Exact Template Attacks with Spectral Computation

Meriem MAHAR Maamar OULADJ Sylvain GUILLEY
Hacène BELBACHIR Farid MOKRANE

Université Paris 8, LAGA, UMR 7539, Paris, France.

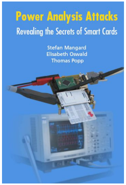
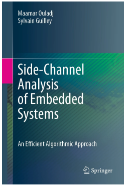
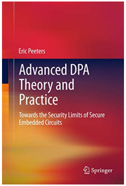
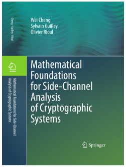
CERIST, Algiers, Algeria.

Secure-IC S.A.S., Rennes, France,
and École Normale Supérieure (ENS), Paris, France.

CATI, RECITS Laboratory, USTHB, Algiers, Algeria.

December 16-18, 2024.

Books and Manuals about Side-Channel Analysis

Cover page	Year	Authors	Title	Cover page	Year	Authors	Title
	2007	Stefan Mangard, Elisabeth Oswald, Thomas Popp	*"Power analysis attacks — revealing the secrets of smart cards"*, Springer		2021	Maamar Ouladj, Sylvain Guilley	*"Side-Channel Analysis of Embedded Systems — An Efficient Algorithmic Approach"*, Springer
	2013	Eric Peeters	*"Advanced DPA Theory and Practice: Towards the Security Limits of Secure Embedded Circuits"*, Springer		2024	Wei Cheng, Sylvain Guilley, Olivier Rioul	*"Mathematical Foundations for Side-Channel Analysis of Cryptographic Systems"*, Springer

Outline

- Introduction

Outline

- Introduction
- Exact template attack distinguisher expression
  $\Longrightarrow$ data complexity reduction

Outline

- Introduction
- Exact template attack distinguisher expression
  $\Longrightarrow$ data complexity reduction
- Spectral expression of the distinguisher
  $\Longrightarrow$ computational complexity reduction

Outline

- Introduction
- Exact template attack distinguisher expression
  $\Longrightarrow$ data complexity reduction
- Spectral expression of the distinguisher
  $\Longrightarrow$ computational complexity reduction
- Experimental validation

Outline

- Introduction
- Exact template attack distinguisher expression
  $\Longrightarrow$ data complexity reduction
- Spectral expression of the distinguisher
  $\Longrightarrow$ computational complexity reduction
- Experimental validation
- Conclusion and perspectives

Seminal CRYPTO'99 paper: 10351 citations.

Differential Power Analysis

Paul Kocher, Joshua Jaffe, and Benjamin Jun

Cryptography Research, Inc.
870 Market Street, Suite 1088
San Francisco, CA 94102, USA.
http://www.cryptography.com
E-mail: {paul,josh,ben}@cryptography.com.

Abstract. Cryptosystem designers frequently assume that secrets will be manipulated in closed, reliable computing environments. Unfortunately, actual computers and microchips leak information about the operations they process. This paper examines specific methods for analyzing power consumption measurements to find secret keys from tamper resistant devices. We also discuss approaches for building cryptosystems that can operate securely in existing hardware that leaks information.

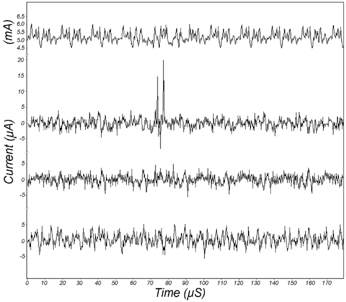


Figure 4: DPA traces, one correct and two incorrect, with power reference.

Simple monovariate attack.

Information Leakage: . . . . Device Analysis

But in practice, traces are vectorial.

Daniel Genkin, Lev Pachmanov, Itamar Pipman, and Eran Tromer, *ECDH key-extraction via low-bandwidth electromagnetic attacks on PCs*. CT-RSA 2016.

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;
- Z is the vectorial Boolean function of T and k in which there is a leakage; Typically, Z is a function of $X \oplus k$

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;
- Z is the vectorial Boolean function of T and k in which there is a leakage; Typically, Z is a function of $X \oplus k$
- M is the leakage model corresponding to Z;

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;
- Z is the vectorial Boolean function of T and k in which there is a leakage; Typically, Z is a function of $X \oplus k$
- M is the leakage model corresponding to Z;
- L is the side-channel leakage measured by the attacker;

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;
- Z is the vectorial Boolean function of T and k in which there is a leakage; Typically, Z is a function of $X \oplus k$
- M is the leakage model corresponding to Z;
- L is the side-channel leakage measured by the attacker;
- N is the noise.

