la norme ISO/IEC 9798-5 [9]. GQ2 fait appel aux trois paramètres suivants :

- Un paramètre noté k appelé **paramètre de sécurité**.
- Un paramètre noté m appelé **paramètre de multiplicité**.
- Un paramètre noté v appelé **exposant de vérification** et défini par $v = 2^{k+1}$.

La construction d'une bi-clé GQ2 s'effectue selon les étapes suivantes :

- On choisit aléatoirement deux nombres premiers p_1 et p_2 congrus à 3 modulo 4
- On calcule le module n égal au produit de p_1 par p_2
- La clé publique GQ2 se compose du module n et de m nombres publics notés $(G_1, .., G_m)$, chaque G_i étant le carré d'un petit nombre premier noté g_i et appelé **nombre de base**.
- La clé publique GQ2 doit vérifier la propriété suivante :
  Pour au moins un nombre de base noté g, nous avons : $\left(\frac{g}{p_1}\right) = -\left(\frac{g}{p_2}\right)$ où $\left(\text{-}\right)$ désigne le symbole de Jacobi ([11], §2.4)
- La clé privée GQ2 se compose des nombres premiers p_1,p_2 et de m nombres secrets notés $(Q_1, .., Q_m)$ reliés aux nombres publics par la relation suivante :
$$\forall i \in \{1, .., m\}, G_i Q_i^v = 1 \bmod n$$

2.2 Le protocole d'authentification GQ2

Le protocole GQ2 s'effectue entre un prouveur et un vérifieur. Le vérifieur connaît la clé publique GQ2 $(n, G_1, .., G_m)$ et le prouveur connaît la clé privée GQ2 $(p_1, p_2, Q_1, .., Q_m)$. Ils possèdent en commun l'exposant de vérification $v = 2^{k+1}$ et le paramètre de multiplicité m.

Le prouveur GQ2 réalise alors systématiquement les étapes suivantes :

1. Sélection d'un nombre aléatoire positif et inférieur à n, noté r,
2. Calcul de $W = r^v \bmod n$ appelé **témoin** et noté W,
3. En réponse à un défi émis par le vérifieur, consistant en m nombres aléatoires de k-bits notés $(d_1.., d_m)$, calcul du nombre $D = r.Q_1^{d_1}..Q_m^{d_m}$ appelé **réponse** et noté D,

4. Effacement du nombre aléatoire r.

Le vérifieur réalise systématiquement les étapes suivantes :

1. Réception de la part du prouveur du témoin W,
2. Sélection de m nombres aléatoires de k-bits notés $(d_1, .., d_m)$,
3. En réponse à un nombre D émis par le prouveur, calcul du nombre $W' = D^v.G_1^{d_1}...G_m^{d_m} \bmod n$ et vérification de la condition $W' = W \wedge W' \neq 0$
4. Si la condition précédente est vérifiée, acceptation du prouveur.

Lorsque ce protocole est effectué un nombre t de fois, on parle du protocole **GQ2 itéré à l'ordre** t. Conformément à la méthode décrite en [11], note 10.30, le protocole d'authentification peut être transformé en mécanisme de signature électronique.

3 Analyse de sécurité du protocole GQ2

3.1 Rappels de concepts mathématiques utiles

Cette section rappelle les principales notions mathématiques nécessaires à l'énoncé des preuves de sécurité. On définit l'ensemble des mots $E^* = \{0,1\}^*$, Pour tout élément x de E^*, on désigne par $|x|$ la longueur du mot x, définie par $|x| = inf\{n/x \in \{0,1\}^n\}$.

