DESIGN, AUTOMATION & TEST IN EUROPE
27 – 31 March, 2017 · STCC · Lausanne · Switzerland
The European Event for Electronic System Design & Test

Side-Channel Plaintext-Recovery Attacks on Leakage-Resilient Encryption

Thomas Unterluggauer, Mario Werner, and Stefan Mangard,
IAIK, Graz University of Technology

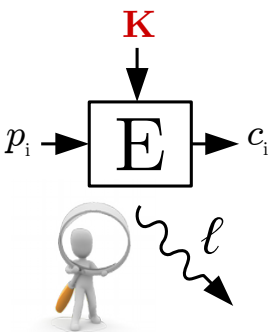
30. March 2017

Content

- Differential power analysis for key recovery
- Re-keying countermeasure: few data inputs
- Summary:
  - Re-keying induces DPA that allows to recover constant plaintexts
  - Streaming mode: first-order DPA
  - Block mode: profiled second-order DPA
  - Multi-party communication, memory encryption
    - Particularly critical for long-term keys

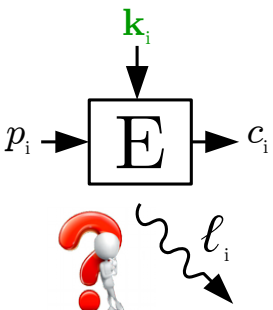
Motivation

- Symmetric cryptography, e.g., block cipher E
- Key K used for multiple p_i, c_i
- Differential Power Analysis (DPA)
  - n encryptions: $E_K(p_i)$
  - Observe power consumption
  - Statistical analysis reveals K



Motivation

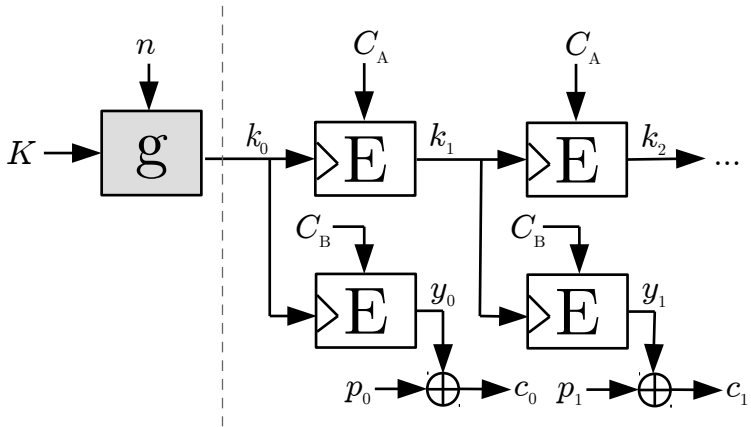
- Protect implementation (masking)
- Change key frequently (re-keying)
  - Reduce input data complexity
  - Leakage-resilient encryption
  - Protects the key
  - Plaintext?



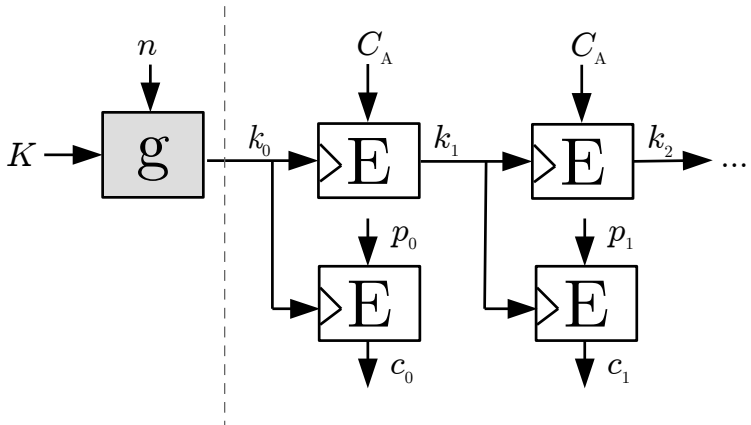
Leakage-Resilient Encryption

- Extends re-keying to messages of arbitrary length
- Secure (leak-free) initialization
  - Derive session key k_i from master key K
- Security proof:
  - Assumption: bounded side-channel leakage of the used primitive
  - Scheme's total leakage on the key is bounded

Leakage-Resilient Streaming Mode [SPY+10]

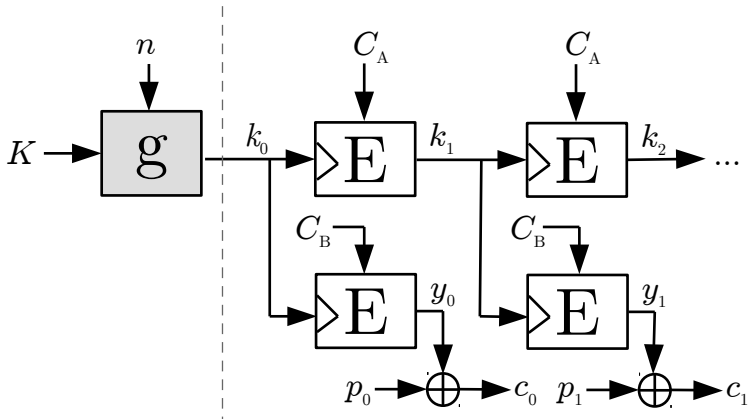


Leakage-Resilient Block Mode [TS15]



