Musings on c-differential and c-boomerang uniformity

Pante Stănică

Department of Applied Mathematics,
Naval Postgraduate School, Monterey, CA 93943–5216

Since the security of S-boxes depends on its resistance against differential and boomerang attacks, to name just a few, a few concepts have been introduced to measure the resistance against these.

We let $\mathbb{F}_q$ be the finite field with $q = p^n$ elements, p prime, $n \geq 1$ integer. For any (n, n)-function $F : \mathbb{F}_q \to \mathbb{F}_q$, and $a, b \in \mathbb{F}_q$, we let $\Delta_F(a, b) = \#\{x \in \mathbb{F}_q \mid F(x + a) - F(x) = b\}$ be the (a, b)-th entry of the Difference Distribution Table (DDT) of F. The value $\delta_F = \max\{\Delta_F(a, b) \mid a, b \in \mathbb{F}_q, a \neq 0\}$ is the *differential uniformity* of F. When $\delta_F = 1$, we call F to be *perfect nonlinear* (PN) function and if $\delta_F = 2$, F is called *almost perfect nonlinear* (APN) function. The S-boxes with low differential uniformity provide the optimal resistance against the differential attack.

In 1999, Wagner proposed a new attack on block ciphers, namely, the boomerang attack. The theoretical underpinning of this attack was developed by Cid, Huang, Peyrin, Sasaki and Song at Eurocrypt '18, and continued by Boura and Canteaut in '18, with the introduction of the Boomerang Connectivity Table and boomerang uniformity. For a permutation $F : \mathbb{F}_q \to \mathbb{F}_q$, $a, b \in \mathbb{F}_q$, we let $\mathcal{B}_F(a, b) = \#\{x \in \mathbb{F}_q \mid F^{-1}(F(x + a) + b) - F^{-1}(F(x) + b) = a\}$ be the (a, b)-th entry of the Boomerang Connectivity Table (BCT) and $\beta_F = \max\{\mathcal{B}_F(a, b) \mid a, b \in \mathbb{F}_q^*\}$ be the boomerang uniformity of F. Later, Li, Qu, Sun, Li in '19 gave an equivalent definition to compute BCT, which does not involve the compositional inverse of the function F, allowing one to extend this notion to non-permutations.

The concept of DDT and differential uniformity was extended in '20 by this author, along with Ellingsen, Felke, Riera, Tkachenko to c-differentials (see also the work of Bartoli and Timpanella, for the particular quasi-planar case $c = -1$): the (*multiplicative*) *c-derivative* of F with respect to $a \in \mathbb{F}_q$ is the function ${}_cD_aF(x) = F(x+a) - cF(x)$, for all $x \in \mathbb{F}_q$. The entries of the c-Difference Distribution Table (c-DDT) are ${}_c\Delta_F(a, b) = \#\{x \in \mathbb{F}_q : F(x + a) - cF(x) = b\}$, and $\delta_{F,c} = \max\{{}_c\Delta_F(a, b) \,|\, a, b \in \mathbb{F}_q, \text{ and } a \neq 0 \text{ if } c = 1\}$, is the *$c$-differential uniformity* (cDU) of F.

The concept of BCT and boomerang uniformity was generalized by this author in '20-'21. If one restricts to permutations, the notion simply looks at the probability of the propagations $cF(x)+b$ and $c^{-1}F(x+a)+b$, being the same constant a, as the propagation of the input, under the inverse S-box. Precisely, for $F : \mathbb{F}_q \to \mathbb{F}_q$, $c \in \mathbb{F}_q^*$, the entries of the c-BCT at $(a, b) \in \mathbb{F}_q \times \mathbb{F}_q$, denoted by ${}_c\mathcal{B}_F(a, b)$ is the number of solutions in $\mathbb{F}_q \times \mathbb{F}_q$ of the (c-boomerang) system

$$\begin{cases} F(x) - cF(y) = b \\ F(x + a) - c^{-1}F(y + a) = b. \end{cases} \tag{1}$$

The c-boomerang uniformity of F is defined as $\beta_{F,c} = \max\{{}_c\mathcal{B}_F(a, b) \mid a, b \in \mathbb{F}_q^*\}$.

In this survey talk, we go through some very recent results and ideas on this new type of differential and boomerang uniformity, some of which we have been involved in developing.