Performance Evaluation of Protocols Resilient to Physical Attacks

Sylvain GUILLEY†, Laurent SAUVAGE†, Jean-Luc DANGER†, Nidhal SELMANE* and Denis RÉAL†.
*TELECOM-ParisTech, †Secure-IC S.A.S., ‡French DoD (Information Superiority)
Contact: {sylvain.guilley@TELECOM-ParisTech.fr}

Introduction

Context

- Cryptographic implementations are vulnerable to physical attacks.
- Many countermeasures to resist them have been proposed in the past.
- However, they are often too specific to a given attacker.
- Therefore, a new trend consists in making cryptographic implementations resilient to physical attacks.
- This strategy makes it possible to prove the countermeasure against all possible types of attackers.
- For a given security objective, they all permit to reach the same security level.
- Therefore, they differentiate only according to their efficiency.

State-of-the-Art

Indexed Key Update (IKU)

IKU is secure against passive attacks.

- Alice (A) and Bob (B) agree on a key thanks to: \( E^{k_0} \).
- When A needs to update the index, it sends: \( E_{k_1}^{-1}(I) \rightarrow B \) and \( E_{k_2}^{-1}(I) \rightarrow B \).
- Then, they use the cryptographic block cipher \( E \) with the current indexed key.


Fresh Re-Keying (FRK)

FRK is secure against passive attacks.

- The session key is determined randomly.
- Then, the cryptographic block cipher \( E \) is used with the agreed key.


Comparation of IKU & FRK

Passive and Active Attacks

Two contributions

- Protection against both passive and active attacks.
- Improvements in terms of:
  - I/O bandwidth
  - computational performance.

New Resilient Schemes Secure Against Passive and Active Attacks

Open Issue and Proposed Solution

- Problem: asymmetry between passive and active attacks:
  - against passive attacks, a key can be used \( q \) times, but
  - against active attacks, without protections, two encryptions enable an attack (DPA).
- Solution: prevent the attacker from choosing the plaintext.
  - this does not forbid passive attacks, since ciphertext attacks can be done, but
  - against active faults, the attack hypotheses are denied.

Blinding the Plaintext thanks to a MGF

Resilient MGF, used as partial AONT (All-or-Nothing Transform).

Optimizations

A. IKU+ and FRK+:
Because of the MGF (Mask Generation Function) the attacker cannot choose the plaintext.

B. Trick: Replace the strong encryption function in IKU by a lightweight equivalent: IKU* and IKU*+

C. FRK-H: instead of drawing a new key when necessary, the partners A and B can simply hash it with a lightweight algorithm \( h \) (hence the name FRK-H).

Summary

The differences between IKU* and FRK* fade away when \( n \rightarrow +\infty \).

Notations:

- \( D \) is the IKU key tree depth;
- \( B \) is the size in bits of the \( q \) block cipher;
- \( \sigma \) is the number of blocks to encrypt;
- \( \eta \) is the number of queries for a passive attack to successfull;
- \( |X| \) is the performance of operation \( X \);
- \( E \) and \( d \) are cryptographic-grade operations, whereas
- \( f \) is a lightweight operation.

Additional Requirements

- IKU and IKU* require \( \cdots \)-NVM but no TRNG;
- IKU* and IKU*+ require \( \cdots \) both NVM and TRNG;
- FRK, FRK+ & FRK-H require \( \cdots \) TRNG but no NVM.

Acknowledgements

- ANR Project ARPEGE ANR-09-SEGI-013.
- SecReSoC (Secure Reconfigurable System on Chip).
- Houssine MAGHREBI, for the presentation of this poster.