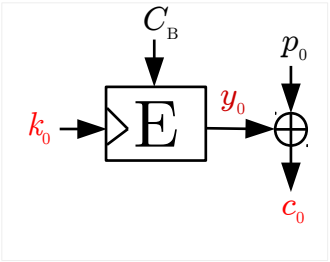
DPA on
Leakage-Resilient Encryption

DPA on Streaming Mode (1)



DPA on Streaming Mode (2)

- Encryption of constant p_0 with different keys k_0, k_0', k_0''
- Leakage model for $y_0 = c_0 \oplus p_0$, e.g., HW
- Compute leakage for all possible values of p_0
- Statistical distinguisher to get correct p_0



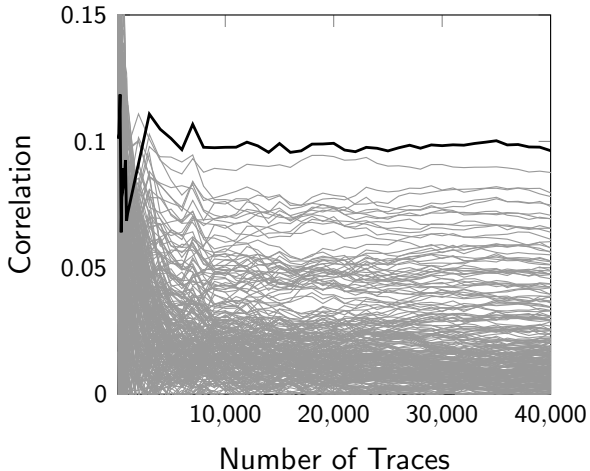
DPA on Streaming Mode (3)

- Standard DPA on XOR
- Applies to all stream ciphers
  - Key stream always changes:
    - pad must not be reused
  - Encryption of the same plaintext...

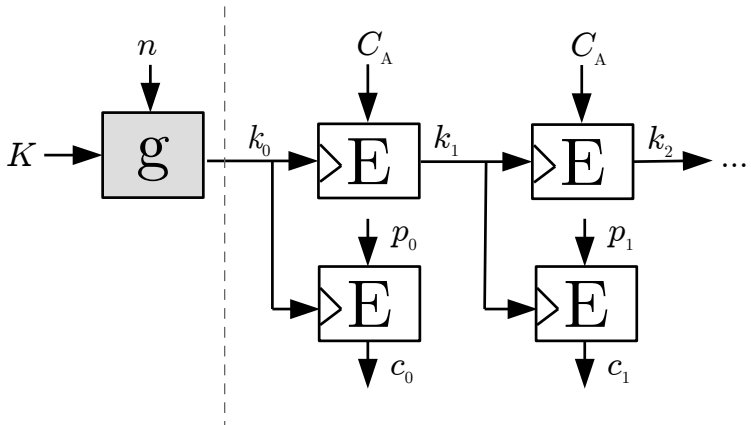
DPA on Streaming Mode: Evaluation

- Implementation of LR streaming mode
- Single AES core with one round per cycle
  - Multiplexing: pad computation and key update
  - Apply 128-bit pad to plaintext in parallel
- Sakura G board
  - Spartan 6 LX75 FPGA @ 24 MHz
  - Hardware trigger
  - LeCroy WP725Zi @ 250 MS
  - Correlation with byte-wise hypotheses

DPA on Streaming Mode: Evaluation

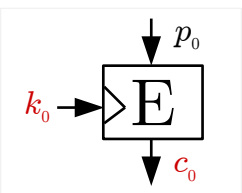


DPA on Block Mode (1)



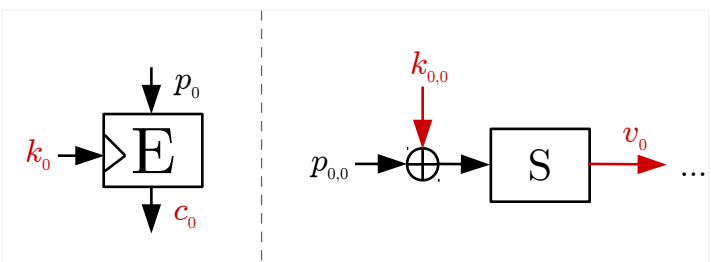
DPA on Block Mode (2)

