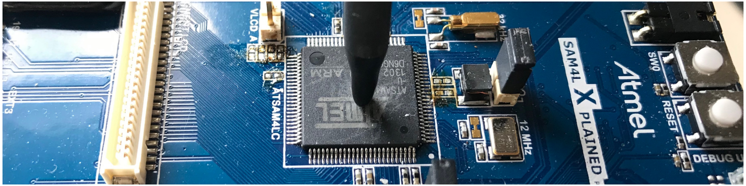


Side-channel Analysis of Cryptographic Implementations

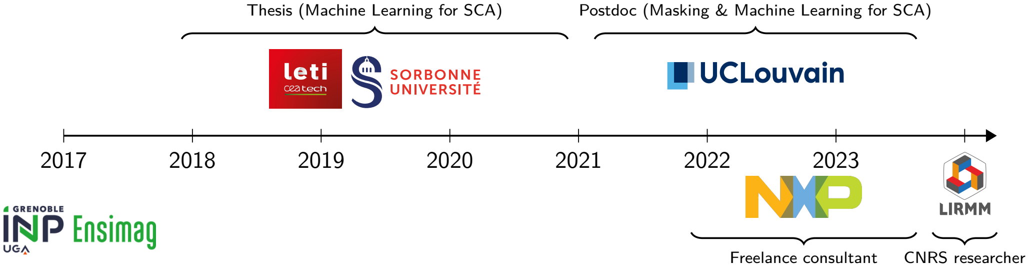
Evaluation & Counter-Measures

Loïc Masure (loic.masure@lirmm.fr)

Forum InCyber, 1 Avril 2025

cnrs LIRMM UNIVERSITÉ DE MONTPELLIER

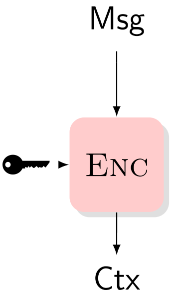
Who am I?


Thesis (Machine Learning for SCA)
Postdoc (Masking & Machine Learning for SCA)
leti
ceatech
SORBONNE UNIVERSITÉ
UCLouvain
2017
2018
2019
2020
2021
2022
2023
GRENOBLE INP UGA Ensimag
LIRMM
Freelance consultant
CNRS researcher

Agenda

Content

Context : Side-Channel Analysis (SCA)

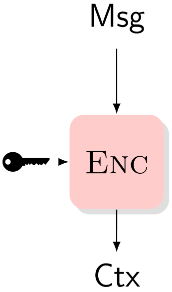


🔑: N bits ($\frac{N}{n}$ chunks of $n \ll N$ bits)

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

"Cryptographic algorithms don't run on paper,

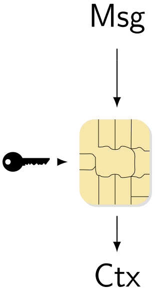


: N bits ($\frac{N}{n}$ chunks of $n \ll N$ bits)

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

"Cryptographic algorithms don't run on paper, they run on physical devices"

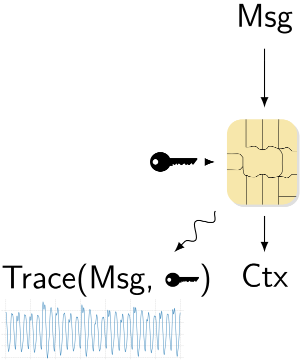


🔑: N bits ($\frac{N}{n}$ chunks of $n \ll N$ bits)

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

"Cryptographic algorithms don't run on paper, they run on physical devices"

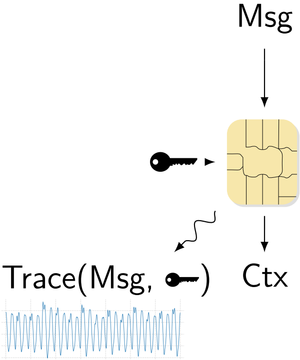


: N bits ($\frac{N}{n}$ chunks of $n \ll N$ bits)