On suppose connues les notions de machines de Turing, de complexité d'une machine de Turing et de machine de Turing probabiliste à temps polynomial (que l'on abrège par MT). On se reportera à [14] pour les définitions mathématiques exactes. On utilise par la suite la notation $M_{w_m}(x)$ pour désigner le mot calculé par la MT M à partir du mot x et de l'aléa (on dit encore ruban) w_m. On rappelle , toutefois, les notions suivantes (elles aussi inspirées de [14]) :

- Deux variables aléatoires (v.a.) $\{U(x)\}$ et $\{V(x)\}$ paramétrées par un ensemble de mots E^* (c'est à dire des v.a. à valeurs dans E^*) sont dites **parfaitement indistinguables** si

$$\forall x \in E^*, U(x) = V(x)$$

  Intuitivement cela signifie que pour tout mot x, on ne peut distinguer deux échantillons de U et de V quelque soit leur taille et la puissance de calcul disponible.
- Soit $P(x, y)$ un **prédicat à deux variables** calculable en temps polynomial en $|x|$. On dit que y est **valide** s'il existe P tel que $P(x, y)$. Pour un x fixé, une donnée y vérifiant $P(x, y)$ est appelé un **témoin** de y.
- Une fonction f de E^* dans R est dite **négligeable** si :

$$\forall c \in \mathbb{N}^*, \exists n_0 \in \mathbb{N}/\forall |G| \geq n_0, f(G) < \frac{1}{|G|^c}$$

Mathématiquement, le protocole GQ2 appartient à la classe des protocoles interactifs à 3 passes, dont on donne la définition ci-dessous :

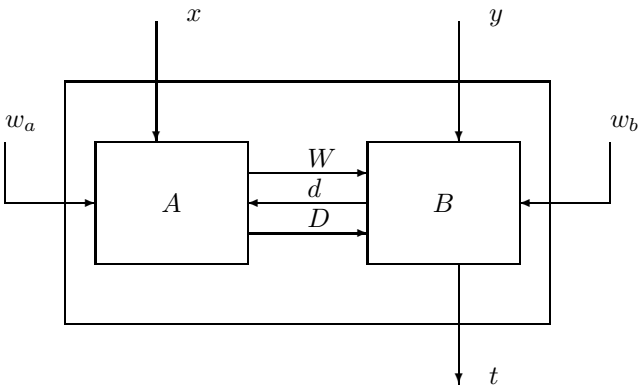
Definition 1. *On appelle* ***protocole interactif à 3 passes*** *le couple, noté* $\langle A(x), B(y)\rangle$*, constitué de deux machines de Turing probabiliste à temps polynomial* A *et* B *et vérifiant la propriété suivante :*

$$\forall(x, y, w_a, w_b)\ , \exists(W, d, D, t)\ /$$
$$A_{w_a}(x, d) = (W, D) \quad et \quad B_{w_b}(y, W, D) = (d, t) \quad et \quad t \in \{0, 1\}$$

avec les notions suivantes associées :
- A *désigne le prouveur et* B *le vérifieur,*
- w_a *et* w_b *désignent les aléas (ou rubans aléatoires) utilisés par* A *et* B *respectivement,*
- (W, d, D) *désigne les données échangées entre* A *et* B *que l'on note encore* $VUE\langle A(x), B(y)\rangle$*,*
- t *désigne la réponse du protocole, que l'on note* $\langle A(x), B(y)\rangle$*,*

Lorsque $\langle A(x), B(y)\rangle = 1$ *on dit que le prouveur* A *est accepté par le vérifieur* B*.*

Schématiquement, un protocole interactif à 3 passes se représente de la manière suivante :



Pour prouver la sécurité du protocole GQ2, nous suivons l'approche élaborée par Goldwasser Micali Rackoff [3], consistant à montrer qu'un protocole interactif à trois passes possède les trois propriétés suivantes :
- **Completeness** : Si le prouveur connait la clé GQ2 (c'est à dire la factorisation du module) alors le vérifieur doit l'accepter avec une probabilité écrasante,

- **Soundness** : Si le prouveur ne dispose pas de clé GQ2 (c'est à dire ne connaît pas la factorisation du module) alors quelque soit la stratégie choisie par le prouveur, le vérifieur doit le rejeter avec une probabilité écrasante.
- **Zero-knowledge** : Quelque soit la stratégie choisie par le vérifieur et quelque soit la quantité d'information qu'il récupère en interagissant avec un prouveur , le vérifieur n'arrivera jamais à récupérer le secret de la factorisation du module détenu par le prouveur.

