Seitenkanal- und fehlerangriffsresistente kryptographische Protokolle

22. SIT-SmartCard Workshop

Dr. Berndt Gammel
Security Innovation
Chip Cards & Security ICs
Infineon Technologies AG
Contents

- Why side-channel attacks hurt
  - DPA and Co. / Countermeasures
  - DFA and Co. / Countermeasures
  - DPA/DFA security for low-cost products?

- Moving to higher abstraction levels
  - Early protocol level countermeasures
  - Leakage-resilient crypto?

- The new approach:
  Protocol-enabled side-channel resistance
  - The idea of the NLM
  - Advantages of protocol-enabled side-channel resistance
  - A first realization: The new CIPURSE™ standard
DPA – Differential Power Analysis
Passive/Non-Invasive Attack

Target of attack:
The secret key used in a cryptographic calculation like AES or RSA is revealed by using power analysis combined with a statistical hypothesis testing approach.

Examples for realization of attack:
The power consumption of the chip during the crypto-operation is recorded and analyzed. The processed operations or the secret key will be revealed.

Example for Simple Power Analysis (SPA)
Analyzing the power consumption of an insecure implementation, the processed secret key is revealed.
Why Side-channel attacks hurt DPA and Co.

- Since the first publication of DPA (1999) there have been dramatic improvements

  - in measuring side-channel leakage, e.g. local electromagnetic emanations (EMA) improve the signal-to-noise ratio.

  - by sophisticated statistical methods, extracting more information from recorded power/EM traces:
    - Higher-Order DPA (HODPA)
    - Correlation power attacks (CPA)
    - Stochastic approach
    - Template attacks and SPA
Why Side-channel attacks hurt DPA and Co.

- Traditional countermeasures:
  - **Ad hoc**: Hiding countermeasures: add noise to reduce SNR. *Effectiveness of noise addition is limited.*
  - **Ab initio**: Logic style countermeasures: try to reduce leakage at source, e.g. SABL, dual-rail logic styles (DCVSL). *Inefficient in terms of area and power.* *Encumbered with lack of standardized design tool support.*
  - **Algebraic**: Masking countermeasures (aka. blinding) promised to be a sound mathematical method against DPA and HODPA. *Nevertheless, most naive masking implementations can be broken, because physics of circuits violates mathematical assumptions: glitches (‘05) and propagation effects (‘09).*
DFA – Differential Fault Analysis
Active/Semi-Invasive

Target of attack:

The secret key used in a cryptographic calculation like AES, or RSA is revealed by inducing few faults during the calculation combined with solving some algebraic equations.

[1] Boneh et al., Eurocrypt’97: disturb RSA-CRT, 1 faulty cipher text
[2] Piret & Quisquarter, CHES’02: disturb 7/8 round AES MC, 2 faulty cipher texts
[3] Saha et al., Eprint’09: disturb 7/8 round AES MC, 1 - 4 faulty cipher texts, 400 sec on PC

Examples for realization of attack:

- Spike attack on power lines, clock pads, or wires
- Electrical discharge fire lighter (Schmidt’09)
- Optical Fault Induction
- Probing station and needles

Injecting a single fault during crypto operations and observing the faulty result (plus a correct one) can reveal the secret key.
DPA & DFA and Countermeasures for Low-Cost Products?

DPA countermeasures:
Significant overhead in software and hardware:
- Area/code penalty: $\times 3-5$
- Performance penalty: $\times 5-50$

DFA countermeasures:
Significant overhead in software and hardware:
- Area/code penalty: $\times 2-5$
- Performance penalty: $\times 2-5$

Vicious circle:
- Redundant information leaks!
- DPA countermeasures require redundancy!
DPA & DFA and Countermeasures for Low-Cost Products?

Consequences:

- Low-cost RFID products may not meet requirements for transaction times with given energy budget (if worthwhile countermeasures are provided).

- ...or the other way round: If more efficient countermeasures were available, higher-valued applications based on low-cost devices would be enabled.

- In the area of high-security products strong countermeasures are available, however the long-term sustainability can still be improved – breaking the arms race with ever improving DPA attack methods.
Cryptography is not enough!
The security pyramid

Traditional approach

Security by cryptography
(black box assumption, integrity of operation)

Physical security by implementation

Apps.