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;
- Z is the vectorial Boolean function of T and k in which there is a leakage; Typically, Z is a function of $X \oplus k$
- M is the leakage model corresponding to Z;
- L is the side-channel leakage measured by the attacker;
- N is the noise.

  Such that:

$$X, k \to Z$$

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;
- Z is the vectorial Boolean function of T and k in which there is a leakage; Typically, Z is a function of $X \oplus k$
- M is the leakage model corresponding to Z;
- L is the side-channel leakage measured by the attacker;
- N is the noise.

  Such that:

$$X, k \to Z \to M(Z) = M$$

Mathematical model and notations

We model the side-channel problem as follows:

- X is the digital part known by the attacker, typically some plaintext or ciphertext (n-bit wide);
- k is the digital part unknown by the attacker, typically some part of key, which is fixed;
- Z is the vectorial Boolean function of T and k in which there is a leakage; Typically, Z is a function of $X \oplus k$
- M is the leakage model corresponding to Z;
- L is the side-channel leakage measured by the attacker;
- N is the noise.
  Such that:

$$X, k \rightarrow Z \rightarrow M(Z) = M \rightarrow L = M + N.$$

Mathematical model and notations

- Those variables are measured many times (Q times);

Mathematical model and notations

- Those variables are measured many times (Q times);
- The noise N are all i.i.d, such that $N \sim \mathcal{N}(0, \Sigma)$;

Mathematical model and notations

- Those variables are measured many times (Q times);
- The noise N are all i.i.d, such that $N \sim \mathcal{N}(0, \Sigma)$;
- The measurements are multidimensional of dimensionality D;

Mathematical model and notations

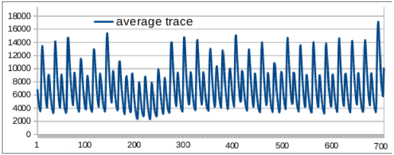
- Those variables are measured many times (Q times);
- The noise N are all i.i.d, such that $N \sim \mathscr{N}(0, \Sigma)$;
- The measurements are multidimensional of dimensionality D;
- Oscilloscopes: D samples per trace and several samples per clock period;

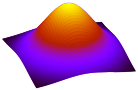
Mathematical model and notations

- Those variables are measured many times (Q times);
- The noise N are all i.i.d, such that $N \sim \mathcal{N}(0, \Sigma)$;
- The measurements are multidimensional of dimensionality D;
- Oscilloscopes: D samples per trace and several samples per clock period;
- Σ: the $D \times D$ covariance matrix of the noise.

Mathematical model and notations

- Those variables are measured many times (Q times);
- The noise N are all i.i.d, such that $N \sim \mathcal{N}(0, \Sigma)$;
- The measurements are multidimensional of dimensionality D;
- Oscilloscopes: D samples per trace and several samples per clock period;
- Σ: the $D \times D$ covariance matrix of the noise.





Mathematical model and notations

If the adversary has an identical copy of the target crypto system:

Mathematical model and notations

If the adversary has an identical copy of the target crypto system:
Template attack = Profiling stage + Matching stage.

If the adversary has an identical copy of the target crypto system:
Template attack = Profiling stage + Matching stage.

- Profiling stage: according to the maximum likelihood principle, the model matrix M_k and the covariance matrix Σ are estimated as:

$$M_k = average(L_k); \qquad \Sigma = \frac{1}{Q}(LL^\mathsf{T} - MM^\mathsf{T});$$

Mathematical model and notations

Template attack = Profiling stage + Matching stage.

Mathematical model and notations

Template attack = Profiling stage + Matching stage.

- Matching stage:
  - $L = M_{k^*} + N \quad : D \times Q$ matrices
  - $p_{N_q}(L_q - M_{q,k}) = \frac{1}{\sqrt{(2\pi)^Q |\Sigma|}} e^{-\frac{1}{2}(L_q - M_{q,k})^T \Sigma^{-1} (L_q - M_{q,k})}$
  - Since N is independent from M_k:

$$p(L|M_k) = p_N(L - M_k) = \prod_q p_{N_q}(L_q - M_{q,k})$$

Template attack = Profiling stage + Matching stage.

- Matching stage:
  - $L = M_{k^*} + N \quad : \; D \times Q$ matrices
  - $p_{N_q}(L_q - M_{q,k}) = \frac{1}{\sqrt{(2\pi)^Q |\Sigma|}} e^{-\frac{1}{2}(L_q - M_{q,k})^T \Sigma^{-1} (L_q - M_{q,k})}$
  - Since N is independent from M_k:

Theorem (Theorem 1 of [1])

Template attacks guess the key as:

$$\hat{k} = \underset{k}{\operatorname{argmin}} \; \operatorname{tr}((L - M_k)^{\mathsf{T}} \Sigma^{-1} (L - M_k)).$$

Mathematical model and notations

Template attack = Profiling stage + Matching stage.