Mathématiquement, cela se traduit de la manière suivante :

Definition 2. *On dit qu'un protocole interactif $\langle A(x), B(y)\rangle$ est une* ***preuve zero-knowledge de connaissance d'un prédicat P(Q,G)*** *si les trois propriétés suivantes sont respectées :*

1. *Propriété de* ***« consistance »*** *(completeness) :*
   Pour tout G valide, si A connaît un témoin de G, alors A convainc B soit formellement :

$$\forall (G,Q), P(Q,G) \Rightarrow Pr_{w_a,w_b}[\langle A_{w_a}(Q), B_{w_b}(G)\rangle] \geq 1 - e^{-|G|}$$

2. *Propriété de* ***« significativité »*** *(soundness) :*
   Pour tout G valide, si un prouveur $\tilde{A}$ est capable de convaincre B avec une probabilité non négligeable alors il doit nécessairement connaître un témoin de G, soit formellement :

$$\forall c \in \mathbb{N}^*, \exists M \text{ une } MT / \forall \tilde{A} \text{ une } MT, \exists n_0 \in \mathbb{N}, \forall G / |G| > n_0,$$

$$Pr_{w_{\tilde{a}},w_b}[\langle \tilde{A}_{w_{\tilde{a}}}(Q), B_{w_b}(G)\rangle] \geq \frac{1}{|G|^c} \Rightarrow Pr_{w_m}[P(M_{w_m}(G), G)] \geq 1 - e^{-|G|}$$

3. *Propriété de* ***« sans connaissance »*** *(zero-knowledge) :*
   Pour tout G valide, toute information obtenue par un vérifieur $\tilde{B}$ au cours de l'exécution du protocole avec A, peut être obtenue par $\tilde{B}$ à l'aide d'une simulation sans interaction avec A, soit formellement :

$$\forall \tilde{B} \text{ une } MT, \exists M \text{ une } MT \ / \ \forall (G,Q) \ / \ P(G,Q) \ \forall (a,b,c)$$

$$Pr_{w_a,w_{\tilde{b}}}[VUE\langle A_{w_a}(Q), \tilde{B}_{w_{\tilde{b}}}(G)\rangle = (a,b,c)] = Pr_{w_m}[P(M_{w_m}(G) = (a,b,c)]$$

3.2 GQ2 est une preuve zero-knowledge de connaissance de la factorisation

Pour établir que GQ2 est une preuve zero-knowledge de connaissance de la factorisation, nous devons démontrer que

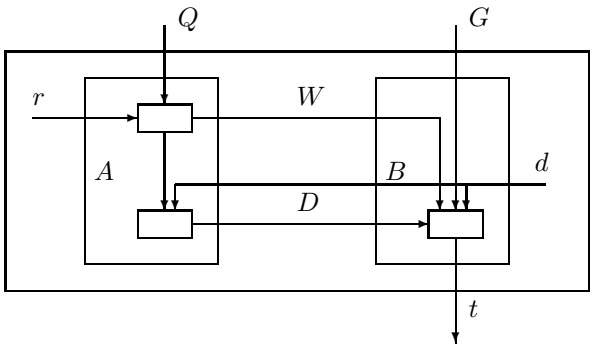
- GQ2 est un protocole interactif à 3 passes au sens de la définition 1,
- Le prédicat associé à GQ2 est équivalent au prédicat associée à la factorisation et défini par $F(p_1, p_2, n) \equiv (n = p_1 * p_2)$,
- GQ2, comme protocole interactif, respecte les propriétés « completeness », « soundness » et « zero-knowledge » au sens de la définition 2.