Protocols

Crypto-Primitives

Basic Arithmetic Units

Circuit Design/Logic Styles

Semiconductor Physics

ABSTRACTION LEVEL
Cryptography is not enough!

New approaches

Mitigate assumptions of black-box cryptography by considering:

- leaky computation ("leakage-resilient cryptography")
- faulty computation
- thwart physical attacks on protocol level not only within crypto-primitives
Moving to higher abstraction levels:
Early Protocol-Level Countermeasures

- One solution for this idea is given in Kocher’s 1999 patent “Leak-Resistant Cryptographic Indexed Key Update“ US 6,539,092:

- Problems of the approach:
  - Synchronization of key updates requires additional programming of “index/key“ on IC,
  - as well as many an increasing number of addt’l. encryptions on terminal side (although logarithmic in the index)
Moving to higher abstraction levels:
Leakage-Resilient Crypto

- A new and very active research community:
  - aims at designing new cryptographic primitives, which are not base on
    the black-box assumption of traditional cryptography.
  - allow certain amount of leakage in intermediate computation steps:
    - bounded/continual leakage models.
    - usually based on ‘only computation leaks’ paradigm
      (Michali-Reyzin’04).
  - First proposals for resilient pseudorandom functions, stream ciphers,
    and signature schemes have been published.

- Difficulties with LRC approach:
  - Does the leakage model map to reality?
  - Generally, the existing crypto primitives can no longer be used.
The idea & question:
Can we treat the problems of cryptographic security and side-channel security separately?
A new principle:

Do not solve the independent problems of

- cryptography
- side-channel/fault resistance

at once within the crypto algorithm, because highly complex (confusion/diffusion/...) operations are notoriously hard to protect against all kinds of attacks, i.e. DPA, DFA.

Protocol-enabled side-channel resistance is a joint development of

Wieland.Fischer
Berndt.Gammel
Stefan.Mangard

@ Infineon.com
Moving to higher abstraction levels: Protocol-enabled side-channel resistance

- **Targets:**
  - An authentication protocol in the symmetric key setting, such that no side-channel protected crypto primitives are needed. (e.g. “plain” implementation AES).
  - Protocol must fit to small, resource-constrained implementations.

- **Basic principle to counter differential side-channel attacks on the cipher algorithm (e.g. AES):**
  - Never use a key twice.
    - i.e. use a fresh key in each authentication (and for each encrypted or MACed message block).
Moving to higher abstraction levels: Side-channel resilient session key derivation

Take a look at the conventional DPA-prone situation in a session key derivation:

Master key

public string

$K_{ID}$

$C_{KID}(r)$

$r$

$K_0$

block cipher (e.g. AES)

session key
Moving to higher abstraction levels:
Side-channel resilient session key derivation

Divide-and-conquer approach:
- Transform input of cipher using a map which can be easily protected against SCA.
- Separate the requirements on cryptography and SCA

Diagram:
- Master key
- Public random string
- Block cipher (AES)
- Map NLM
- Intermediate key
- Session key
- NLM(K_{ID}, r)
- K_{ID}
- C_{K'}(K_{ID})
- K_0
Moving to higher abstraction levels:
Side-channel resilient session key derivation

but wait...

... aren’t we caught in a bootstrap paradox?
Answer:
(1) No, there is no paradox at all.
(2) The DPA problem is now radically simplified, due to the separation of the cryptographic and DPA resistance problems.

Requirements for map NLM and cipher C:

C:  ¬ Cryptographic security
    ¬ Secure against SPA (only).

