Sécurité Exacte des Schémas de Signature Forward-Secure

Fabrice Ben Hamouda
Encadrants : Michel Abdalla et David Pointcheval
Équipe Crypto CASCADE — ENS

Contexte général En cryptographie, le sécurité d'un schéma se prouve généralement par réduction d'un problème supposé difficile (comme la factorisation d'entiers) à la sécurité du schéma. Il y a quelques années, Bellare et Rogoway ([3]) ont mis l'accent sur la sécurité exacte, c'est-à-dire l'importance de tenir compte de la *tightness* des réduction analysées pour choisir les paramètres d'un schéma (et donc pour connaître son efficacité). Un schéma est dit *tight* si la réduction prouve que, si un attaquant peut casser la sécurité du schéma en un certain temps t et avec une certaine probabilité, alors il est possible de casser le problème difficile associé avec approximativement le même temps et la même probabilité.

Résultats Nous nous sommes intéressés à la sécurité exacte des signatures *forward-secure*. Les schémas de signature *forward-secure* ont été inventés par Bellare et Miner ([2]). Ils consistent à découper la durée d'utilisation de la paire de clés de signature en T périodes. À chaque changement de période, la clé secrète est mise à jour, mais la clé publique reste inchangée. Si la clé secrète est compromise pendant la période i, seules les signatures de la période i et des périodes suivantes sont caduques. Toutes les signatures des périodes précédentes restent valides.

Tout d'abord, nous avons proposé une extension de la construction générique d'Abdalla et al. ([1]) au cas *forward-secure*. Cette nouvelle construction permet d'obtenir des signatures *forward-secure* plus *tight* que celles déjà existantess, mais pas complètement *tight*. Puis nous avons proposé une instanciation générique de cette construction en utilisant des problèmes liés à la factorisation. Et nous avons proposé diverses instanciations de cette seconde construction. L'une de ces instanciations améliore l'efficacité et la taille des précédentes signatures *forward-secure* connues. Cette première partie a donné lieu à une soumission à la conférence Asiacrypt 2012[1].

Ensuite, nous avons étudié s'il est possible d'obtenir des signatures *forward-secure* complètement *tight*. Nous avons montré un résultat d'impossibilité pour une large classe de signatures *forward-secure*. Ce résultat prouve que les réductions proposées pour les schémas de la première partie sont optimales. De plus, grâce à l'analyse précise des hypothèses de ce résultat, nous avons également pu proposer les deux premiers schémas de signature *forward-secure* avec une réduction complètement *tight*. Ces dernières constructions nous ont amené à introduire une nouvelle notion de sécurité pour les schémas de signature classique, intéressante en elle-même : la non-contrefaçon dans un contexte multi-utilisateur avec corruptions (SUF-MUC).

[1] M. Abdalla, P.-A. Fouque, V. Lyubashevsky, and M. Tibouchi. Tightly-secure signatures from lossy identification schemes. In *EUROCRYPT 2012*, LNCS. Springer, 2012.

[2] M. Bellare and S. K. Miner. A forward-secure digital signature scheme. In M. J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 431–448. Springer, Aug. 1999.

[3] M. Bellare and P. Rogaway. The exact security of digital signatures : How to sign with RSA and Rabin. In U. M. Maurer, editor, *EUROCRYPT'96*, volume 1070 of *LNCS*, pages 399–416. Springer, May 1996.

[1] Les auteurs de l'article soumis sont Michel Abdalla, Fabrice Ben Hamouda et David Pointcheval.