GQ2 est un protocole interactif à 3 passes

En notant : $G = (n, g_1, .., g_m)$, $Q = (p_1, p_2, Q_1, .., Q_m)$ et $d = (d_1, .., d_m)$ on peut définir les deux MT :

- $A_r(Q, d) = (W, D)$ où $W = r^v \bmod n$ et $D = r.Q_1^{d_1}...Q_m^{d_m} \bmod n$
- $B_d(G, W, D) = (d, t)$ où $t = 1 \Leftrightarrow W = D^v.g_1^{2\times d_1}....g_m^{2\times d_m} \bmod n$

Le schéma ci-dessous permet de vérifier simplement que GQ2 est bien un protocole à 3 passes au sens de la définition 1 :



Le prédicat associé à GQ2 est équivalent au prédicat associé à la factorisation

Le prédicat associé à GQ2 est défini par l'expression suivante :

$$P(Q, G) \equiv \left(\wedge_{i:1..m} g_i^2 Q_i^v \equiv 1 \bmod n\right)$$

Il est clair que la connaissance de G et de la factorisation du module n permet de déterminer le témoin Q de G (algorithme classique d'extraction de racine v-ième). Réciproquement, sachant qu'il existe un nombre de base g tel que $\left(\frac{g}{p_1}\right) = -\left(\frac{g}{p_2}\right)$ en posant $X = g$ et $Y \equiv Q^{-v/2} \bmod n$, on vérifie que $X^2 \equiv Y^2 \bmod n$ mais que $X \neq \pm Y \bmod n$. On en déduit donc la factorisation de $n = gcd(X - Y, n) \times gcd(X + Y, n)$.

De fait, si GQ2 est une preuve zero-knowledge de la connaissance du prédicat $P(Q, G) \equiv \left(\wedge_{i:1..m} g_i^2 Q_i^v \equiv 1 \bmod n\right)$, il est aussi une preuve zero-knowledge de la connaissance de la factorisation du module n.

GQ2 respecte la propriété « completeness »

Par construction de la réponse D, le protocole GQ2 respecte trivialement la propriété « completeness ».

GQ2 respecte la propriété « soundness »

Dans [8], on montre que la connaissance de deux triplets entrelacés

$\{(W,d,D),(W,e,C)/d \neq e\}$ permet d'en déduire la factorisation du module. Toutefois, pour en déduire que GQ2 respecte la propriété « soundness », il faut aussi s'assurer que l'on peut produire de tels triplets en un temps polynomial.

Conformément à la définition 2, il nous faut donc construire une MT notée M telle que si $\tilde{A}$ est une MT qui convainc B avec une probabilité non négligeable, c'est à dire formellement $Pr_{w_{\tilde{a}},d}[\langle \tilde{A}_{w_{\tilde{a}}}(G), B_d(G)\rangle] \geq \frac{1}{|G|^c}$ alors la MT M peut calculer un témoin de G c'est à dire formellement $Pr_{w_m}[P(M_{w_m}(G),G)] \geq 1 - e^{-|G|}$. La construction de M repose sur une première MT, notée M', paramétrée par $v = 2^{k+1}$ et m, et définie par :

Entrée : W, d, D, e, E, $G = (n, g_1, ..., g_m)$
$X \leftarrow \left(\frac{E}{D}\right)^{v/2} \bmod n$
$Y \leftarrow g_1^{d_1-e_1} \times .. \times g_m^{d_m-e_m} \bmod n$
$Q^* \leftarrow NULL$
Si $gcd(X-Y,n) \neq 1, n$ **alors**
$p_1 \leftarrow gcd(X-Y,n)$
$p_2 \leftarrow gcd(X+Y,n)$
$(Q_1,..,Q_m) \leftarrow$ racine v-ième de $(g_1,..,g_m)$ sachant p_1, p_2
$Q^* \leftarrow (Q_1,..,Q_m)$
Fin si
Sortie : Q^*

La MT M , paramétrée par le vérifieur de $GQ2$ noté $B_d(G)$ et par le prouveur $\tilde{A}_{w_a}(G)$, se définit alors de la manière suivante :

