Automatic derivation of optimal side-channel attacks rounded at a given order

N. Bruneau, C. Christen, A. Facon, S. Guilley

Presented by Prof. J.-L. Danger

Presentation Outline

Presentation Outline

Security requirements for cryptographic libraries

Attacks on crypto libs

It is necessary to protect software implementations of cryptographic libraries.

Solution: secure crypto libs

Secure-IC offers in its portofolio a full-fledged library (incl. post-quantum crypto) suitable for:

- Crypto such as symmetric and asymmetric encryption and decryption, and hashing
- Key management capabilities
- Secure protocols, such as MACsec, IPsec, TLS and SSH
- Enabling Secure applications such as HTTPS, SMTPS, VPN

Methodology of test

Software code protections are reviewed in ETSI TR [?].

We focus on the protection of crypto libs, for which risks are:

1. Correctness (see CVE)—test by KAT, certification by CAVP/CMVP, methodology such as MISRA, tools like valgrind, etc.
2. Resistance to physical perturbation attacks—redundancy, invariants, etc.
3. Resistance to side-channel attacks (see ISO 17825):
   3.1. Sensitive control-flow (i.e. *remote* cache-timing attacks, or *physical* leakage exploitable by SPA)—which is addressed by Catalyzr (academic tools: ct-verif, etc.)
   3.2. Sensitive values (i.e. horizontal attacks such as correlation-collision, and vertical attacks, such as DEMA)—which is addressed by masking and/or balancing

The order of tests is: 1 $\longrightarrow$ (2 or 3), and 3.1 $\longrightarrow$ 3.2.

Value-based side-channel leakage mitigation

Regarding protection of data leakage (physically measured), there are two strategies (balancing and masking).

1. Balancing [MOP06, Chap. 7] relies on the ability to find two equivalently leaking bits.
2. Masking [MOP06, Chap. 9] do not require hypotheses on the underlying hardware: we focus on this countermeasure in the sequel.
   - a dominant paradigm is that of uniform multi-share masking, typically in a characteristic two Galois field
   - Additive masking. Illustrative examples are AES or lightweight block cipher PRESENT (algorithm *a* in ISO/IEC 29192 [ISO]).

Presentation Outline

Virtualyzr: hardware evaluation on HDL code

- Dynamic execution to find weaknesses:
  - Fast evaluation close to real-world analyses
  - Locate the date(s) of the leakage

Catalyzr: software evaluation on source code (ANSI C)

- Symbolic analysis:
  - 100% coverage of the code
  - Identify even small vulnerabilities (which would require millions of traces in dynamic analysis)
  - Pinpoint the violations directly in the source code

State-of-the-art in symbolic execution

Work of Barthe et al. (EUROCRYPT 2015) [BBD+15]

A proof of masking correction:

- Exhaustive check of the property: "all d-uple of intermediate variables is independent from the secret"
- Leverages the property that $M \oplus E$, where E is an expression independent from random mask M, is simply distributed as another uniformly distributed random mask M'.
- Used to attest of the soundness of a masking scheme, or to find explicit counter-examples.

Presentation Outline

Contribution #1

- We automate the proof of a Boolean additive masking scheme directly from within a compiler:
  - From a practical point of view, this allows to streamline the evaluation: the user codes the countermeasure in the language of its own, and then an automated verdict is provided.
  - We position the analysis after the optimization passes, hence we analyze the actual assembly (i.e., machine code) which will be executed. This means that we detect faults caused by the compiler, which could break the countermeasure.

Contribution #2

- In addition to proving the soundness (or not), we generate the optimal attack:
  - Indeed, being secure at order d is actually **not a metric from the attacker standpoint**, but a *design-for-security* evidence for *obligation of means*.
  - But outputting the **optimal attack**, we can evaluate the real security level (recall that a countermeasure at order 2 can be defeated faster with a 3rd order attack than with a 2nd order attack, provided the multiplicity of leakages increases the SNR of the 3rd order attack beyond that of the 2nd order attack.)
  - For the sake of tractability of the computation, we also allow the optimal attack [BGHR14] to be rounded at a given order [BGH+16]

Implementation

- Compiler: LLVM
- Symbolic expressions extraction: saw plugin
- Computation of the terms: Julia formal language
- Simplification of the terms: Sage
- Attack: compilation of optimized C code generated from Sage

Presentation Outline

Use-case on PRESENT (nibble-oriented)

PRESENT [BKL+07]: nibble-oriented block cipher

- Substitution box expanded as a polynomial, using Lagrange interpolation theorem
- Therefore based on addition (XOR) and multiplication in $\mathbb{F}_{16}$, allowing Masking

Substitution box is the hard part

- $\mathbb{F}_{16} \approx \mathbb{F}_2[x]/x^4 + x + 1$
- Result:
  $\text{sbox}(A) = \sum_{i=0}^{14} a_i A^i = 12 + 7A^2 + 7A^3 + 14A^4 + 10A^5 + 12A^6 + 4A^7 + 7A^8 + 9A^9 + 9A^{10} + 14A^{11} + 12A^{12} + 13A^{13} + 13A^{14}$.

