New Ways to Analyze AES

Advisor(s): Christian Rechberger and Lorenzo Grassi

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

Motivation

Block ciphers play an important role in symmetric cryptography providing the basic tool for encryption. They are the oldest and most scrutinized cryptographic tools. One of the weakest cryptographic attacks that can be launched against them is the secret-key distinguisher. In this attack, there are two oracles: one that simulates the cipher for which the cryptographic key has been chosen at random and the other simulates a truly random permutation. The adversary can query both oracles and her task is to decide which oracle is the cipher and which is the random permutation. The attack is considered to be successful if the number of queries required to make a correct decision is below a well defined level.
AES is probably the most widely studied and used block cipher. So far, secret-key distinguishers that exploit non-random properties which are independent of the secret key are known for up to 4 rounds of AES. Recently, new distinguishers for 5-round of AES have been proposed. Your task in this project is to implement these new AES secret-key distinguishers.

Goals and Tasks

- Understand secret-key distinguishers for AES
- Implement new distinguishers for 5-round of AES

Literature

- L. Grassi et al.
  Subspace Trail Cryptanalysis and its Applications to AES
  Cryptology ePrint Archive, Report 2016/592 2016
  http://eprint.iacr.org/2016/592

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

- C/C++ programming or similar

Advisor / Contact

christian.rechberger@iaik.tugraz.at