Entrée : G, c
Pour i **de** 1 **à** $L = 32|G|^{4c}$ **faire :**
$w_a \leftarrow ()$;$d \leftarrow ()$;$e \leftarrow ()$ /* sélection aléatoire */
$Q \leftarrow NULL$
Si$\langle \tilde{A}_{w_a}(G), B_d(G)\rangle$ **et** $\langle \tilde{A}_{w_{\tilde{a}}}(G), B_e(G)\rangle$ et $e \neq d$ **alors**
$(W,d,D) \leftarrow VUE\langle \tilde{A}_{w_a}(G), B_d(G)\rangle$
$(W,e,E) \leftarrow VUE\langle \tilde{A}_{w_a}(G), B_e(G)\rangle$
$Q \leftarrow M'(W,d,D,e,E,G)$
si $Q \neq NULL$ **alors** sortir de la boucle POUR **Fin si**
Fin si
Fin Pour
Sorter : Q

M' étant une MT, il est clair que M est aussi une MT. Il faut évaluer la probabilité que $M(G)$ soit bien un témoin de G. Pour cela, il faut calculer la probabilité des deux tests SI-ALORS présent dans l'algorithme M. En adaptant un lemme probabiliste donné par [19], on montre que :

Lemma 1. *Soient $\tilde{A}$ et B deux MT. Si on suppose $log(|n|) = o(m.k)$ alors*

$$\forall c \in \mathbb{N}^*, \forall G/|G| > |n|, Pr_{w_{\tilde{a}},d}[\langle \tilde{A}_{w_{\tilde{a}}}(G), B_d(G)\rangle] \geq \frac{1}{|G|^c} \Rightarrow$$
$$Pr_{w_{\tilde{a}},d,e}[\langle \tilde{A}_{w_{\tilde{a}}}(G), B_d(G)\rangle, \langle \tilde{A}_{w_{\tilde{a}}}(G), B_e(G)\rangle, d \neq e] \geq \frac{1}{16|G|^{3c}}$$

Intuitivement, cela signifie que si un prouveur $\tilde{A}$ ne connaissant pas une clé privée GQ2 peut être accepté par un vérifieur B avec une probabilité non négligeable, alors la probabilité d'observer des triplets de la forme

$$\{(W, d, D), (W, e, C)/d \neq e\}$$

dans les échanges entre $\tilde{A}$ et B est, elle aussi, non négligeable.

Par ailleurs, on dispose du lemme suivant qui prolonge le résultat obtenu en [8] :

Lemma 2. *Si A et B désignent respectivement le prouveur et le vérifieur du protocole GQ2 et s'il existe deux triplets $(W, d, D) = VUE\langle \tilde{A}_{w_a}(G), B_d(G)\rangle$ et $(W, e, E) = VUE\langle \tilde{A}_{w_a}(G), B_e(G)\rangle$ tels que $d \neq e$ alors il existe deux entiers X et Y tels que $Pr_{w_{\tilde{a}},d,e}[gcd(X - Y, n) \neq 1, n] = \frac{1}{2}$*

En effet, par définition d'une clé GQ2, il existe $i \in \{1, .., m\}$ tel que $\left(\frac{g_i}{p_1}\right) = -\left(\frac{g_i}{p_2}\right)$. Avec les notations du lemme, on pose $X = \left(\frac{E}{D}\right)^{v/2} \bmod n$ et $Y = g_1^{d_1 - e_1} \times .. \times g_m^{d_m - e_m} \bmod n$. par construction $X^2 = Y^2 \bmod n$ mais $X \neq \pm Y \bmod n$.

Pour conclure, la probabilité que $M(G)$ soit un témoin de G est donc :

$$Pr_{w_{\tilde{a}},d,e}[P(M(G), G)] \geq 1 - \left(1 - \frac{1}{2 \times 16|G|^{3c}}\right)^{32|G|^{4c}} \geq 1 - e^{-|G|}$$

Ainsi, si les clés GQ2 respectent les conditions du paragraphe 2.1 et si les paramètres k et m de GQ2 vérifient la condition « $log(|n|) = o(m.k)$ » , alors le protocole GQ2 possède la propriété « soundness ».

En adaptant la preuve au protocole GQ2 itéré à l'ordre t, il n'est pas difficile de corriger l'hypothèse sur les paramètres k,t et m et montrer qu'avec la condition « $log(|n|) = o(t.m.k)$ » le protocole GQ2 itéré à l'odre t possède encore la propriété « soundness ».