- Encryption of constant p_0 with different keys k_0, k_0', k_0''
- Block cipher: no simple leakage model using p_0
- Unknown Plaintext Template Attacks [HTM09]
  - Constant key and varying, unknown plaintext
  - Idea: switch roles of key and plaintext



DPA on Block Mode (3)

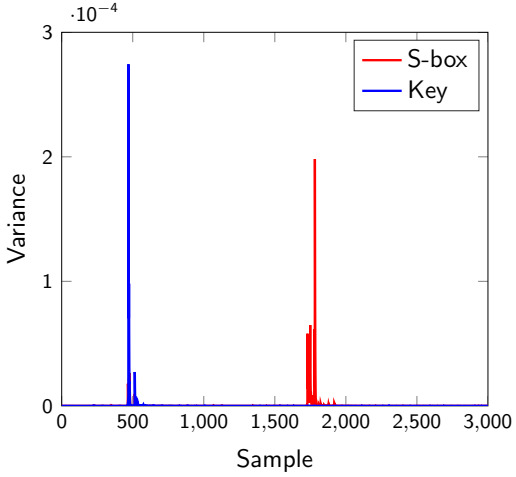
- Profiling phase: templates for $k_{0,0}$ and v_0
- Attack phase:
  - Probabilities for $k_{0,0}$ and v_0
  - Joint probability of $k_{0,0}$ and $v_0 \rightarrow p_{0,0}$
  - Many different keys to get unique $p_{0,0}$



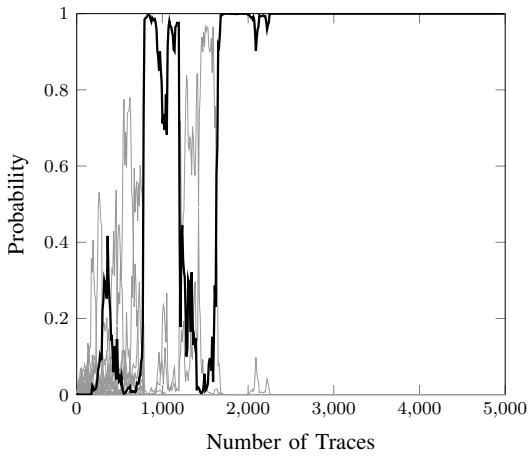
DPA on Block Mode: Evaluation

- Implementation of LR block mode
- AES: Byte-oriented C Implementation (AVR-Crypto-Lib)
- ChipWhisperer-Lite
  - Atmel XMEGA128D4-U @ 7.4 MHz
  - Sampling on board 29.5 MS
- Template building using 30 000 traces
  - Hamming weight of a byte (key / sbox)
  - Multivariate Gaussian templates (50 POI)

DPA on Block Mode: Evaluation



DPA on Block Mode: Evaluation



Applications

- Leakage rises with the amount of processed data
  - Mixing constant with varying data
  - Key vs. plaintext leakage
- Communication protocols
  - SSL: fresh session key
    - Download static file from, e.g., webserver
  - LR encryption: transmission errors
    - Constrained resources: re-encryption
  - Key wrapping insufficient

Application: Memory Encryption

- RAM encryption: fresh key on startup, e.g., Intel SGX
  - Critical if long-term key is loaded into RAM
    - Plaintext recovery = key recovery
- Storage with LR encryption:
  - Read-modify-write operations
    - Key update when a part changes
    - E.g., 1 byte in 128-bit block
- RAM encryption using counter mode:
  - Pad computed from address and block counter
  - Key changes on every copy and write-back

Conclusion

- Security of re-keying in LR encryption
  - Protects the key from SCA
  - Vulnerability: re-encryption of constant plaintexts
  - 1st order DPA on stream cipher
  - 2nd order template attack on block mode
- Classical setting: mixing constant with varying data
- Relevance: memory encryption and multi-party communication
- Use masking in these applications

DESIGN, AUTOMATION & TEST IN EUROPE
27 – 31 March, 2017 · STCC · Lausanne · Switzerland
The European Event for Electronic System Design & Test

Side-Channel Plaintext-Recovery Attacks on Leakage-Resilient Encryption

Thomas Unterluggauer, Mario Werner, and Stefan Mangard,
IAIK, Graz University of Technology

30. March 2017

References

[HTM09] Neil Hanley, Michael Tunstall, and William P. Marnane.

Unknown plaintext template attacks.

In *WISA 2009*, pages 148–162, 2009.

[SPY+10] François-Xavier Standaert, Olivier Pereira, Yu Yu, Jean-Jacques Quisquater, Moti Yung, and Elisabeth Oswald.

Leakage resilient cryptography in practice.

In *Towards Hardware-Intrinsic Security – Foundations and Practice*, pages 99–134. 2010.

[TS15] Mostafa M. I. Taha and Patrick Schaumont.

Key updating for leakage resiliency with application to AES modes of operation.

IEEE Trans. Information Forensics and Security, 10(3):519–528, 2015.