NLM: ¬ Secure against SPA and DPA
     (hence it is called Non-Leaking Map)
     ¬ Need not be cryptographically strong
     ¬ Strong diffusion (prevent divide-and-conquer in DPA)
     ¬ Stateless (otherwise synchronization problem like Kocher’s)
     ¬ Simple to protect against DPA,
       i.e. regular algebraic structure that can be easily masked/randomized
     ¬ Small in hardware implementation
     ¬ Fast in software implementation
Moving to higher abstraction levels:
Non-Leaking Map

An efficient choice for NLM is:

\[ \text{NLM: } F_2[x]/p(x) \times F_2[x]/p(x) \rightarrow F_2[x]/p(x) : (k, r) \rightarrow k \cdot r. \]

- Properties of polynomial \( p(x) \):
  - irreducible
  - high weight (good diffusion)
  - degree of \( p(x) \) is a security parameter

- Example: On the RFID we generate two secret values \( r_1, r_2 \) from which the public value \( r = r_1 \cdot r_2 \) and a secret value \( k_P \) is deduced:

  \[
  k_P = r \cdot k_{\text{ID}} = (k_{\text{ID}} \cdot r_1) \cdot r_2
  \]

- Security can be made „symmetric“. Terminal can use \( r \) provided by client and apply an additive secret sharing:

  \[
  r \cdot k_{\text{ID}} = r_a k_{\text{ID}} + r_b k_{\text{ID}} \quad \text{with} \quad r = r_a + r_b
  \]
Moving to higher abstraction levels:

Security Aspects

- **Protection against side-channel attacks:**
  Differential side-channel attacks:
  - In our scheme the same input is never encrypted under the same key.

- **Protection against fault attacks:**
  Differential fault attacks require (at least) a pair of
  - one correct output
  - one erroneous output
to recover the key.
  - In our scheme the same input is never encrypted under the same key.
Moving to higher abstraction levels:
Secure Communication Channel

- Once a session key $K_0$ has been derived in a side-channel secure way, subsequent secure messaging with encryption or MAC protection can be easily set up:

  - Use a key evolution scheme, deriving a fresh key for each message (encryption or MAC) block.

  - Use established cryptographic building blocks, e.g., Matyas-Meyer-Oseas one-way compression function:
A similar solution proposed later on in academic literature ...

**Africacrypt 2010:**

Advantages of Protocol-enabled side-channel resistance

- Established cryptographic primitives, like the AES encryption standard, can be used.  
  *In contrast to DPA resilient cryptography, no new cryptographic algorithms need to be developed.*

- Cryptographic primitive must only be secure against SPA.  
  *Hence, only efficient and cheap countermeasures need to be implemented.*  
  *As shown, the NLM can be protected very efficiently against DPA.*

- Compared to traditional DPA/DFA countermeasures (hiding, masking, circuit design,...)  
  - performance penalty in software  
  - hardware overhead (= area = costs)  
  is smaller by an order of magnitude.
Advantages of Protocol-enabled side-channel resistance (2)

- The complexity of secure implementations is significantly reduced.
  
  The risk for flaws in the implementation is reduced.
  
  The efforts for the security evaluation are reduced.

- Low-cost products which so far could not be protected against DPA, because of resource constraints, can now be efficiently protected.
  
  Hence, higher-valued applications are enabled on resource-constrained devices.

- For high-end security products the long-term sustainability can be improved.
  
  A step towards breaking the arms race with ever improving DPA attack techniques.
A first realization: The new CIPURSE™ standard

The first realization of the new leakage resilient cryptographic protocol is the CIPURSE™ standard of the OSPT*) Alliance.

*) OSPT = Open Standard for Public Transport

Other realizations will follow…
The OSPT Alliance – at a glance

Provide an Open Standard for Public Transport

- An international association chartered to define a new open standard for secure transit fare collection. (Launched in 2010 and founded in 2011).
- The initiative is open for transport industry player - the global multi-provider community.
- The solution will build on open standards.
- Key benefits for public transport agencies:
  - advanced security and performance for public transport applications,
  - optimized interoperability,
  - availability of multiple sources for chip products and vendors that may competitively offer a variety of products
- The chosen standard is CIPURSE™.

www.osptalliance.org
Protocol-enabled side-channel resistance

- is a step towards closing the gap between cryptographic and side-channel security

- is a step towards closing the gap for the attacker!
Protocol-enabled side-channel resistance: Close the gap for the attacker!

Crypto

DPA

Copyright © Infineon Technologies 2011. All rights reserved.
Thank you for your attention!
Innovative semiconductor solutions for energy efficiency, mobility and security.