Preuve à divulgation nulle de connaissance

Ludovic PATEY

31 décembre 2009

Résumé

Dans cet article, nous introduisons la notion de *preuve à divulgation nulle de connaissance* à des fins de vulgarisation tout en essayant de conserver un cadre formel.

Table des matières

1 Introduction

Les nouvelles technologies ont connu ces dernières années un succès sans cesse grandissant, au point de modifier la société en profondeur, la transformant en une *société de l'information et de la communication.*

De nouvelles problématiques jusqu'alors marginales se sont alors posées, notamment la sécurisation des communications par le biais de protocoles chiffrés. C'est l'objet d'étude d'une science ancienne, mais renouvelée dans les années 1970 : la Cryptologie ou science du chiffrement. Parmi les objets d'études de la cryptologie se trouve l'authentification, c'est à dire la vérification de l'identité d'une personne (entité) afin de lui permettre la plupart du temps d'accéder à des informations.

Le processus d'authentification le plus largement utilisé de nos jours consiste à partager une information secrète entre une entité A devant être authentifiée et une entité B vérificatrice, connue d'eux seulement. L'authentification consiste donc à transmettre l'information secrète de A vers B. L'identité est prouvé par l'aspect secret de l'information, rendant ainsi celle-ci critique : si une entité tierce C arrive à se procurer l'information secrète, elle pourra se faire passer pour A auprès de B et effectuer ainsi une *élévation de privilèges.*

Dans un environnement restreint, la confidentialité de l'information secrète peut être relativement bien conservée. En revanche, elle devient beaucoup plus problématique dans un grand réseau comme internet. De plus, rien ne garantit que l'entité vérificatrice n'est pas malveillante. En théorie, ce dernier cas ne devrait pas poser de problème car l'information secrète est sensé être unique en fonction de B, mais en réalité, beaucoup d'utilisateurs choisissent la même information secrète pour toutes les entités vérificatrices.

Ces différentes limites du système d'authentification "naturel" ont conduit à chercher un système permettant de prouver son identité, sans dévoiler d'autre information que celle de son identité. Ce système est un cas particulier de ce qu'on appelle *preuve à divulgation nulle de connaissance*.

Les systèmes de preuve à divulgation nulle de connaissance ont d'abord été introduites sous la forme de preuve d'appartenance à un langage, puis comme preuve de connaissance en absolu.

2 Système de preuve interactive

Afin de donner un cadre formel aux notions à manipuler, nous devons définir ce qu'est une entité. Intuitivement, les entités peuvent s'apparenter à des humains ou des ordinateurs dont les caractéristiques communes qui nous intéressent sont la présence d'une mémoire, la capacité d'effectuer des calculs et la présence de périphériques d'entrée et de sortie (les yeux et la bouche pour les humains).

Nous en venons naturellement à vouloir utiliser les *machines de Turing* comme modélisation de nos entités.

2.1 Machine de Turing

Une machine de Turing représente un modèle abstrait de tout système de calcul possédant une mémoire finie non bornée. Elle fut introduite par Turing afin de formaliser la notion d'algorithme. La célèbre thèse de *Church-Turing* affirme que tout ce qui est *calculable* peut l'être par une machine de Turing.

2.1.1 Définition

D'un point de vue formel, une machine de Turing peut être définie comme un 7-uplet $(\Sigma, Q, \sigma, \delta, \Delta, q_0, F)$ où

- Σ est un ensemble de symboles appelé *alphabet*, comprenant un symbole particulier noté $\#$.
- Q est un ensemble non vide fini d'états.
- $\sigma : Q \times \Sigma \to \Sigma$ est une fonction d'*impression*.
- $\delta : Q \times \Sigma \to Q$ est une fonction de *transition*.
- $\Delta : Q \times \Sigma \to \{-1, 1\}$ est une fonction de *déplacement*.

Une machine de Turing dispose en outre d'un ruban de mémoire de longueur finie à gauche et de longueur infinie à droite. Les accès à la mémoire se font à l'aide d'une tête de lecture pouvant se déplacer à droite et à gauche, lire le symbole d'une case et y écrire un nouveau symbole.

