Implémentation boîte-blanche d'un algorithme de signature à clé publique : HFE

Pierre Galissant et Louis Goubin

Université Paris-Saclay, UVSQ, CNRS, Laboratoire de mathématiques de Versailles, 78000, Versailles, France
{pierre.galissant, louis.goubin}@uvsq.fr

Depuis son introduction en 2002 par Chow *et al*, la recherche autour de la cryptographie boîte-blanche a principalement été centrée sur les chiffrements par blocs standards tels que l'AES ou le DES. De nombreux candidats ont été proposés - [3, 4, 8, 2, 10, 7] par exemple - et tous ont été cassés, soit par des attaques structurelles, soit par des attaques génériques telles que la DCA, la LDA ou des attaques par fautes. Concernant les candidats asymétriques, très peu de solutions ont été proposées : le candidat [1] ne résiste pas aux attaques classiques et les travaux de [6] changent les algorithmes de signature et de vérification. Après près de deux décennies de recherche, il est raisonnable de dire qu'obtenir une implémentation boîte-blanche d'une primitive standard est un problème ouvert difficile. Le but de ce travail est de montrer les richesses de la cryptographie multivariée dans le contexte boîte blanche et de proposer une implémentation d'une instantiation de HFE [9] pour la signature et le chiffrement.

En revisitant la notion de multiple affine, nous proposons la première implémentation d'un algorithme de signature à clé publique dans le sens suivant :

- Notre algorithme de signature atteint un niveau de sécurité 80 bits contre toutes les attaques boîte-noire connues à clair-choisi.
- Notre implémentation est prouvée "*unbreakable*" [5] dans le modèle boîte-blanche conditionellement à la sécurité d'un problème *IP* (Isomorphism of Polynomials). Il n'est pas plus simple de retrouver la clé dans le modèle boîte blanche que dans le modèle classique.
- Nous revisitons la notion d'"*incompressibility*" [5] dans le modèle boîte-blanche en utilisant une définition plus précise, proposons une conjecture détaillée d'incompressibilité autour des problèmes IP : sous cette hypothèse, il est impossible d'obtenir une implémentation plus petite en moins de 2^{80} opérations.

Les paramètres de cette implémentation sont les suivants:

- La clé secrète est d'approximativement 2^{20} bits $\simeq$ 125 kB ;
- La clé publique est d'approximativement $2^{30}/2$ bits $\simeq$ 62.5 MB;
- L'implémentation boîte-blanche est d'approximativement 2^{41} bits $\simeq$ 256 GB.

References

1. Lucas Barthelemy. Toward an asymmetric white-box proposal. Cryptology ePrint Archive, Report 2020/893, 2020. https://eprint.iacr.org/2020/893.
2. Julien Bringer, Herve Chabanne, and Emmanuelle Dottax. White box cryptography: Another attempt. Cryptology ePrint Archive, Report 2006/468, 2006. http://eprint.iacr.org/2006/468.
3. Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. A white-box DES implementation for DRM applications. In Joan Feigenbaum, editor, *Security and Privacy in Digital Rights Management, ACM CCS-9 Workshop, DRM 2002, Washington, DC, USA, November 18, 2002, Revised Papers*, volume 2696 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 2002.
4. Stanley Chow, Philip A. Eisen, Harold Johnson, and Paul C. van Oorschot. White-box cryptography and an AES implementation. In Kaisa Nyberg and Howard M. Heys, editors, *SAC 2002*, volume 2595 of *LNCS*, pages 250–270, St. John's, Newfoundland, Canada, August 15–16, 2003. Springer, Heidelberg, Germany.
5. Cécile Delerablée, Tancrède Lepoint, Pascal Paillier, and Matthieu Rivain. White-box security notions for symmetric encryption schemes. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *SAC 2013*, volume 8282 of *LNCS*, pages 247–264, Burnaby, BC, Canada, August 14–16, 2014. Springer, Heidelberg, Germany.
6. Qi Feng, Debiao He, Huaqun Wang, Neeraj Kumar, and Kim-Kwang Raymond Choo. White-box implementation of shamir's identity-based signature scheme. *IEEE Syst. J.*, 14(2):1820–1829, 2020.
7. Mohamed Karroumi. Protecting white-box AES with dual ciphers. In Kyung Hyune Rhee and DaeHun Nyang, editors, *ICISC 10*, volume 6829 of *LNCS*, pages 278–291, Seoul, Korea, December 1–3, 2011. Springer, Heidelberg, Germany.
8. Hamilton E. Link and William D. Neumann. Clarifying obfuscation: Improving the security of white-box encoding. Cryptology ePrint Archive, Report 2004/025, 2004. http://eprint.iacr.org/2004/025.
9. Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.
10. Yaying Xiao and Xuejia Lai. A secure implementation of white-box AES. 2nd International Conference on Computer Science and its Applications (CSA 2009), 2009.