La conséquence est que s'il existe une attaque permettant de tromper le vérifieur avec une probabilité de réussite supérieure à 2^{-tkm}, alors il existe un algorithme de factorisation du module n en temps polynomial.

GQ2 respecte la propriété « zero-knowledge »

Il s'agit de montrer que l'observation des échanges entre un vérifieur malhonnête

et un prouveur A connaissant le témoin Q de G apporte la même information que les échanges simulés par $\tilde{B}$ à l'aide d'une MT $M(G)$ ne connaissant pas le témoin de G.
Mathématiquement, il faut donc construire une MT $M(G)$ dont la loi de probabilité est indistinguable de la variable aléatoire $VUE\langle A_r(Q), \tilde{B}_{w_d}(G)\rangle$

Le tableau ci-dessous indique le mode de génération des deux v.a. :

v.a. $VUE\langle A_r(Q), \tilde{B}_{w_b}(G)\rangle$:	v.a. M(G) :
	répéter
$r \leftarrow \{0,..,n-1\}()$ v.a. de loi uniforme	$d_0 \leftarrow \{0,..,2^{km}-1\}()$ v.a. de loi uniforme
$W \leftarrow r^v \bmod n$	$d_1 = (d_{11},...,d_{1m}) \leftarrow \{0,..,2^{km}-1\}()$ v.a. de loi fixée par $\tilde{B}$
$d_0 \leftarrow \{0,..,2^{km}-1\}()$ v.a. de loi fixée par $\tilde{B}$	$D \leftarrow \{0,..,n-1\}()$ v.a. de loi uniforme
$d_1 = (d_{11},...,d_{1m}) \leftarrow d(d_0, W)$: Fonction d fixée par $\tilde{B}$	$W \leftarrow D^v \times G_1^{d_{11}} \times .. \times G_m^{d_{1m}} \bmod n$
$D \leftarrow r \times Q_1^{d_{11}} \times .. \times Q_m^{d_{1m}} \bmod n$	**Jusqu'à** $d_1 = d(d_0, W)$
Renvoie (W, d_1, D)	**Renvoie** (W, d_1, D)
La vue $VUE\langle A_r(Q), \tilde{B}_{w_b}(G)\rangle$ est fonction des v.a. r et d_0 indépendantes.	La v.a. $M(G)$ est fonction des v.a. d_0, d_1 et D indépendantes Il est clair que : Si 2^{km} est polynomial en n alors l'algorithme définissant $M(G)$ est une MT
Remarque : dans les deux cas, la loi de la v.a. d_0 et la fonction d modélisent en fait la caractère « malhonnête » de $\tilde{B}$	

On montre alors que les deux lois de probabilité $VUE\langle A_r(Q), \tilde{B}_{w_d}(G)\rangle$ et de $M(G)$ sont égales. Plus précisément, on a :

$$Pr_{d_0,d_1,D}[P(M_{d_0,d_1,D}(G) = (a,b,c)] = \begin{cases} 0 \text{ si } c^v G_1^{b_1} \times .. \times G_m^{b_m} \neq a \bmod n, \\ \frac{1}{n} Pr_{d_0}[d(d_0,a) = b] \text{ sinon} \end{cases}$$

$$Pr_{d_0,d_1,D}[P(M_{d_0,d_1,D}(G) = (a,b,c)] = Pr_{r,d_0}[VUE\langle A_r(Q), B_{d_0}(G) = (a,b,c)\rangle]$$

Ainsi, si les clés GQ2 respectent les conditions du paragraphe 2.1 et si les paramètres k et m de GQ2 vérifient la condition « 2^{km} varie polynomialement en —n— » alors le protocole GQ2 possède la propriété « zero-knowledge ».

En adaptant la preuve au protocole GQ2 itéré à l'ordre t, il n'est pas difficile de corriger la condition sur les paramètres k,t et m et montrer qu'avec la condition « $t \times 2^{km}$ varie polynomialement en —n— » le protocole GQ2 itéré à l'ordre t possède encore la propriété « zero-knowledge ».

