INFMDI356
Étude de l'article : On The Fly Signatures based on Factoring

Diala KHEIR kheir@enst.fr
Sébastien MARTINI martini@enst.fr
Samuel TIBERGHIEN tiberghien@enst.fr

2 février 2007

1 Introduction

L'article [3] étudié propose un nouveau schéma d'authentification et de signature. L'orginalité de ce schéma prouvé est d'être spécialement conçu pour minimiser les calculs nécessaires à son utilisation ; de sorte qu'il soit parfaitement utilisable sur des supports à capacité de calcul restreinte comme les smart cards.

Dans les sections suivantes nous rappelons brièvement l'état de l'art des schémas d'identification et de signature, en particulier ceux à apport de connaissance nul (zero-knowledge). Puis, nous présentons les schémas d'identification et de signature de l'article étudié, que nous désignerons par PS (Poupard–Stern). Finalement, nous introduisons l'idée des preuves que nous reproduirons lors de notre exposé.

2 Identification et Signature

Il existe plusieurs méthodes d'identification fortes par défi/réponses (à clé symétrique, ou à clé publique,...), le schéma de PS est un système de preuve interactif sans divulgation de connaissance, l'étude est concentrée sur ce type de méthode d'identification, ainsi que sur le schéma de signature associé.

Les principales caractéristiques de ce type de schéma sont :

- Les systèmes de preuves interactifs zero-knowledge sont basés sur des échanges entre deux parties : un prouveur et un vérifieur probabiliste en temps polynomial. Le prouveur cherche à convaincre le vérifieur de son identité, en apportant la preuve de connaissance d'un secret, et ce sans le divulguer. La sécurité apportée par ce type de protocole est calculatoire, il peut être itéré l fois, afin de renforcer sa complexité et de diminuer la probabilité d'être dupé par un acteur malhonnête.
- Un round (une itération complète du protocole) est généralement décomposé en trois échanges (Cf. section 2.1) : 1) l'engagement lors duquel le prouveur se lie à un élément aléatoire, 2) un challenge émis par le vérifieur pour lutter contre le rejeu, 3) la réponse du prouveur reposant sur l'engagement, le challenge, et le secret pourra être vérifiée par le vérifieur et ne divulguera aucune information sur le secret du prouveur.
- Les principaux schémas de signature reposent sur des problèmes réputés difficiles : la factorisation d'entier (ce schéma est basé sur ce problème), le problème équivalent d'extraction de racines carrée modulo un entier composé (Feige-Fiat-Shamir, Rabin), le logarithme discret (schéma de Schnorr), le problème RSA (schéma de Guillou-Quisquater, signature RSA).

À sécurité prouvée équivalente, la démocratisation de ces systèmes peut dépendre des efforts réalisés pour minimiser les complexités de calcul (surtout du côté du prouveur), et minimiser l'espace mémoire utilisé. Ce schéma a été élaboré dans cet objectif ; il cherche à réduire la taille

des clés, la taille de la signature, à privilégier (côté prouveur) les calculs offline aux calculs online et à réduire le nombre d'opérations online.

2.1 Schéma d'identification

Soient, P prouveur, V vérifieur, $N = PQ$ tels que $(P-1)/2 = p$ et $(Q-1)/2 = q$ avec P, Q, p et q premiers, $z \in (\mathbb{Z}/N\mathbb{Z})^*$ tel que $pq \mid \omega_N(z)$. Le schéma d'identification est le suivant :

1. $P \rightarrow V$: $z^r \ mod\ N$, tel que $r \in_R [0, A[$
2. $V \rightarrow P$: $e \in_R [0, B[$
3. $P \rightarrow V$: $r + (N - \varphi(N))e$

Finalement, V vérifie que $r + (N - \varphi(N))e < A$ (ce cas de figure peut se présenter car les opérations ne sont pas modulaires) et que $z^{r+(N-\varphi(N))e-Ne} = z^r \ mod\ N$.

L'étape 1 peut être pré-calculée, alors que les étapes 2 et 3 sont effectuées au vol. Le principal calcul au vol, celui de l'étape 3 ne fait intervenir que deux opérations non modulaires. Grâce à l'utilisation de coupons le calcul de 1 peut être haché et par conséquent sa longeur réduite, diminuant le nombre de bits transmis. Nous verrons lors de la preuve que le taux d'échec de l'exécution de ce protocole peut être considéré comme négligeable.

2.2 Schéma de signature

Afin de tranformer le schéma d'identification en schéma de signature, le challenge aléatoire e est remplacé par une fonction de hachage (qui peut être considérée comme un oracle aléatoire). Cette technique est courante et est employée entre autre dans [1].

1. Pré-calcul : $x = z^r \ mod\ N$, tel que $r \in_R [0, A[$
2. Calculs : $e = H(m, x)$, tel que $e \in_R [0, B[$ et $y = r + (N - \varphi(N))e$, si $y \geq A$ reprendre à l'étape 1
3. Sortie : (x, e, y)

Chacun peut s'assurer de la validité de la signature d'un message en vérifiant : $z^{y-Ne} = x \ mod\ N$, $e = H(m, x)$ et $y < A$.