- Matching stage:
  - $L = M_{k^*} + N$: $D \times Q$ matrices
  - $p_{N_q}(L_q - M_{q,k}) = \frac{1}{\sqrt{(2\pi)^Q|\Sigma|}} e^{-\frac{1}{2}(L_q - M_{q,k})^T \Sigma^{-1}(L_q - M_{q,k})}$
  - Since N is independent from M_k:

Theorem (Theorem 1 of [1])

Template attacks guess the key as:

$$\hat{k} = \underset{k}{\operatorname{argmin}} \ \operatorname{tr}((L - M_k)^{\mathsf{T}} \Sigma^{-1}(L - M_k)).$$

A scalability problem!

Optimization

The guessed key can be carried out by [5, 3]:

$$\hat{k} = \underset{k}{\operatorname{argmin}} \sum_{x=0}^{2^n-1} n_x(\tilde{L}_x - \tilde{M}_{x,k})^{\mathsf{T}} \Sigma^{-1} (\tilde{L}_x - \tilde{M}_{x,k}) \ . \tag{1}$$

where:

- n_x is the number of times the message x is involved,
- $\tilde{L}_x$ is the average trace over all the traces corresponding to the same message x,
- $\tilde{M}_{x,k}$ is leakage model corresponding to the pair (x, k).
- $\Sigma = \frac{1}{N} L L^{\mathsf{T}} - \frac{1}{2^n} \tilde{M} \tilde{M}^{\mathsf{T}}$

Optimization

The guessed key can be carried out by [5, 3]:

$$\hat{k} = \underset{k}{\operatorname{argmin}} \sum_{x=0}^{2^n-1} n_x(\tilde{L}_x - \tilde{M}_{x,k})^{\mathsf{T}} \Sigma^{-1} (\tilde{L}_x - \tilde{M}_{x,k}) \ . \tag{1}$$

where:

- n_x is the number of times the message x is involved,
- $\tilde{L}_x$ is the average trace over all the traces corresponding to the same message x,
- $\tilde{M}_{x,k}$ is leakage model corresponding to the pair (x, k).
- $\Sigma = \frac{1}{N} L L^{\mathsf{T}} - \frac{1}{2^n} \tilde{M} \tilde{M}^{\mathsf{T}}$

The attack (1) is more efficient in terms of computation, and memory space, than the theorem 1, as soon as the number of traces Q is greater than the number of plaintexts involved in the leakage model (e.g., for *AES*, it is $Q > 2^n = 256$).

State of the art = **coalescence**: replace n_x by $1/2^n$, $\forall x \in \{0, \ldots, 2^n - 1\}$.

Obviously, this is untrue, because traces are acquired one-by-one, hence one cannot make the assumption that every class is equally populated!

To compute (1) without using the approximation by the LLN, contrary to the state of the art, one can consider:

Proposition (Exact Template Attack – Expression of the Maximum Likelihood Distinguisher)

$$\hat{k} = \operatorname*{argmin}_k \sum_{x=0}^{2^n-1} n_x \tilde{M}_{x\oplus k}^{\mathsf{T}} \Sigma^{-1} \tilde{M}_{x\oplus k} - 2 \sum_{x=0}^{2^n-1} (n_x \tilde{L}_x^{\mathsf{T}})(\Sigma^{-1} \tilde{M}_{x\oplus k}) \ .$$

Spectral expression

Recalling that, for any pair of pseudo-Boolean functions f and g, we have:

$$\sum_{x=0}^{2^n-1} f(x).g(x \oplus k) = (f \otimes g)(k) = WHT(WHT(f) \bullet WHT(g))(k),$$

where

1. "$\bullet$" denotes the direct product between two pseudo-Boolean functions (that is, the term-to-term product),
2. "$\otimes$" denotes the convolution product between two pseudo-Boolean functions,
3. WHT denotes the Walsh-Hadamard Transform.