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

"Cryptographic algorithms don't run on paper, they run on physical devices"

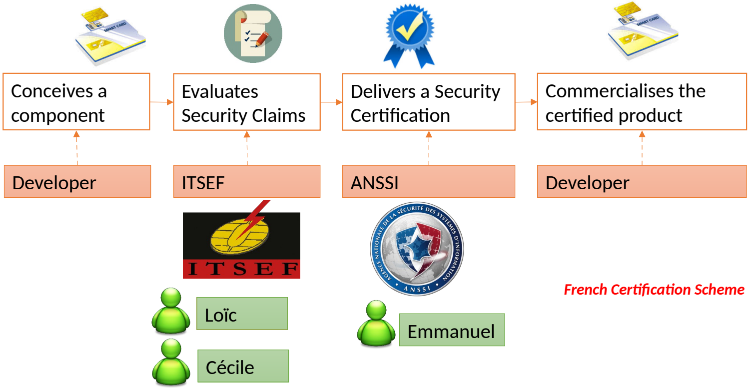


: N bits ($\frac{N}{n}$ chunks of $n \ll N$ bits)

Black-box cryptanalysis: 2^N
Divide-and-conquer: $2^n \cdot \frac{N}{n}$
$\approx$ "quantum" break

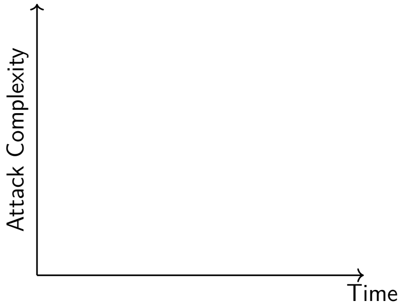
Content

Certification against SCA



Security graded w.r.t. attack complexity in terms of human, material, and financial means

Evaluate Security against Side-Channel Attacks

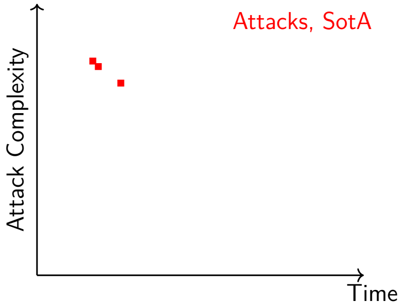


a

Attack approach (industry):

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks

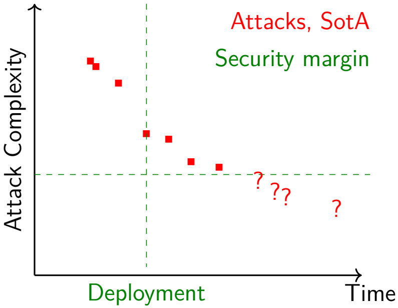


a

Attack approach (industry):
Current security level ✓

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



[a]

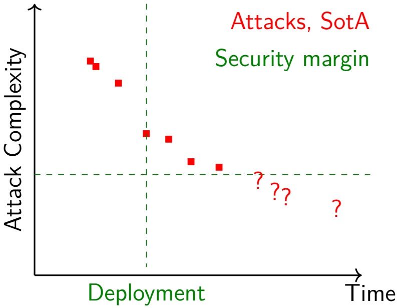
Attack approach (industry):

Current security level ✓

Certification & deployment 

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



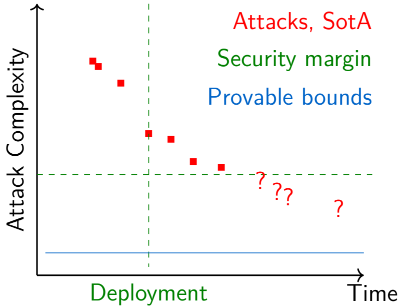
[a]

Attack approach (industry):

- Current security level ✓
- Certification & deployment
- Future improvement → reevaluation ✗