2.3 Comparaison avec les autres schémas de signatures

Schémas de signatures	**Principales caractéristiques / Comparaisons avec PS**
Poupard–Stern	Favorise les pré-calculs, 1 mult. non modulaire online, possibilité d'utiliser les coupons, clé secrète de la taille de la moitié du modulo.
RSA	Equivalence non prouvée avec le problème de factorisation. Non prouvé NHZK. La signature est réalisée avec la clé privée, forcément grande. Complexité importante des calculs, stockage important dans le cas de l'utilisation du thèorême Chinois.
Rabin	Calculs offline impossibles. Complexité du calcul de racine carrée modulo N et exponentiation modulaire (RSA) comparables. Vérification de signature très rapide.
Feige-Fiat-Shamir	Dérivé d'un schéma d'identification ZK. Requiert en moyenne (seulement) $k/2$ mult. modulaires. L'importante (énorme) taille des clés publique et privée ($k \times \lvert N \rvert$), nécessite un important espace de stockage.
El Gamal / DSA	Pré-caluls possibles, seulement 2 multiplications modulaires online. Longeur de signature importante pour El Gamal, et vérification de signature coûteuse.
Schnorr	Variante de El Gamal. Pré-computations possibles, plus efficace que DSA (une seule multiplication modulaire online), courte taille de signature.
GPS	Variante de Schnorr, pré-calculs offline, 1 mult. non-modulaires online, clefs publique/privé.

3 Démonstration

Lors de notre présentation, nous reproduirons la preuve que c'est bien un protocole d'identification, et que c'est bien zero-knowledge et ce même si le vérifieur est malhonnête. L'approche suivie est celle de [1].

3.1 Preuve du protocole d'identification

(P, V) est un IPS (interactive proof system) pour un schéma d'identification s'il vérifie les deux propriétés suivantes :

- Completness : l'exécution entre un prouveur P honnête qui connaît le secret (la factorisation de la clé publique N) et un vérifieur V honnête sera toujours réussie avec une forte probabilité.
- Soundness : si $\tilde{\mathrm{P}}$ malhonnête est accepté par V avec une probabilité non négligeable, alors $\tilde{\mathrm{P}}$ est capable de factoriser N efficacement. Il sera montré que sous cette hypothèse la complexité de résolution de la factorisation reste calculatoirement impossible (sans la connaissance du secret).

3.2 Preuve du zero-knowledge

Le système (P, V) est Zero-Knowledge, s'il vérifie la propriété :

- Zero-knowledge : même si un prouveur répète le protocole d'identification de multiples fois, aucun vérifieur $\tilde{\mathrm{V}}$ même malhonnête, et à puissance de calcul infinie ne peut déduire une quelconque information sur le secret. Il faut montrer que pour tout $\tilde{\mathrm{V}}$ il existe une machine S capable de simuler en temps polynomial la communication entre P et $\tilde{\mathrm{V}}$ de sorte que sa sortie (la distribution de triplets (x_i, e_i, y_i)) soit statistiquement indistingable de l'originale. S ne connaît pas le secret, n'intéragit qu'avec $\tilde{\mathrm{V}}$, n'est pas détectable par $\tilde{\mathrm{V}}$, construit ses triplets (x_i, e_i, y_i) en partant de la "rèponse" pour obtenir la "question" x (en calculant $z^{y-Ne} = x \ mod \ N$).

4 Conclusion

Grâce à leur complexité de calcul avantageuse les algorithmes symétriques ont été historiquement privilégiés. Bien qu'ils soient efficaces, ils ont un défaut important dans le fait que chaque automate (vérifieur) doit stocker une clef maître.

Cependant, il existe une nouvelle classe de protocole d'identification et de signature d'inspiration asymétrique, qui a réduit ses besoins calculatoires au point de pouvoir être déployable sur des smart-cards traditionnelles sans crypto-processeur.

Le schéma étudié est de cette catégorie, il repose sur un problème difficile, ne révèle pas d'information sur son secret, et est efficace.

Il est toutefois nécessaire de préciser, que le schéma de ce type qui risque de s'imposer est le GPS [2], son schéma d'identification a été normalisé en 2004, et présente l'avantage d'offrir une paire de clefs publique/privé et d'avoir des tailles de clefs compatibles avec celles de RSA.

Références

[1] U. Fiege, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. In *STOC '87 : Proceedings of the nineteenth annual ACM conference on Theory of computing*, pages 210–217, New York, NY, USA, 1987. ACM Press.

[2] Marc Girault, Guillaume Poupard, and Jacques Stern. On the fly authentication and signature schemes based on groups of unknown order. *Journal of Cryptology*, Volume 19 :463,487, 2006.

[3] Guillaume Poupard and Jacques Stern. On the fly signatures based on factoring. In *CCS '99 : Proceedings of the 6th ACM conference on Computer and communications security*, pages 37–45, New York, NY, USA, 1999. ACM Press.