Tweakable AES-like Block Ciphers

Advisor(s): Maria Eichlseder and Lorenzo Grassi

Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

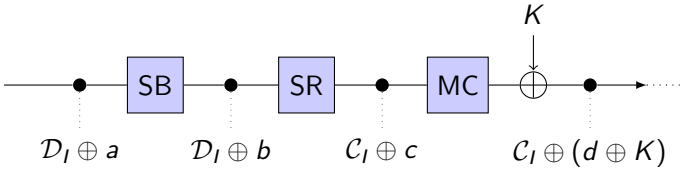
Motivation

AES is one of the most-used and well-analyzed symmetric primitives in the world. It has inspired many new cryptanalytic techniques as well as many designs. Among many others, Deoxys, Joltik and Kiasu are examples of tweakable AES-like block ciphers (all submitted to CAESAR competition). In contrast to standard block ciphers, tweakable block ciphers provide an additional input called tweak, which is used to select one specific instance of the block cipher.
Analyzing the effects of the tweak on the security of the design is not a trivial task. Recent attacks on Kiasu show that an adversary can exploit the tweak to extend existing attacks by one round. On the other hand, AES has also recently inspired new cryptanalysis approaches: For example, for a structured set of 2^{32} chosen plaintexts with one active diagonal, the number of different pairs of ciphertexts that lie in a particular subspace after 5 rounds of AES is always a multiple of 8.

Your task in this thesis is to investigate and study these new properties on tweakable AES-like block ciphers, focusing on the role of the tweak.

Goals and Tasks

- Get familiar with the required background: Tweakable ciphers, subspace cryptanalysis
- Study existing attacks
- Implement experiments to investigate required properties on tweakable AES-like block ciphers
- Determine if the attacks can be extended



$$\mathcal{D}_0 = \left\{ \begin{bmatrix} x_1 & 0 & 0 & 0 \\ 0 & x_2 & 0 & 0 \\ 0 & 0 & x_3 & 0 \\ 0 & 0 & 0 & x_4 \end{bmatrix} \;\middle|\; \forall x_1, x_2, x_3, x_4 \in \mathbb{F}_{2^8} \right\}.$$

Literature

- L. Grassi, C. Rechberger, and S. Rønjom
  A New Structural-Differential Property of 5-Round AES
  Advances in Cryptology – EUROCRYPT 2017
- C. Dobraunig, M. Eichlseder, and F. Mendel
  Square Attack on 7-Round Kiasu-BC
  Applied Cryptography and Network Security – ACNS 2016

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- Interest in cryptanalysis of block-ciphers
- Programming (C/C++, Java or Python)

Advisor / Contact

lorenzo.grassi@iaik.tugraz.at