2.1.2 Principe de fonctionnement

À l'instant initial, le ruban de mémoire contient un nombre fini de symboles différents de $\#$. La tête de lecture est positionnée au niveau de la première case de gauche.

À chaque étape, la machine se trouve dans un état q et la tête de lecture est devant une case mémoire contenant le symbole a. La machine va alors

- écrire le symbole $\sigma(q, a)$ à l'emplacement mémoire courant
- déplace sa tête de lecture vers la gauche si $\Delta(q, a)$ vaut -1 et vers la droite sinon.

– passe de l'état q à l'état $\delta(q, a)$

La machine s'arrête lorsqu'elle se trouve dans un des états finaux ($q \in F$). Notons qu'une machine de Turing peut ne jamais s'arrêter.

2.2 Machine de Turing interactive

Dans le cas des systèmes de preuve interactive, il est nécessaire d'introduire une variante des machines de Turing : les *machines de Turing interactives*. Le principe de fonctionnement est le même, mais elles possèdent cinq rubans :

- Un ruban des données initiales, accessible en lecture seule.
- Un ruban de travail, accessible en lecture et écriture.
- Un ruban aléatoire ω_M suivant une distribution uniforme.
- Un ruban de communication IN, en lecture seule.
- Un ruban de communication OUT en écriture seule.

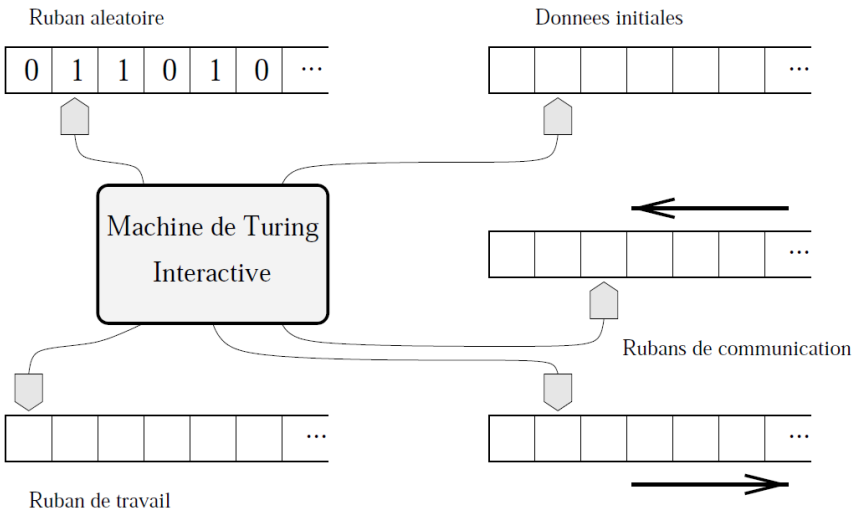

FIGURE 1 – Machine de Turing interactive

On remarquera que le ruban aléatoire contient un ensemble infini de symboles différents de #, ce qui n'est pas sensé être le cas avec les rubans d'une machine de Turing normale.

2.3 Système de preuve interactive

Nous avons besoin de la notion de *protocole interactif*.

Il s'agit de la donnée de deux machines de Turing interactives A et B, ayant en commun le ruban de données initiales et telles que le ruban de communication IN de la première soit le ruban OUT de la seconde et réciproquement. Les machines interagissent comme suit : A l'état initial, le ruban de données initiales comporte la donnée I.

Chaque machine est activée tour à tour, effectuant un calcul et envoyant un message sur son ruban de communication OUT. Dès lors qu'elle a envoyé son message, elle cesse d'être active et la seconde machine prend le relais. Le protocole se termine lorsque l'une des deux machines s'arrête avant d'avoir envoyé un message sur son ruban de communication de sortie. Une fois le protocole terminé, la machine B *accepte* ou *rejette* la donnée I.

Une restriction importante nécessaire pour que l'on puisse parler de protocole interactif est que la machine B agisse en un temps polynomial en fonction de la longueur de l'entrée I du ruban de données initiales. Pour les preuves d'appartenance à un langage, la machine A ne possède pas de restriction quand à sa complexité. Pour les preuves de connaissance, la machine A doit également s'exécuter en un temps polynomial. Nous ne détaillerons pas les preuves d'appartenance à un langage.