3.3 Conclusion sur la sécurité du protocole GQ2

En supposant que les clés GQ2 respectent les conditions énoncées dans le paragraphe 2.1, on distingue alors deux cas selon les paramètres k,t et m du protocole GQ2 :

- Cas du protocole GQ2 non itéré (t=1) :
  GQ2 possède trivialement la propriété de completeness.
  Sous l'hypothèse $log(|n|) = o(m.k)$, GQ2 possède la propriété de « soundness ».
  Sous l'hypothèse « 2^{km} varie polynomialement en $|n|$ », GQ2 possède la propriété de « zero-knowledge ».
  Toutefois, les deux conditions sur les paramètres k et m deviennent contradictoires. Le protocole ne peut respecter à la fois les deux conditions.

- Protocole GQ2 itéré (à l'ordre t) :
  GQ2 possède trivialement la propriété de completeness.
  Sous l'hypothèse $log(|n|) = o(t.m.k)$, GQ2 possède la propriété de « soundness ».
  Sous l'hypothèse $t \times 2^{km}$ varie polynomialement en $|n|$, GQ2 possède la propriété de « zero-knowledge ».
  En conséquence, si t et 2^{km} varient polynomialement en $|n|$, le protocole GQ2 itéré à l'ordre t respecte les trois propriétés requises et définit bien une preuve « zero-knowledge » de connaissance de la factorisation du module n.

4 Analyse des performances du protocole GQ2

4.1 Comparaison entre les différents protocoles d'authentification

Nous avons comparé les performances du protocole GQ2 aux principaux protocoles d'authentification existants :
- Protocole de Feige Fiat Shamir [2][1],
- Protocole de Schnorr [16],
- Protocole GQ1 [6],
- Protocole GPS (Mode 1) [5],[4],
- Protocole d'authentification RSA unilatéral et mutuel [9].

Les spécifications détaillées de ces différents protocoles sont extraites de la norme ISO/IEC 9798-5 [9]. Les critères de comparaison retenus ont été les suivants :
- CM : Complexité de communication entre le vérifieur et le prouveur évaluée en Kbit
- CPC : Complexité de calcul du prouveur évaluée en nombre de multiplications modulaires
- CPV : Complexité de calcul du vérifieur évaluée en nombre de multiplications modulaires

– CS : Stockage requis par le prouveur évalué en Kbit

Afin de se ramener à une mesure unique pour CPC et CPV, nous avons fait les hypothèses suivantes concernant l'évaluation des opérations arithmétiques en nombre de multiplications modulaires :

– Le calcul de $A^2 \bmod C$, dans l'hypothèse où $|A| \sim |C|$, est évalué à 0,75 fois une multiplication modulo C
– Le calcul de $A^B \bmod C$ est évalué à —B—-1 carrés modulo C et $HW(B)-1$ multiplications [4] modulo C.
– Le calcul de $A_1^{B_1} \times ... \times A_x^{B_x} \bmod C$ est évalué à $max(|B_1|, .., |B_x|) - 1$ carrés modulo C et $HW(B_1) + ... + HW(B_x) - 1$ multiplications modulo C par A_i.

Le tableau ci-dessous résume les performances comparées des différents protocoles d'authentification, pour chaque critère et en considérant le cas d'un module [5] de 1024 bits pour l'ensemble des protocoles. Les paramètres des différents protocoles sont ceux spécifiés dans l'annexe C.4.3 de la norme ISO/IEC 9897-5 [9].

	CS(K bits)	CPC	CPV	CM(K bits)
Fiat Shamir	5,00	11,00	11,00	8,00
GQ1	2,00	33,50	21,50	2,00
GQ2	5,50	7,75	3,75	2,00
Schnorr	2,31	200,00	208,00	1,17
GPS	1,16	192,00	200,00	1,27
RSA Unilateral Authentication	2,50	320,00	13,00	1,84
RSA Mutual Authentication	2,50	333,00	333,00	2,42

En dépit d'une étape supplémentaire dans le protocole (résultant du caractère zéro-knowledge), GQ2 réduit considérablement le temps de calculs par rapport à RSA. Comme le montre le tableau ci-dessus, pour un module de 1024 bits, le ratio RSA/GQ2 est de l'ordre de 40 pour le prouveur et de l'ordre de 3,5 pour le vérifieur.

