Linear and differential properties of S-boxes with respect to modular addition

Matúš Jókay, Peter Špaček, and Pavol Zajac*

Slovak University of Technology in Bratislava, Ilkovicova 3, 812 19 Bratislava,Slovakia

There is a lot of research ongoing on linear and differential properties of S-boxes. Typically, S-boxes are studied as vectorial Boolean functions with respect to an algebra over finite field $\mathbb{F}_2$, but can be generalized to arbitrary grupoids [2]. Recent study [1] has pointed out the fact that differential attacks can be conducted with respect to alternative operations in practice.

In many block ciphers, especially of post-Soviet Union origin (e.g. Russian GOST, or Ukrainian Kalyna), key addition is performed by modular addition, i.e. addition in ring $\mathbb{Z}_{2^n}$ for some n. While not entirely straightforward, it is possible to adapt differential cryptanalysis to differences in $\mathbb{Z}_{2^n}$. Moreover, we can try to replace non-linear S-boxes in these ciphers with some affine functions over $\mathbb{Z}_{2^n}$, and adopt techniques of linear cryptanalysis to attack the cipher.

In our contribution we do not dwell on the above mentioned cryptanalytic techniques, but are interested in properties of S-boxes with respect to differences and affine approximations over $\mathbb{Z}_{2^n}$. We define two associated quantities:

- S-box differential with respect to $(dx, dy) \in \mathbb{Z}_{2^n} \times \mathbb{Z}_{2^n}$:

$$D_{(dx,dy)} = \left|\{x; S(x + dx) - S(x) = dy\}\right|.$$

- S-box affine approximation with respect to $(q, c) \in \mathbb{Z}^*_{2^n} \times \mathbb{Z}_{2^n}$:

$$L_{(q,c)} = \left|\{x; q \cdot S(x) - x = c\}\right|.$$

With these quantities we can associate corresponding spectra, and maxima over non-trivial parameters (dx, dy), or (q, c), respectively. To resist cryptanalysis, corresponding S-box should have a flat spectrum.

Similar to standard S-box characterization, we can define affine equivalence with respect to operations over $\mathbb{Z}_{2^n}$. Two S-boxes S_1, S_2 are affine equivalent, if there exist $a_1, a_2 \in \mathbb{Z}^*_{2^n}$, and $b_1, b_2 \in \mathbb{Z}_{2^n}$, such that

$$\forall x : S_2(x) = a_1 \cdot S_1(a_2 \cdot x + b_2) + b_1.$$

Number of affine classes with respect to operations over $\mathbb{Z}_{2^n}$ is much higher than if we use the standard affine equivalence of Boolean functions. For $n = 3$, there are 58 classes (obtained experimentally). For $n = 4$ there are at least 2^{30} classes (trivial lower bound).

In our contribution we examine the properties of small bijective S-boxes (with $n = 3$, $n = 4$) and analyse their resistance against differential and linear attacks with respect to modular addition.

References

[1] Civino R, Blondeau C, Sala M. *Differential attacks: using alternative operations.* Designs, Codes and Cryptography. 2019; 87(2–3):225–47.

[2] Grošek O, Satko L, Nemoga K. *Generalized perfectly nonlinear functions.* Tatra Mountains Math. Publ. 2000; 20: 121–131.

*This research was supported by grant VEGA 1/0159/17.