Analyse de la sécurité de primitives symétriques définies nativement sur de grands corps

Contexte. Le stage se déroulera au centre Inria de Paris (2 rue Simone Iff, Paris 12ème), au sein de l'équipe-projet SECRET (`https://www.paris.inria.fr/secret`). Il sera encadré par Anne Canteaut et Léo Perrin.

Contacts. `anne.canteaut@inria.fr`, `leo.perrin@inria.fr`

Description. Différents protocoles cryptographiques avancés, comme le calcul multi-partite (MPC), le chiffrement homomorphe (FHE) ou plus récemment les preuves à apport nul de connaissance Snark et Stark doivent être combinés avec des primitives (chiffrement ou fonction de hachage) ayant des propriétés d'implémentation très particulières. Les premiers travaux sur le sujet, notamment sur les primitives appropriées pour le MPC et le FHE, ont exprimé le besoin de minimiser le nombre de multiplications booléennes effectuées par la primitive. La profondeur multiplicative du circuit est également apparue comme un critère important. Ces critères ont donné lieu à la conception de diverses primitives, notamment le chiffrement par bloc Low-MC [3] et les chiffrements à flot Flip [13] et Kreyvium [8].

Plus récemment, l'apparition des preuves dites zk-Stark et zk-Snark [6] et le raffinement des critères précédents ont mis en avant la nécessité de minimiser le nombre de multiplication dans des corps finis $\mathbb{F}_q$ de plus grande taille, typiquement $\mathbb{F}_{2^n}$ avec n de l'ordre de 128 ou des corps premiers. Ces contraintes ont donc revivifié une idée ancienne dans la conception de primitives symétriques : celle de l'utilisation de transformations ayant une représentation simple sous forme univariée, comme un polynôme creux de $\mathbb{F}_q[X]$. De telles tentatives avaient en effet déjà eu lieu avec le chiffrement de Knudsen-Nyberg [14] puis avec Misty [12], tous deux cassés par des techniques de cryptanalyse différentielle d'ordre supérieur [11, 16, 10].

Le chiffrement MiMC [2] et ses variantes vont encore plus loin dans cette direction puisqu'il s'agit à l'origine d'une simple construction itérative, enchaînant un grand nombre de fois l'opération $x \mapsto x^3$ dans $\mathbb{F}_q$ et une addition de clef. Plus récemment encore, plusieurs auteurs ont proposé d'imiter la construction de l'AES en remplaçant l'étage de substitution par une seule fonctions $x \mapsto x^{-1}$ dans $\mathbb{F}_q$ [5]. La version la plus simple de ces chiffrements, Jarvis, a été attaquée par la résolution du système polynomial sous-jacent, au moyen du calcul d'une base de Gröbner [1]. Les propositions plus récentes comme Vision [4] demandent encore à être analysées.

L'objectif du stage est d'analyser la sécurité de ces familles de primitives et notamment de tenter d'exploiter la structure algébrique univariée simple de ces schémas pour monter une attaque. Beaucoup d'attaques actuelles (*cube attacks*, *division property*, *higher-order differential*...) se fondent en effet sur la simplicité de la structure multivariée (i.e. la forme algébrique normale) de la transformation mais aucune, à part la toute récente attaque algébrique sur Jarvis, n'exploite la simplicité de la représentation univariée. On peut ici noter que, dans le cas du filtrage d'un chiffrement à flot, l'emploi d'une fonction représentée par un polynôme univarié simple introduit des faiblesses importantes dans le chiffrement [15, 9].

Plusieurs pistes pourront être explorées pour analyser la sécurité de ces propositions récentes. Par exemple, dans le cas où $q = 2^n$ comme dans la version originale de MiMC, il pourrait être possible de monter des attaques exploitant la forme polynomiale de la fonction sur un sous-corps $\mathbb{F}_{2^m}$ où m divise n. C'est une direction rendue encore plus pertinente par de récents résultats sur MiMC [7] montrant l'absence systématiques de certains termes dans sa représentation univariée. Le cas des transformations définies sur un corps premier est, lui, entièrement nouveau en termes d'outils de cryptanalyse, et demande donc à être exploré en détail.

Références

[1] Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, and Markus Schofnegger. Algebraic cryptanalysis of STARK-friendly designs: Application to MARVELlous and MiMC. Cryptology ePrint Archive, Report 2019/419, 2019. `https://eprint.iacr.org/2019/419`.

[2] Martin R. Albrecht, Lorenzo Grassi, Christian Rechberger, Arnab Roy, and Tyge Tiessen. MiMC: Efficient encryption and cryptographic hashing with minimal multiplicative complexity. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *ASIACRYPT 2016, Part I*, volume 10031 of *LNCS*, pages 191–219. Springer, Heidelberg, December 2016.

[3] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 430–454. Springer, Heidelberg, April 2015.

[4] Abdelrahaman Aly, Tomer Ashur, Eli Ben-Sasson, Siemen Dhooghe, and Alan Szepieniec. Design of symmetric-key primitives for advanced cryptographic protocols. Cryptology ePrint Archive, Report 2019/426, 2019. `https://eprint.iacr.org/2019/426`.

[5] Tomer Ashur and Siemen Dhooghe. MARVELlous: a STARK-friendly family of cryptographic primitives. Cryptology ePrint Archive, Report 2018/1098, 2018. `https://eprint.iacr.org/2018/1098`.

[6] Eli Ben-Sasson, Alessandro Chiesa, Daniel Genkin, Eran Tromer, and Madars Virza. SNARKs for C: Verifying program executions succinctly and in zero knowledge. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Part II*, volume 8043 of *LNCS*, pages 90–108. Springer, Heidelberg, August 2013.

[7] Clémence Bouvier, Anne Canteaut, and Léo Perrin. On the algebraic degree of iterated power functions. Cryptology ePrint Archive, Report 2022/366, 2022. `https://eprint.iacr.org/2022/366`.

[8] Anne Canteaut, Sergiu Carpov, Caroline Fontaine, Tancrède Lepoint, María Naya-Plasencia, Pascal Paillier, and Renaud Sirdey. Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression. *Journal of Cryptology*, 31(3):885–916, July 2018.

[9] Anne Canteaut and Yann Rotella. Attacks against filter generators exploiting monomial mappings. In Thomas Peyrin, editor, *FSE 2016*, volume 9783 of *LNCS*, pages 78–98. Springer, Heidelberg, March 2016.

[10] Orr Dunkelman and Nathan Keller. An improved impossible differential attack on MISTY1. In Josef Pieprzyk, editor, *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 441–454. Springer, Heidelberg, December 2008.

[11] Thomas Jakobsen and Lars R. Knudsen. The interpolation attack on block ciphers. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 28–40. Springer, Heidelberg, January 1997.

[12] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 54–68. Springer, Heidelberg, January 1997.

[13] Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 311–343. Springer, Heidelberg, May 2016.

[14] Kaisa Nyberg and Lars R. Knudsen. Provable security against a differential attack. *Journal of Cryptology*, 8(1):27–37, December 1995.

[15] Sondre Rønjom and Carlos Cid. Nonlinear equivalence of stream ciphers. In Seokhie Hong and Tetsu Iwata, editors, *FSE 2010*, volume 6147 of *LNCS*, pages 40–54. Springer, Heidelberg, February 2010.

[16] Yosuke Todo. Integral cryptanalysis on full MISTY1. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 413–432. Springer, Heidelberg, August 2015.