Borner le poids des chemins différentiels de la fonction de hachage Troïka

Christina Boura [*1], Yann Rotella [†1] et Margot Funk [‡1]

[1]Université Paris-Saclay, UVSQ, Laboratoire de mathématiques de Versailles

Assurer la non-existence de chemins différentiels de probabilité élevée – ou de manière équivalente de poids faible – est un des attendus d'une analyse de sécurité d'une primitive cryptographique symétrique. Lorsque la couche linéaire d'un algorithme de type substitution-permutation (SPN) suit une logique bit par bit, il est difficile, même sur peu de tours, de calculer une borne inférieure sur le poids de ses chemins différentiels. C'est le cas de la fonction de hachage Troïka qui a pour particularité d'opérer sur des vecteurs d'éléments du corps $\mathbb{F}_3$ [1]. Il existe très peu de résultats génériques sur l'utilisation du corps $\mathbb{F}_3$ en cryptographie. Les concepteurs de Troïka, pour étudier sa résistance contre les attaques différentielles, ont modélisé la propagation des différences à l'aide d'un modèle MILP (*Mixed Integer Linear Programming*) à optimiser. Cependant, cette approche n'est pas la plus adaptée pour étudier des algorithmes construits sur le principe du *weak alignment*. En 2017, Silvia Mella, Joan Daemen et Gilles Van Assche ont proposé une autre méthode, basée sur des parcours d'arbres, pour borner sur quelques tours le poids des chemins différentiels de tels algorithmes [2]. Nous avons adapté leur méthode au cas du corps $\mathbb{F}_3$ afin d'étudier les chemins différentiels de Troïka. Nous nous sommes concentrés sur des chemins différentiels portant sur 6 itérations de la fonction de tour de Troïka et avons montré qu'il n'en existe pas ayant un poids inférieur à 66.

Puisqu'un chemin différentiel de 6 tours de poids W contient toujours un chemin différentiel de 3 tours de poids $\lfloor W/2 \rfloor$, nous procédons en deux temps. Tout d'abord, fixant $W = 66$, nous cherchons de manière exhaustive tous les chemins différentiels de 3 tours de poids inférieur à $\lfloor W/2 \rfloor$. Nous étendons ensuite tous les chemins collectés en des chemins de 6 tours. Si aucun des chemins ainsi formés n'a un poids inférieur à W, alors les poids des chemins différentiels de 6 tours sont bornés inférieurement par W.

Il est impossible de parcourir tous les chemins de 3 tours de manière exhaustive. Suivant la méthodologie décrite dans [2], nous avons défini plusieurs arbres dont les sommets représentent des chemins différentiels et dont nous voulons extraire un sous-ensemble de chemins différentiels ayant un faible poids. L'objectif est de définir les arbres en question de sorte à pouvoir les élaguer efficacement et ne parcourir que leur portion qui nous intéresse. Pour cela, il faut prendre en compte les particularités de la couche linéaire de la fonction de tour de Troïka. Celle-ci présente beaucoup de similitudes avec celle de Keccak et nous pouvons, comme dans [2] classifier les états selon leur appartenance ou non au noyau (*Column Parity Kernel*). Les états appartenant au noyau sont les états pour lesquels l'application linéaire de la fonction de tour correspond simplement à une permutation des coordonnées de l'état. Cette distinction tire son intérêt du fait que les états dans le noyau sont davantage susceptibles d'avoir un faible poids. De fait, nous avons conçu des algorithmes spécifiquement dédiés à leur recherche.

Références

[1] Stefan Kölbl, Elmar Tischhauser, Patrick Derbez, and Andrey Bogdanov. Troika : a ternary cryptographic hash function. *Designs, Codes and Cryptography*, 88 :91–117, January 2019.

[2] Silvia Mella, Joan Daemen, and Gilles Van Assche. New techniques for trail bounds and application to differential trails in keccak. *IACR Trans. Symmetric Cryptol.*, 2017(1) :329–357, 2017.

[*]christina.boura@uvsq.fr
[†]yann.rotella@uvsq.fr
[‡]margot.funk2@uvsq.fr