Differential-Linear Attacks from New Distinguishers: The case of SERPENT and PRESENT

Thierno Mamoudou Sabaly*[1]

[1]Université de Lorraine, CNRS, Inria, LORIA, Nancy, France – Université de Lorraine, CNRS, Inria, LORIA – France

Résumé

Differential-linear distinguishers were introduced by Langford and Hellman in 1994. They consist of combining a differential distinguisher followed by a linear distinguisher, and then studying the bias obtained from pairs of plaintexts with a fixed difference and linear approximations of the corresponding ciphertexts to construct a differential-linear distinguisher. The original method was improved by Bar-On et al. in 2019 with the introduction of the DLCT (Differential Linear Connectivity Table). More recently, in 2024, Hadipour et al. further enhanced this approach by introducing multiple intermediate tables-similar to the case of boomerang distinguishers-to better tune the computation of the middle part of the distinguisher. Additionally, they proposed an automated tool to find differential-linear distinguishers, which led to improvements and the identification of new distinguishers for several schemes, including SERPENT and PRESENT. However, although these distinguishers are optimal in terms of correlation, they do not necessarily lead to the best attacks.

In this work, our objective was to identify distinguishers, based on the model of Hadipour et al., that are better suited for key-recovery attacks. To this end, we incorporated the key-recovery extended rounds into their tool and adapted the objective function to achieve a better trade-off between the distinguisher probability and the number of key bits to be guessed. We applied our enhanced tool to SERPENT and PRESENT. For SERPENT, our attack reaches 12 rounds with a time complexity of $2^{220.9}$ and a data/memory complexity of $2^{125.01}$. For PRESENT-80 (respectively PRESENT-128), our attacks reach 16 (respectively 18) rounds with a time complexity of $2^{73.88}$ (respectively 2^{124}) and a data/memory complexity of $2^{57.88}$ (respectively $2^{63.25}$).

*Intervenant