Les preuves de connaissance peuvent se formaliser par un prédicat $P(I, S)$ où I représente l'entrée, S la donnée secrète (*témoin*). Pour respecter les contraintes de preuve de connaissance, ce prédicat doit être calculable en un temps polynomial en fonction de $|I|$.

La machine A est le *prouveur* et possède un ruban supplémentaire en lecture seule contenant le secret S. La machine B est appelée *vérifieur*.

Nous pouvons maintenant introduire la notion fondamentale de *système de preuve interactive de connaissance*

Définition 1. Un **système de preuve interactive de connaissance** est un protocole interactif entre un prouveur A et un vérifieur B tel que :

- pour tout entier k et pour tout I suffisamment grand tel que $P(I, S)$ est satisfiable, A disposant d'un témoin S convainc B avec une probabilité supérieure à $1 - |I|^{-k}$, les probabilités étant calculées sur le contenu des rubans aléatoires ω_A et ω_B (on dit que la preuve est **consistante**).
$$\forall k \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall I \in \{I / \exists S\ P(I, S) \wedge |I| \geq n_0\}$$
$$\text{Pro}\left[A \text{ connaissant } S \text{ convainc } B\right] \geq 1 - \frac{1}{|I|^k}$$
- pour tout entier k, il existe une machine de Turing probabiliste agissant en un temps polynomial en fonction de $|I|$ notée M telle que, pour toute machine de Turing interactive $\tilde{A}$ et pour tout entier k', si $\tilde{A}$ convainc B avec une donnée initiale I suffisamment grande avec probabilité supérieure à $|I|^{-k}$, alors M produit S tel que $P(I, S)$ en interrogeant $\tilde{A}$ avec une probabilité supérieure à $1 - \frac{1}{[I]^k}$ (on dit que la preuve est **significative**).
$$\forall k \in \mathbb{N}\ \exists M \forall \tilde{A}\ \forall k' \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall I \in \{I / |I| \geq n_0\}$$
$$\text{Pro}\left[\tilde{A} \text{ convainc } B \text{ dela connaissance de } S \text{ tel que } P(I, S)\right] \geq \frac{1}{|I|^k}$$
$$\Rightarrow \text{Pro}\left[M \text{ produit } S \text{ tel que } P(I, S)\right] \geq 1 - \frac{1}{|I|^{k'}}$$

Le critère de consistance précise que si A connaît effectivement le secret, B ne risque pas de le rejeter, tandis que le critère de significativité garantit que B rejettera les preuves de machines ne connaissant pas le secret.

Si l'on retire le critère de consistance, il suffit de rejeter toute preuve pour pouvoir être un système de preuve interactive. De même, si l'on retire le critère de significativité, un système acceptant toute preuve répondrait aux conditions. On voit donc que les deux critères sont nécessaires.

Un système d'authentification basé sur un partage de secret tel qu'utilisé de nos jours répond aux deux critères, mais présente le problème de dévoiler le secret pour prouver son identité. Nous allons donc maintenant nous intéresser à des systèmes de preuve préservant le secret.

3 Système de preuve à divulgation nulle de connaissance

3.1 Indistinguabilité de variables aléatoires

Le principe de divulgation nulle de connaissance repose sur un principe d'*indistinguabilité de variable aléatoire* :

Nous nommerons *juge* l'entité modélisée par une machine de Turing dont le rôle est de distinguer deux familles de variables aléatoires.

Définition 2. Soient $U(m)$ et $V(m)$ deux familles de variables aléatoires paramétrées par les mots d'un langage $\mathcal{L}$.

- Si, pour tout $m \in \mathcal{L}$, on ne peut pas distinguer deux distributions, quelles que soient la taille des échantillons et la puissance de calcul du juge, on dira que les variables aléatoires sont **parfaitement indistinguables**.
  D'un point de vue formel :
  $$\forall m \in \mathcal{L}\ U(m) = V(m)$$

- Si, pour tout $m \in \mathcal{L}$, on ne peut pas distinguer deux distributions en ne voyant qu'un nombre polynomial d'éléments, on dira que les variables aléatoires sont **statistiquement indistinguables**.
  $$\sum_{\alpha \in \{0,1\}^*} |\mathrm{Pro}\,[U(m) = \alpha] - \mathrm{Pro}\,[V(m) = \alpha]| \leq \frac{1}{|m|^k}$$

- Si, pour tout $m \in \mathcal{L}$, on ne peut pas distinguer en temps polynomial (et par conséquent en ne voyant qu'un nombre polynomial d'éléments) deux distributions, on dira que les variables aléatoires sont **calculatoirement indistinguables**.