$$WHT(f)(u) = \sum_x (-1)^{u \cdot x} f(x).$$

Spectral expression

$$\begin{aligned}
\hat{k} &= \operatorname*{argmin}_k \sum_{x=0}^{2^n-1} n_x \tilde{M}^{\mathsf{T}}_{x\oplus k} \Sigma^{-1} \tilde{M}_{x\oplus k} - 2\sum_{x=0}^{2^n-1} (n_x \tilde{L}^{\mathsf{T}}_x)(\Sigma^{-1} \tilde{M}_{x\oplus k}) \\
&= \operatorname*{argmin}_k \; n(.) \otimes \mathscr{M}(.)(k) - 2\sum_{u=1}^{D} L_{cumul}[u] \otimes \tilde{\mathbb{M}}[u](k) \\
&= \operatorname*{argmin}_k \; WHT\Big[WHT(n) \bullet WHT(\mathscr{M}) - 2\sum_{u=1}^{D} WHT(L_{cumul}[u]) \bullet WHT(\tilde{\mathbb{M}}[u])\Big](k).
\end{aligned}$$

Spectral expression

$$\hat{k} = \underset{k}{\operatorname{argmin}} \sum_{x=0}^{2^n-1} n_x \tilde{M}_{x\oplus k}^{\mathsf{T}} \Sigma^{-1} \tilde{M}_{x\oplus k} - 2 \sum_{x=0}^{2^n-1} (n_x \tilde{L}_x^{\mathsf{T}})(\Sigma^{-1} \tilde{M}_{x\oplus k})$$

$$= \underset{k}{\operatorname{argmin}}\ n(.) \otimes \mathscr{M}(.)(k) - 2 \sum_{u=1}^{D} L_{cumul}[u] \otimes \tilde{\mathbb{M}}[u](k)$$

$$= \underset{k}{\operatorname{argmin}}\ WHT\left[WHT(n) \bullet WHT(\mathscr{M}) - 2 \sum_{u=1}^{D} WHT(L_{cumul}[u]) \bullet WHT(\tilde{\mathbb{M}}[u]) \right](k).$$

So, we can carry out an exact template attack, by pre-processing $WHT(\mathscr{M})$, $WHT(\tilde{\mathbb{M}}[u])$ (for each u value), during the profiling phase, then guessing the key $\hat{k}$ accordingly.

Results and experimental validation

- We employed raw traces from the SCA database (ASCAD) of the French National Agency for Information Systems Security (ANSSI) [2].

Results and experimental validation

- We employed raw traces from the SCA database (ASCAD) of the French National Agency for Information Systems Security (ANSSI) [2].
- The encryption algorithm target is a protected software implementation of AES running on an $\mathrm{ATMEGA\text{-}8515}$ μ-processor.

Results and experimental validation

- We employed raw traces from the SCA database (ASCAD) of the French National Agency for Information Systems Security (ANSSI) [2].
- The encryption algorithm target is a protected software implementation of AES running on an $\mathrm{ATMEGA\text{-}8515}$ μ-processor.
- The target variable is $Z = \mathrm{SBox}(x[2] \oplus k[2])$.

Results and experimental validation: Success rate /#traces

Blue = coalescence – red = our approach.

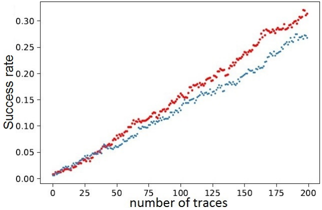


Figure: $D = 2$

Results and experimental validation: Success rate /#traces

Blue = coalescence – red = our approach.

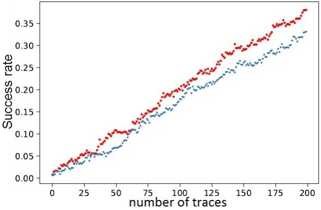


Figure: $D = 3$

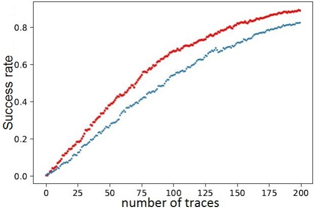


Figure: $D = 4$

Results and experimental validation: Success rate /#traces

Blue = coalescence – red = our approach.

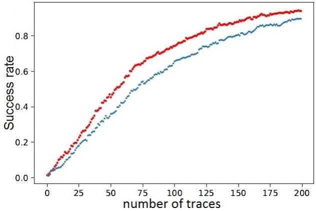


Figure: $D = 5$

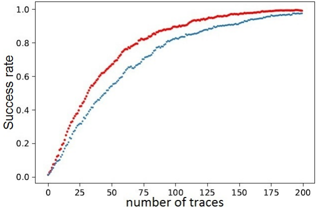


Figure: $D = 10$

Results and experimental validation: Success rate /#traces

Blue = coalescence – red = our approach.

