

# Signatures numériques et preuves à divulgation nulle, cryptanalyse, défense et outils algorithmiques\*

[Thèse de doctorat, École Nationale Supérieure des Télécommunications, Paris, Mai 1995.\*\*]

David Naccache

Gemplus Card International  
1 place de Navarre, F-95208, Sarcelles, France  
100142.3240@compuserve.com

**Résumé.** La *simplicité* d'un algorithme, mesurée par le *nombre* et la *nature* des opérations effectuées lors de son exécution, est un critère de qualité reconnu et apprécié. L'apparition récente d'appareils d'identification miniaturisés à faible capacité de calcul, a progressivement poussé les cryptologues à considérer des protocoles dont la sécurité n'est pas la seule contrainte. L'algorithme proposé en 1984 par **Ong, Schnorr** et **Shamir** est un exemple caractéristique illustrant le danger à trop simplifier. Heureusement, l'étrange efficacité de ce protocole et l'élégance de sa description ont suscité une grande excitation qui eut pour conséquence sa cryptanalyse par **Pollard** et **Schnorr**.

Dans ce document, nous présenterons deux approches de réparation, *prouvées équivalentes à la factorisation* et conçues *spécifiquement* afin de contrecarrer l'attaque de **Pollard** et **Schnorr**. Le coût de cette réparation reste très acceptable et peut s'exprimer différemment en terme de taille de clés, nombre de multiplications et quantité de bits transmis.

L'algorithme de **Fiat** et **Shamir** est certainement le protocole d'identification le mieux connu et le plus étudié. Ce procédé, qui présente l'intérêt d'être simple et rapide, doit son indéniable succès au faible nombre de multiplications nécessaires à sa réalisation (4% du RSA) et à la grande variété de *compromis mémoire-transmission* permettant au vérifieur d'atteindre tout niveau de sécurité désiré.

Plusieurs auteurs ont remis en question la sécurité du **Fiat-Shamir**, en montrant que celle-ci, assujettie à des précautions de réalisation *très strictes*, nécessite des tests additionnels de la part du vérifieur. Nous montrerons que l'inventaire de ces tests doit être étendu davantage. Cette nouvelle *faille de fonctionnement*, facile à réparer une fois l'attaque connue, revêt néanmoins une certaine importance pratique car des quantités

---

\* Digital Signatures and Zero-Knowledge Proofs, Cryptanalysis, Protection and Algorithmic Tools

\*\* PhD Thesis, École Nationale Supérieure des Télécommunications, Paris, May 1995.

massives de vérificateurs (mis sur le marché avant la publication de notre article) sont toujours en service aujourd'hui.

La signature aveugle est une technique permettant de protéger l'identité des utilisateurs d'un réseau tout en s'assurant de la validité de leurs signatures. Ce procédé, qui empêche l'établissement des liens (*création de dossiers*) entre données et individus, semble à première vue une solution parfaite, permettant de veiller à l'usage approprié des informations produites par un public souvent concerné par l'informatisation accrue de son environnement.

Malheureusement, nous mettons en évidence une faille qui permet de détourner ces protocoles de leur but et augmenter la virulence de certaines menaces criminelles. Un cas réel sera utilisé comme exemple.

La multiplication dans  $\mathbb{Z}_n$  étant la clé de voûte des algorithmes à clé révélée, la mise en œuvre optimisée de l'opération  $c = a \times b \bmod n$  conditionne naturellement la faisabilité de nombreuses applications. Le besoin d'un procédé de réduction rapide et adapté au contexte de la cryptographie (où  $n$  change beaucoup plus rarement que  $a$  et  $b$ ) a motivé la mise au point d'algorithmes dont les temps d'exécution atteignent 60% de la division classique. En règle générale, ces méthodes font appel à des constantes ( $K$ ) dépendant de  $n$  mais précalculées une fois pour toutes. L'idée de **Montgomery** consiste à décaler le nombre à réduire vers la droite après avoir annulé son mot le moins significatif par l'ajout d'un multiple approprié de  $n$ . La grande simplicité de ce principe explique l'exceptionnelle rapidité et les faibles ressources caractérisant cette fonction.

Dans ce document, nous montrerons qu'il est possible de se passer de  $K$  en modifiant les messages échangés lors d'un protocole ou en intégrant  $K$  directement dans les clés. Cette stratégie, qui s'applique à la quasi-totalité des protocoles, accélère les processeurs spécialisés et économise la mémoire nécessaire à la sauvegarde de  $K$ .

La méthode de **Barrett**, dont le principe consiste à approcher l'entier à réduire par un nombre quasi réduit, diffère peu de l'algorithme de Montgomery en terme de ressources et de complexité. Ce procédé utilise une constante  $L$  limitant d'avance la taille maximale des nombres à réduire. Alors que le choix  $L = 2N$  (où  $N$  représente la taille de  $n$ ) s'avère optimal pour l'exponentiation, on constate que les performances du procédé se dégradent au fur et à mesure que l'écart entre  $L$  et  $c$  se creuse. La variante améliorée que nous présenterons, a été mise au point afin de parer à ce défaut spécifique. Une extension de l'algorithme à la réduction des polynômes sera présentée également.

Malgré un pouvoir illimité, attribué au prouveur ( $P$ ) par le modèle de la divulgation nulle, l'existence de prouveurs quadratiques (et donc polynomiaux) soulève la question de la *complexité minimale* de  $P$  à laquelle nous tenterons d'apporter un élément de réponse en décrivant un prouveur de complexité *linéaire*.

La norme DSA du *US National Institute of Standards and Technology* est un procédé de signature destiné aux applications civiles et militaires non-confidentielles. La popularité prévisible de ce schéma suscite aujourd'hui

des efforts de recherche destinés à explorer son adaptation à diverses situations pratiques.

Nous montrerons que plusieurs facettes de cette norme peuvent encore être polies en exhibant des procédés permettant de signer, vérifier et compresser des *lots* de signatures à moindre effort, des protocoles où le signataire évite le calcul de  $1/q \bmod q$  ou  $r$  (*signatures jetables*) et une astuce permettant d'inclure  $q$  directement dans  $p$  (réduction de  $\cong 60\%$  de la taille des clés). Toutes ces variantes sont compatibles avec la norme et offrent un éventail de compromis de transmission, calcul et taille de clés.

Finalement, il sera question de la génération de permutations (plusieurs preuves à divulgation nulle "consomment" une permutation aléatoire par session) et d'une explication de la mauvaise adéquation entre les bases de Gröbner et la cryptographie à clé révélée.

Un survol rapide de plusieurs travaux en cours (nouveau procédé de chiffrement à clé révélée, variante du protocole de **Stern**, amélioration du *RSA pour paranoïdes*, des "signatures courtes", une famille d'identités combinatoires et un état de l'art en matière de coprocesseurs cryptographiques) clôturera notre exposé.

Trois de nos résultats sont cités dans l'ouvrage de **Schneier**, "*Applied Cryptography: Protocols, Algorithms and Source Code in C*".