Références

1. U.Feige, A.Fiat et A.Shamir, Zero knowledge proofs of identity, Crypto'89, *Lecture Notes in Computer Sciences 435*, pp. 526-544, 1990, Springer.
2. A.Fiat et A.Shamir, How to prove yourself : practical solution of identification and signature problems, Crypto'86, *Lecture Notes in Computer Sciences 263*, pp. 186-194, 1987, Springer.
3. S.Goldwasser, S.Micali et C.Rackoff, The Knowledge Complexity of Interactive Proof Systems, *SIAM journal of computing*, vol.18, pp. 186-208, 1989.

[4] $HW(B_1)$ représente le poids de Hamming de x
[5] ou, le nombre premier dans le cas de Schnorr

4. G.Poupard et J.Stern, Security Analysis of a practical " on the fly " Authentication and Signature generation, Eurocrypt'98, *Lecture Notes in Computer Sciences 1403*, pp. 422-436, 1998, Springer.
5. M.Girault, Self-Certified Public Keys, Eurocrypt'91, *Lecture Notes in Computer Sciences 36*, pp. 437-451, 2001, Springer.
6. L.Guillou et JJ.Quisquater, A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory, Eurocrypt'88, *Lecture Notes in Computer Sciences 330*, pp. 123-128, 1988, Springer.
7. L.Guillou et JJ.Quisquater, How to explain zero-knowledge protocols to yours children, Crypto'89, *Lecture Notes in Computer Sciences 435*, pp. 628-631, 1990, Springer.
8. L.Guillou, JJ.Quisquater et M.Ugon, Cryptographic authentication protocols for smarts cards, *Computer Network Magazine*, vol. 36, pp. 437-451, 2001.
9. , ISO/IEC-9798-5, Information technology - Security techniques . Entity authentication. Part 5 : Mechanisms using zero-knowledge techniques. Publication en cours.
10. ISO/IEC-14888-2, Information technology - Security techniques. Digital signature appendix. Part 2 : Integer factorization based mechanisms. Publication en cours.
11. A.Menezes, P. Van Oorschot et S.Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
12. H.Ong et C.P.Schnorr, Fast Signature generation with a Fiat-Shamir-like scheme, Eurocrypt'90, *Lecture Notes in Computer Sciences 473*, pp. 432-440, 1991, Springer.
13. D.Pointcheval, Les preuves de connaissance et leurs preuves de sécurité, thèse de doctorat, 1996.
14. G. Poupard, Authentification d'entité, de messages et de clés cryptographiques : théorie et pratique, thèse de doctorat, 2000.
15. R.Rivest, A.Shamir et L.Adleman, A Method for obtaining digital signatures and public-key cryptosystems, *Communications of the ACM*, vol. 21, pp. 120-126, 1978.
16. C.P.Schnorr, Efficent Identification and Signatures for Smarts Cards, Crypto'89, *Lecture Notes in Computer Sciences 435*, pp. 235-251, 1990, Springer.
17. C.P.Schnorr, Security of 2^t-Root Identification and Signatures, Crypto'97, *Lecture Notes in Computer Sciences 1294* pp. 540, 1997.
18. V.Shoup, On the Security of a practical identification scheme, Eurocrypt'96, *Lecture Notes in Computer Sciences 1070* pp. 340-353, 1996, Springer.
19. D.Pointcheval et J.Stern, Security Proofs for Signature Schemes, Eurocrypt'96, *Lecture Notes in Computer Sciences 1070*, pp. 387-398, 1996, Springer.
20. O.Goldreich, Zero-knowledge twenty years after its invention, *U.S.C. Computer Science Department*, Technical Report 2002/186, pp. 387-398, 2002.