New Key-Schedules for AES-256

Advisor(s): Lorenzo Grassi and Christian Rechberger

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

Motivation

In contrast to the serious effort applied to algorithm design, the aspect of key schedules for block ciphers has received comparatively little attention. This is despite the fact that many published block ciphers are vulnerable to known attacks that exploit the weaknesses of their key schedules.
AES is one of the most-used and well-analyzed symmetric primitives in the world. However, as for many other ciphers, the key schedule of AES has clear weaknesses that directly assist the execution of some effective attacks, e.g. invariant subspace attack and related-key attacks.

Your task in this thesis is to investigate and practical test new possible key-schedules for AES-256 (which aim to improve its security against the invariant subspace attack), focusing on the impact of related-key attacks.

Goals and Tasks

- Get familiar with the required background: AES, Differential Attacks, Related-Key Attacks
- Study existing attacks
- Implement experiments to investigate security of new AES-256 key-schedules against related-key attacks

Literature

- E.Biham
  New Types of Cryptanalytic Attacks using Related Keys
  Advances in Cryptology – EUROCRYPT 1993

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