Commutative Cryptanalysis as a Generalization of Differential Cryptanalysis

Christof Beierle

Ruhr University Bochum, Bochum, Germany
christof.beierle@rub.de

Let $E = (E_k)_{k \in \kappa}$ be a family of permutations over a finite abelian group $(G, +)$. In the context of block ciphers, we usually take $G = \mathbb{F}_p^n$. In the framework of *commutative cryptanalysis* (originating from Wagner's commutative diagram cryptanalysis [D. Wagner. Towards a unifying view of block cipher cryptanalysis. Fast Software Encryption: FSE 2004. Springer, 2004]), an adversary tries to exploit the existence of permutations P_1, P_2 over G such that the cryptographic primitive E fulfills $E_k \circ P_1(x) = P_2 \circ E_k(x)$ for many inputs $x \in G$ and for a significant portion of weak keys k. This framework naturally generalizes differential cryptanalysis. Indeed, the case of differentials is obtained by choosing P_1 and P_2 as translations $x \mapsto x + \alpha$ and $x \mapsto x + \beta$, respectively. In case that G is a field, also c-differentials are covered by this framework. In the recent work [J. Baudrin, P. Felke, G. Leander, P. Neumann, L. Perrin, L. Stennes. Commutative Cryptanalysis Made Practical. IACR Transactions on Symmetric Cryptology, 2023(4), 299–329, 2023] the authors focused on the case of $G = \mathbb{F}_2^n$ and P_1, P_2 being affine permutations and they generalized the notion of differential uniformity to the notion of *affine uniformity*, by not only taking into account translations, but arbitrary affine permutations.

In this talk, I will explain the framework of commutative cryptanalysis in more detail and discuss the applicability in the context of cryptographic attacks. In particular, I will focus on the relations between the general commutative framework, the special case of affine permutations P_1, P_2, and the special case of differential cryptanalysis. By doing so, I outline what are the most promising choices for (P_1, P_2) when it comes to conduct a cryptographic attack.

This talk is based on joint ongoing work with Jules Baudrin, Patrick Felke, Gregor Leander, Patrick Neumann, Léo Perrin, and Lukas Stennes.