A new tool for differential analysis of functions in characteristic 2

Alev Topuzoğlu
Sabancı University, Turkey

30th Applications of Computer Algebra - ACA 2025

Recent advances in differential cryptanalysis necessitate acquiring increasingly more knowledge of differential properties of S-boxes. Here we present a new tool enabling a detailed differential analysis of functions $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Given a function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, the behavior of D_aG, the *first derivative of G in the direction* $a \in \mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$, where $D_aG(x) = G(x) + G(x+a)$, plays a major role in assessing the resistance of G against the differential attack and its refinements.

A natural way of studying the differential properties of G, as is recently exhibited in [1], is to consider the so-called *difference square* corresponding to G, which is defined as follows. By fixing an ordering of the elements of $\mathbb{F}_{2^n}$, therefore putting $\mathbb{F}_{2^n} = \{x_1 = 0, x_2 = 1, \ldots, x_{2^n}\}$, it is the $2^n - 1$ by 2^n array, where the a-th row $\Delta_a(G)$, $a \in \{x_2, \ldots, x_{2^n}\}$, consists of the derivatives $D_aG(x_1), \ldots, D_aG(x_{2^n})$. This view point leads to some unexpected new results, for instance, finding the partial quadruple system associated to G, or the number of vanishing flats with respect to G for some particular G.

It is shown in [1] that some interesting patterns in difference squares emerge, which motivate the introduction of a new concept, the *APN-defect* of G, which can be thought of as measuring the distance of G to the set of almost perfect nonlinear (APN) functions.

The aim of this talk is to explain how this measure can be used to identify *quasi-APN* functions, which behave favorably in terms of their differential properties, how to calculate it for some functions of interest, and why a careful study of difference squares may lead to the construction of new APN functions.

This is joint work with Nurdagül Anbar and Tekgül Kalaycı.

References

[1] Nurdagül Anbar, Tekgül Kalaycı, Alev Topuzoğlu. Analysis of functions of low differential uniformity in characteristic 2: A new approach (I). *Submitted*, 2024.