WHITE-BOX ATTACK RESISTANT CRYPTOGRAPHY

Dušan Klinec

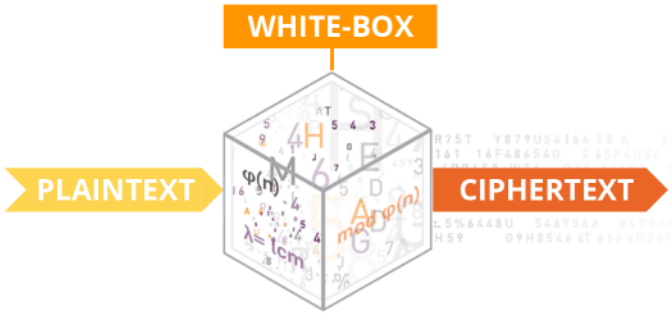
Advisor: RNDr. Petr Švenda, Ph.D.
Masaryk University, Faculty of Informatics

MOTIVATION

To execute cryptographic algorithms on untrusted platforms securely, in particular by protecting cryptographic material (e.g. encryption keys) from attacker observing such execution.

ATTACKER CAN

- trace the program flow
- see/modify program's memory
- change the program's logic
- induce faults

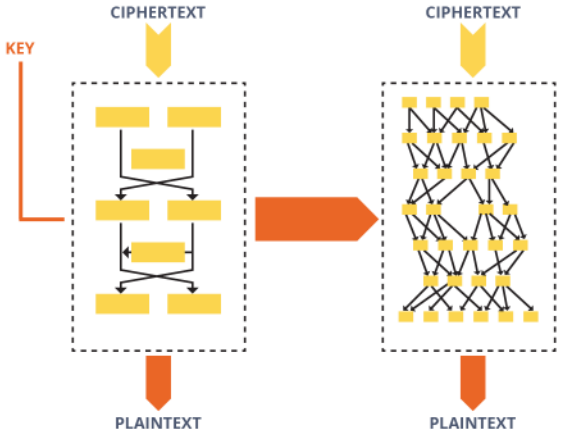


WHITE-BOX CRYPTOGRAPHY

To transform / re-implement a cryptographic algorithm in such a way that cryptographic assets remain secure even when subject to white-box attack.

TYPICAL USE-CASE

- DRM solutions, key-extraction would compromise the whole DRM system
- protection of licensing algorithm for software protection
- anti-cheating modules for games
- set-top boxes



STATE OF THE ART

The main focus is on white-box transformations of symmetric ciphers. Namely DES, AES.

- **DES:** several white-box schemes proposed, each of them broken
- **AES:**
  - 3 main white-box schemes proposed, each of them broken by algebraic analysis.
  - scheme using dual ciphers proposed, claiming its resistance to known attack, no cryptanalysis known.

RESULTS

- Proof that scheme using dual ciphers is not better than previous schemes, i.e. it is prone to algebraic cryptanalysis.
- Proposed a new symmetric encryption algorithm based on AES, with white-box transformations in mind. It fixes weak points of the white-box transformation with security at least as AES have.

CONTRIBUTIONS

- Implementation of 2 AES white-box transformations (default one, dual ciphers).
- Implementation of an algebraic attack on AES white-box transformation.
- Analysis of proposed improvements to new symmetric encryption algorithm based on AES.