Higher-Order Differential Cryptanalysis in Prime Fields

Advisor(s): Lorenzo Grassi and Christian Rechberger and Maria Eichlseder

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

Motivation

Higher-order differential cryptanalysis is a generalization of differential cryptanalysis, an attack used against block ciphers. While in standard differential cryptanalysis the difference between only two texts is used, higher-order differential cryptanalysis studies the propagation of a set of differences between a larger set of texts.
More precisely, let $E_k(\cdot) : \mathbb{F} \to \mathbb{F}$ be an encryption function with a fixed key k, and let $\mathcal{V} \subset \mathbb{F}$ be a subspace. Higher-order differential attacks exploit the fact that $\bigoplus_{x \in \mathcal{V} \oplus c} x = \bigoplus_{x \in \mathcal{V} \oplus c} E_k(x) = 0$ for each (fixed) c *if* the dimension of $\mathcal{V}$ is higher than the degree of $E_k(\cdot)$. In other words, a higher-order differential attack can be mounted by choosing an affine space - like $\mathcal{V} \oplus c$ - of dimension $d+1$ (or, equivalently, of size 2^{d+1}) if $E_k(\cdot)$ has degree at most d.
Since almost all relevant block ciphers are bit-based, almost all works in the literature analyze the security of *boolean* encryption functions $E_k(\cdot) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ w.r.t. such attack. However, quite recently cryptographers have started to consider also cryptographic primitives defined over $\mathbb{F}_p$. This is motivated by recent progress in practical applications of secure multi-party computation (MPC), fully homomorphic encryption (FHE), and zero-knowledge proofs (ZK), which natively support operations in $\mathbb{F}_p$ for large prime p and where primitives from symmetric cryptography are needed.

Your task in this thesis is to investigate and practical test the security of (encryption) functions defined over $\mathbb{F}_p$ with respect to higher-order differential attacks.

Goals and Tasks

- Get familiar with the required background: higher-order differential attack
- Study existing attacks
- Implement experiments to investigate the security of (encryption) functions defined over $\mathbb{F}_p$ with respect to higher-order differential attacks

Literature

- L. R. Knudsen
  Truncated and Higher Order Differentials
  Fast Software Encryption - FSE 1994
- C. Boura, A. Canteaut, and C. D. Cannière
  Higher-Order Differential Properties of Keccak and *Luffa*
  Fast Software Encryption - FSE 2011

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