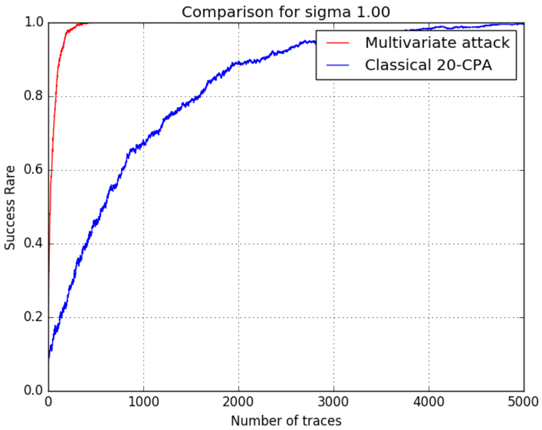
Taylor expansion

For the attack computation to be tractable

- Optimal attack [BGHR14]:
  $\hat{k} = \mathrm{argmax}_k \sum_{q=1}^{Q} \log \sum_m \exp -\frac{1}{2\sigma^2} (x_q - f(t_q, k))^2$, where:
  - q are the traces index
  - m are the masks
  - x_q are the leakages, $x_q = f(t_w, k^*)$ where k^* is the correct key
  - t_q are the known texts, e.g., plaintexts
  - f is the leakage model, e.g., $f(t_q, k) = w_H(S(t_q \oplus k))$ obtained by profiling
  - σ^2 is the noise variance
- Taylor expansion: $\log \mathbb{E} \exp(tX) = \sum_{n=1}^{\infty} \kappa_n \frac{t^n}{n!}$
  - where κ_n is the cumulant of order n of random variable X
- Starting at order $n = d$ and stopping before ∞ for tractability

Attack results

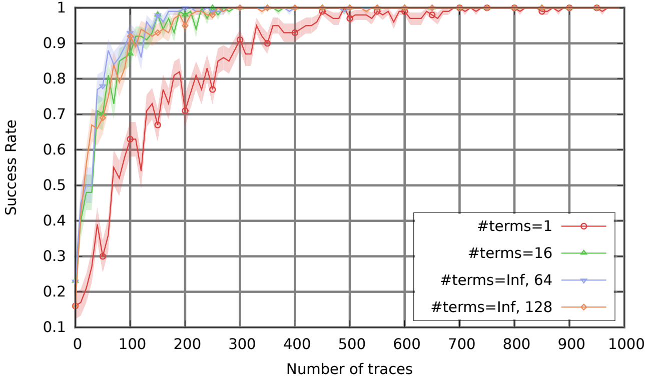
Taking into account all shares gives the true image of security



Multiplication in $\mathbb{F}_{16}$.

Attack results

Attack expansion order is less important that SNR amplification at minimum order



Cube operation in $\mathbb{F}_{16}$, with different attack roundings.

Presentation Outline

Conclusions and Perspectives

Conclusions

- Automated masking side-channel countermeasure after optimization, as per [BBD+15]
- Derivation of the optimal attack, which gives a concrete sense of security

Perspectives

- Extension from *source* to *IR*: OK. However, how about IR→ASM?
- Extend to masking schemes which are not full-entropy or that reuse masks

Bibliographical references I

[BBD+15] Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, and Pierre-Yves Strub.
Verified Proofs of Higher-Order Masking.
In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 457–485. Springer, 2015.

[BGH+16] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Olivier Rioul, François-Xavier Standaert, and Yannick Teglia.
Taylor Expansion of Maximum Likelihood Attacks for Masked and Shuffled Implementations.
In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 573–601, 2016.

[BGHR14] Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, and Olivier Rioul.
Masks Will Fall Off – Higher-Order Optimal Distinguishers.
In Palash Sarkar and Tetsu Iwata, editors, *Advances in Cryptology – ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014, Proceedings, Part II*, volume 8874 of *Lecture Notes in Computer Science*, pages 344–365. Springer, 2014.

Bibliographical references II

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and Charlotte Vikkelsoe.
PRESENT: An Ultra-Lightweight Block Cipher.
In *CHES*, volume 4727 of *LNCS*, pages 450–466. Springer, September 10-13 2007. Vienna, Austria.

[ISO] ISO/IEC 29192-2:2012.
Information technology – Security techniques – Lightweight cryptography – Part 2: Block ciphers.
Publication date: 2012-01, Edition: 1. https://www.iso.org/standard/56552.html.

[MOP06] Stefan Mangard, Elisabeth Oswald, and Thomas Popp.
Power Analysis Attacks: Revealing the Secrets of Smart Cards.
Springer, December 2006.
ISBN 0-387-30857-1, http://www.dpabook.org/.

THANKS FOR YOUR ATTENTION

CONTACT

EUROPE	sales-EU@secure-ic.com
APAC	sales-APAC@secure-ic.com
JAPAN	sales-JAPAN@secure-ic.com
AMERICAS	sales-US@secure-ic.com