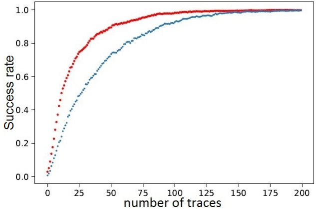


Figure: $D = 20$

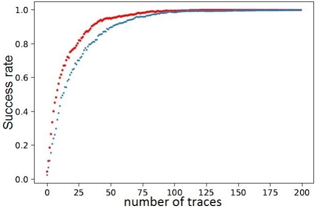
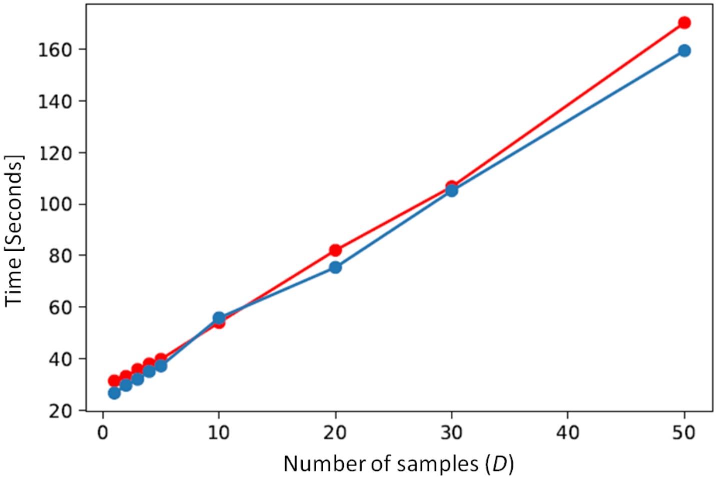


Figure: $D = 50$

Results and experimental validation: Computation time



Conclusions and perspectives

Conclusions:

- New improvement in template attacks' success rate, by not using coalescence;

Conclusions and perspectives

Conclusions:

- New improvement in template attacks' success rate, by not using coalescence;
- At the same time, computational complexity is reduced thanks to a spectral computation;

Conclusions and perspectives

Conclusions:

- New improvement in template attacks' success rate, by not using coalescence;
- At the same time, computational complexity is reduced thanks to a spectral computation;
- A quasilinear instead of a quadratic time complexity (32x faster);

Conclusions and perspectives

Conclusions:

- New improvement in template attacks' success rate, by not using coalescence;
- At the same time, computational complexity is reduced thanks to a spectral computation;
- A quasilinear instead of a quadratic time complexity (32x faster);
- Can be applied to any algorithms that involve SBox whose input is the *XOR*;

Conclusions and perspectives

Conclusions:

- New improvement in template attacks' success rate, by not using coalescence;
- At the same time, computational complexity is reduced thanks to a spectral computation;
- A quasilinear instead of a quadratic time complexity (32x faster);
- Can be applied to any algorithms that involve SBox whose input is the *XOR*;
- Considerable gain in success rate comes at the expense of a marginal loss in computation time, which is explained in terms of complexity.

Source code: https://github.com/SylvainGuilley/Exact_Template_Attacks_With_Spectral_Computation/tree/master

Perspectives:

- How these improvements behave with countermeasures?

Conclusions and perspectives

Perspectives:

- How these improvements behave with countermeasures?
- This approach should be extended to the Linear Regression Analysis (LRA) in [4].

Thank you for your attention

Nicolas Bruneau, Sylvain Guilley, Annelie Heuser, Damien Marion, and Olivier Rioul.
Optimal side-channel attacks for multivariate leakages and multiple models.
J. Cryptographic Engineering, 7(4):331–341, 2017.

Prouff Emmanuel, Strullu Remi, Benadjila Ryad, Cagli Eleonora, and Dumas Cecile.
Study of deep learning techniques for side-channel analysis and introduction to ascad database.
CoRR, pages 1–45, 2018.

Maamar Ouladj and Sylvain Guilley.
Side-Channel Analysis of Embedded Systems.
Springer, 2021.
ISBN: 978-3-030-77221-5.

Maamar Ouladj, Sylvain Guilley, and Emmanuel Prouff.
On the implementation efficiency of linear regression-based side-channel attacks.

In *Constructive Side-Channel Analysis and Secure Design - 11th International Workshop, COSADE 2020, Lugano, Switzerland, October 5-7, 2020, Proceedings (LNCS 12244)*, pages 147–172, 2020.

Maamar Ouladj, Nadia El Mrabet, Sylvain Guilley, Philippe Guillot, and Gilles Millérioux.
On the power of template attacks in highly multivariate context.
Journal of Cryptographic Engineering - JCEN, 2020.