On the Boomerang Uniformity of some Permutation Polynomials

Irene Villa
joint work with
Marco Calderini

University of Bergen
Irene.Villa@uib.no

Abstract

The boomerang attack, introduced by Wagner in 1999 [1], is a cryptanalysis technique against block ciphers based on differential cryptanalysis. In particular it takes into consideration two differentials, one for the upper part of the cipher and one for the lower part, and it exploits the dependency of these two differentials. In a recent work, Boura and Canteaut [2] studied the properties of Sboxes related to the boomerang attack. Other results were presented by Li et al. in [3].

Given a permutation $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the *Boomerang Uniformity* of F, β_F, is defined as follow

$$\beta_F = \max_{a,b \in \mathbb{F}_{2^n}^\star} |\{x \in \mathbb{F}_{2^n} : F^{-1}(F(x)+a) + F^{-1}(F(x+b)+a) = b\}|.$$

Equivalently β_F can be defined as the maximum number of pair $(x, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ that solves the following system of equations

$$\begin{cases} F(x+a) + F(y+a) = b \\ F(x) + F(y) = b, \end{cases}$$

with a and b ranging over $\mathbb{F}_{2^n}^\star$.

In this work we studied the boomerang uniformity of some differentially 4-uniform permutation polynomials.

- The Bracken-Leander function, defined over $\mathbb{F}_{2^{4k}}$ for k odd,

$$F(x) = x^{2^{2k}+2^k+1}.$$

- A class of permutations constructed from the inverse function, of the form

$$F(x) = \begin{cases} 1 & x = c \\ c^{-1} & x = 1 \\ x^{-1} & x \neq 1, c. \end{cases}$$

When n is even and $Tr(c) = Tr(\frac{1}{c}) = 1$ then F is a differentially 4-uniform permutation.

References

[1] D. Wagner. The boomerang attack. In Lars R. Knudsen, editor, *FSE'99*, volume 1636 of *LCNS*, pages 156-170. Springer, Heidelberg, March 1999.

[2] C. Boura, and A. Canteaut. On the boomerang uniformity of cryptographic Sboxes. IACR Trans. Symmetric Cryptol., 3, pages 290-310. 2018.

[3] K. Li, L. Qu, B. Sun, and C. Li. New Results about the Boomerang Uniformity of Permutation Polynomials. Preprint: arXiv:1901.10999