

Motivation

The Square attack is a cryptanalytic attack that is particularly applicable to block ciphers based on substitution-permutation networks. It was originally designed by Lars Knudsen as a dedicated attack against the block cipher Square. Later it has been applied to other block ciphers including AES. Unlike differential cryptanalysis, which uses pairs of plaintexts with a fixed difference, this attack uses sets of plaintexts which part is held constant and another part varies through all possibilities.. Applying the attack on AES one can break up to 6 rounds. In this project, we implement the Square Attack on 3 and 4 rounds of AES.

Goals and Tasks

- ▶ Acquire the necessary background
- ▶ Understand the attack on AES
- ▶ Implement the attack on round-reduced AES

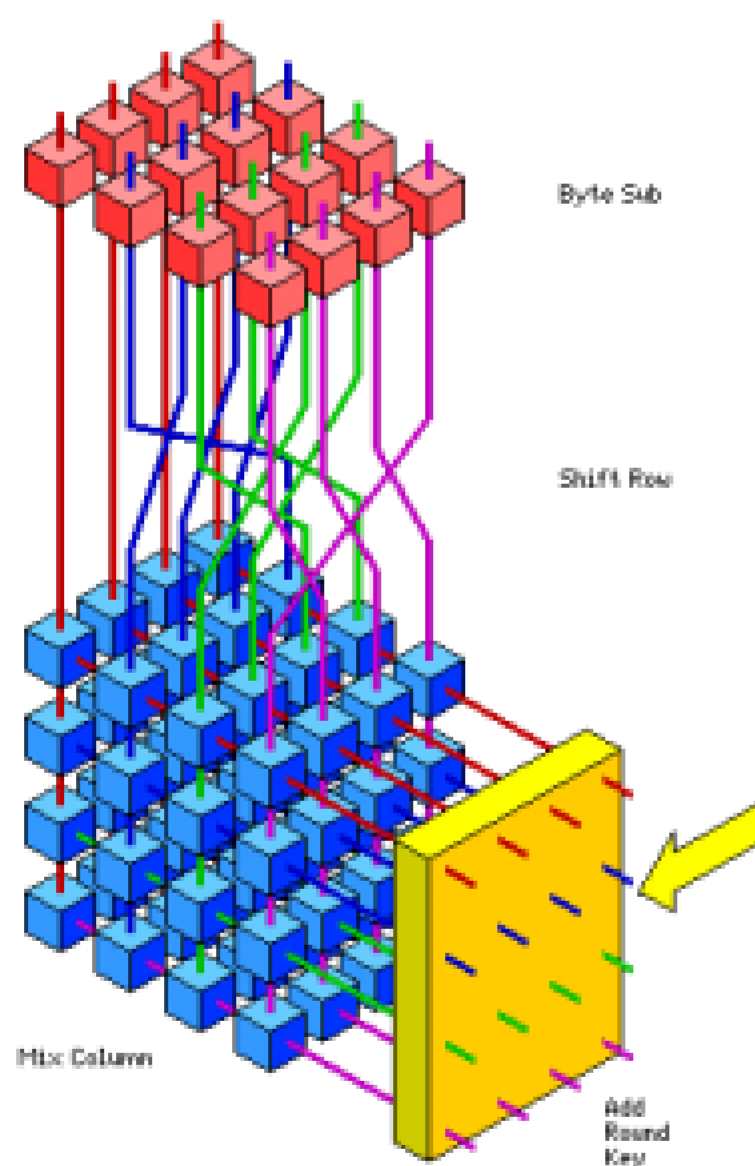


Figure 1: Schematic view of AES.

Literature

- ▶ J. Daemen, L. R. Knudsen, and V. Rijmen. The Block Cipher Square. In E. Biham, editor, *FSE*, volume 1267 of *LNCS*, pages 149–165. Springer, 1997.
- ▶ N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting. Improved Cryptanalysis of Rijndael. In B. Schneier, editor, *FSE*, volume 1978 of *LNCS*, pages 213–230. Springer, 2000.

Deliverables

- ▶ Project files (.zip, cleaned)
- ▶ Documentation (inline)
- ▶ Readme (getting started)
- ▶ Presentation (10 .ppt slides)

Project Schedule

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

Studies

- INF
- SW
- TEL
- TM

Prerequisites

- ▶ C/C++ programming

Advisor / Contact

martin.schlaeffer@iaik.tugraz.at