La notion d'indistinguabilité trouve son intérêt dans celle d'*approximabilité* :

Définition 3. Une famille de variables aléatoires $U(m)$ sur un langage $\mathcal{L}$ est dite **parfaitement** (resp. **statistiquement**, **calculatoirement**) **approximable** s'il existe une machine de Turing M non-déterministe, fonctionnant un un temps moyen polynomial, telle que $U(m)$ et $M(m)$ soient parfaitement (resp. statistiquement, calculatoirement) indistinguables.

Intuitivement, la notion d'approximabilité va permettre de remplacer une famille de variables aléatoires par une machine de Turing avec différent niveaux de qualité.

Comme son nom l'indique, le principe de *divulgation nulle de connaissance* garantit que le vérifieur n'aura, une fois le protocole terminé, acquis aucune autre connaissance que celle de la preuve. Nous allons donc définir une variable aléatoire représentant l'ensemble des connaissances que le vérifieur pourra acquérir au cours du protocole.

Le vérifieur accède tout d'abord à la donnée I sur le ruban de données initiales, et accède également à toutes les interactions de la preuve que nous pourrons considérer comme son historique H. Nous pouvons donc définir la variable aléatoire $\mathrm{Vue}_{A,\tilde{B}}$ représentant l'ensemble des informations auxquelles le vérifieur $\tilde{B}$ a accès au cours de l'exécution du protocole avec le prouveur A.

La dernière étape pour définir la notion de *divulgation nulle de connaissance* est de trouver un moyen de distinguer ce qui est une connaissance préalable de ce qui a été appris au cours du protocole. Pour cela, nous considérons que ce qui est calculable en un temps polynomial est une connaissance que possède déjà le vérifieur. Ainsi, si la vue du vérifieur n'est pas calculable en un temps polynomial, on peut légitimement considérer qu'il a acquis une connaissance venant du prouveur.

3.2 Définition

Nous pouvons donc définir la notion de *divulgation nulle de connaissance* comme suit :

Définition 4. Un système de preuve interactif (A, B) de connaissance du prédicat $P(I, S)$ est dit **parfaitement** (resp. **statistiquement**, **calculatoirement**) **à divulgation nulle de connaissance** si pour tout vérifieur $\tilde{B}$, la famille de variables aléatoires $\text{Vue}_{A,\tilde{B}}(I, H)$ est parfaitement (resp. statistiquement, calculatoirement) approximable sur $\mathcal{L} = \{(I, H) | I \in L \text{ et } |H| \leq |I|^k\}$ pour tout entier k fixé.

Il existe donc plusieurs degrés de divulgation de connaissance dans un protocole interactif. Voyons maintenant un exemple simple de preuve de connaissance. Il permettra notamment de mieux comprendre les raisons d'une approche probabiliste des preuves interactives.

4 Protocole de Fiat et Shamir

Le protocole qui suit a été proposé par Fiat et Shamir et permet de montrer la connaissance d'une racine carrée modulo n d'un entier I. Ce protocole a le bon goût d'être parfaitement à divulgation nulle de connaissance.

4.1 Description du protocole

Le protocole s'effectue entre un prouveur A et un vérifieur B. Etant donné un entier naturel n, le prouveur veut montrer qu'il connaît une racine carré S d'un entier I (donnée initiale) sans pour autant la divulguer.

Le protocole s'effectue itérativement l fois.

- Le prouveur choisit un entier naturel inversible de manière aléatoire suivant une distribution uniforme dans $\mathbb{B}_n$ et calcule son carré x modulo n.
- Le prouveur envoie x au vérifieur.
- Le vérifieur choisit un bit e de manière aléatoire suivant une distribution uniforme.
- Le vérifieur envoie e au prouveur.
- Le prouveur calcule $y = r \times S^e \mod n$ et l'envoie au vérifieur.
- Le vérifieur vérifie l'égalité $y^2 \equiv x \times I^e \mod n$.

