Attaques par invariant : comment s'en protéger?

Christof Beierle, Anne Canteaut, Gregor Leander, Yann Rotella

Attaques par invariant : comment s'en protéger?

Christof Beierle, Anne Canteaut, Gregor Leander et Yann Rotella

Horst Görtz Institute for IT Security, Ruhr-Universität Bochum, Germany
Inria de Paris, équipe-projet SECRET, France
christof.beierle@rub.de, anne.canteaut@inria.fr,
gregor.leander@rub.de, yann.rotella@inria.fr

Pour des raisons évidentes d'implémentation, beaucoup de chiffrements par bloc à bas coût ont un cadencement de clef très simple, où chaque clef de tour correspond exactement à la clef-maître à l'ajout près d'une constante de tour. Pour des réseaux de substitution-permutation (SPN) avec un tel cadencement de clef, un nouveau type d'attaques est apparu [1], appelé attaques par sous-espaces invariants. Depuis 2011, ces attaques et leur généralisation [2] ont ébranlé la sécurité d'autres SPN tels que PRINTcipher, SCREAM, iSCREAM, Midori.
Pour un chiffrement par bloc E_K, nous nous intéressons aux sous-ensembles non-triviaux tels que

$$E_K(\mathcal{S}) = \mathcal{S} \text{ ou } E_K(\mathcal{S}) = \mathbb{F}_2^n/\mathcal{S}.$$

Dans le cas des SPN, nous souhaitons prouver la non-existence de tels ensembles, qui soient invariants à la fois par l'étage linéaire L et l'étage de substitution S.

Observation. Soit $W_L(c_1, ..., c_t)$ le plus petit sous-espace de $\mathbb{F}_2^n$ invariant par L qui contient $c_1, ..., c_t$, où $c_1, ..., c_t$ sont les différences entre les constantes de tour. Nous pouvons garantir une résistance aux attaques par invariant, indépendamment du choix de la couche de substitution si $W_L(c_1, ..., c_t) = \mathbb{F}_2^n$. Lorsque $W_L(c_1, ..., c_t) \subsetneq \mathbb{F}_2^n$, nous pouvons parfois assurer la sécurité au regard des attaques par invariant mais en considérant aussi la couche de substitution. Nous montrons ainsi que LED, Skinny-64, Prince, Mantis$_7$ résistent à ces attaques.

Choix optimal des constantes de tour. Une question naturelle est donc de déterminer, pour une couche linéaire L donnée, le nombre minimimal de tours nécessaires pour que $W_L(c_1, ..., c_t) = \mathbb{F}_2^n$. Il s'avère que la dimension maximale possible de $W_L(c_1, ..., c_t)$ est liée aux facteurs invariants de L.

Théorème 1. *Soit $Q_1, ..., Q_r$ les facteurs invariants de la partie linéaire L et $t \leq r$. Alors*

$$\max_{c_1,...,c_t \in \mathbb{F}_2^n} \dim W_L(c_1, ..., c_t) = \sum_{i=1}^{t} \deg Q_i$$

De plus, nous exprimons la probabilité que $W_L(c_1, ..., c_t)$ couvre tout l'espace quand les constantes de tour sont prises aléatoirement.
Finalement, nous expliquons comment choisir les constantes de tour d'un SPN en fonction de la couche linéaire afin d'assurer la résistance aux attaques par invariant, indépendamment du choix de la boîte S.

Références

[1] Gregor Leander, Mohamed Ahmed Abdelraheem, Hoda AlKhzaimi, and Erik Zenner. A cryptanalysis of PRINTcipher : The invariant subspace attack. In Phillip Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 206–221. Springer, Heidelberg, August 2011.

[2] Yosuke Todo, Gregor Leander, and Yu Sasaki. Nonlinear Invariant Attack - Practical Attack on Full SCREAM, iSCREAM, and Midori64. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 3–33, 2016.