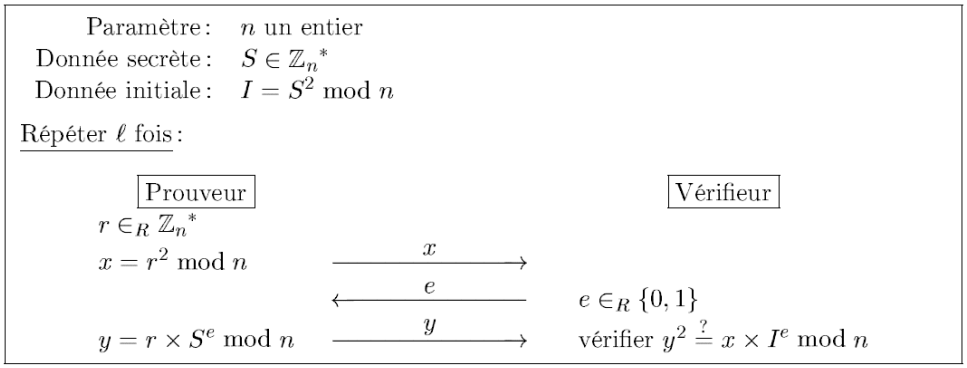

FIGURE 2 – Protocole de Fiat et Shamir

4.2 De la nécessité de l'utilisation de probabilités

Le protocole a recours à plusieurs reprises à des choix probabilistes, et le résultat lui-même est probabiliste : le vérifieur ne pourra jamais être totalement sûr de la connaissance d'une racine carré de I par le prouveur. En effet, si $e = 0$, le prouveur n'a pas besoin de connaître le secret pour donner une réponse valide. On pourrait en déduire que le vérifieur devrait toujours choisir $e = 1$,

mais alors il suffirait au prouveur de choisir $x = \frac{y^2}{I}$ pour obtenir une réponse valide sans pour autant connaître le secret. Une étape suivante dans le raisonnement serait alors de demander les

deux résultats $y_0 = r \mod n$ et $y_1 \equiv r \times S \mod n$, mais alors il suffirait au prouveur de calculer $y_0^- 1 y_1 \mod n$ pour obtenir S et la preuve cesserait d'être à divulgation nulle de connaissance.

S'il est impossible d'obtenir une certitude sur la connaissance de la racine d'un nombre, le vérifieur peut affiner sa certitude autant qu'il le veut en augmentant le nombre d'itérations. En effet, la probabilité que le prouveur connaisse le secret est de $\frac{1}{2^l}$.

4.3 De la preuve au système d'authentification

Une fois un protocole interactif de preuve à divulgation nulle de connaissance trouvé, le passage à un système d'authentification est immédiat. Reprenons donc le protocole de Fiat et Shamir. Il suffit que chaque utilisateur choisisse un nombre I modulo un grand nombre n, et fournisse le couple $(I^2 \mod n, n)$ lors de son inscription sur un site. Lors du processus d'authentification, il suffirait que l'utilisateur entre son secret dans son navigateur (supposé honnête), lequel interagirait avec le site distant suivant le protocole de Fiat et Shamir jusqu'à ce que ce dernier soit convaincu de la connaissance par l'utilisateur du secret, et donc de son identité.

5 Conclusion

Malgré la limite théorique des systèmes de preuve à divulgation nulle de connaissance à une incertitude due à l'usage de probabilités, ces systèmes de preuve sont dans les faits fiables et effectifs, directement applicables à des problématiques de la société de l'information.

Références

[1] A. Fiat and A.Shamir. *How To Prove Yourself : Practical Solutions to Identification and Signature Problems* (1987).

[2] Guillaume Poupard. *Authentification d'Entités, de Messages et de Clés Cryptographiques : Théorie et Pratique.* Thèse de Doctorat de l'École Polytechnique, 2000.

[3] Oded Goldreich. *Foundations of Cryptography : Basic Tools.* 2007