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



[a]

Attack approach (industry):

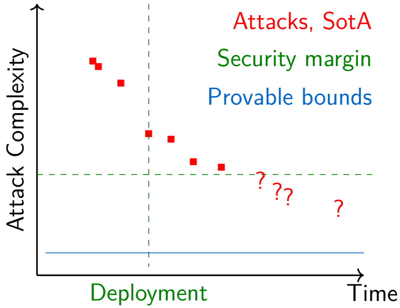
- Current security level ✓
- Certification & deployment
- Future improvement → reevaluation ✗

Approach by *proofs* (academia):

- Rigorous approach ✓
- Potentially conservative ✗

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



[a]

Attack approach (industry):

- Current security level ✓
- Certification & deployment
- Future improvement → reevaluation ✗

Approach by *proofs* (academia):

- Rigorous approach ✓
- Potentially conservative ✗

[a]Shamelessly stolen to O. Bronchain

Today's agenda: evaluation by proofs

Content

How to Evaluate Efficiently?

A good *evaluator* $\mathcal{E} \neq$ A good *adversary* $\mathcal{A}$

Security level:

- Design-dependent ✓

How to Evaluate Efficiently?

A good *evaluator* $\mathcal{E} \neq$ A good *adversary* $\mathcal{A}$

Security level:

- Design-dependent ✓
- Device-dependent ✓

How to Evaluate Efficiently?

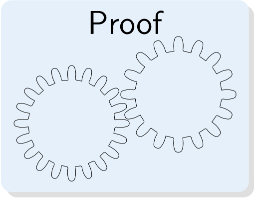
A good *evaluator* $\mathcal{E} \neq$ A good *adversary* $\mathcal{A}$

Security level:

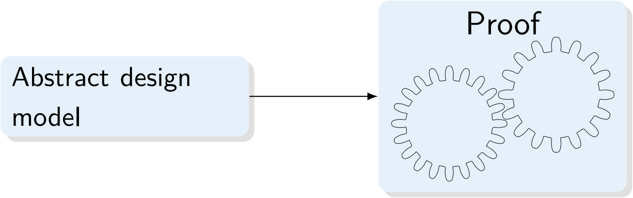
- Design-dependent ✓
- Device-dependent ✓
- Adversary-dependent ✗

How to deal with this problem space?

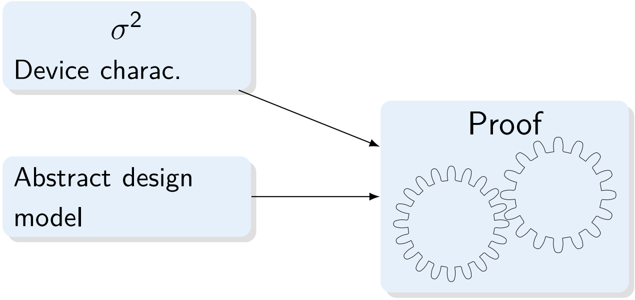
Security Proofs



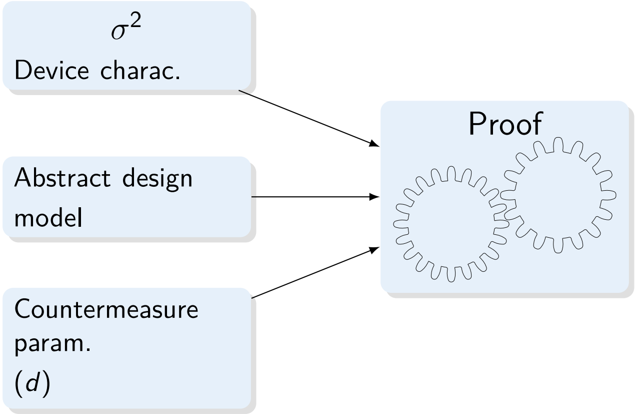
Security Proofs



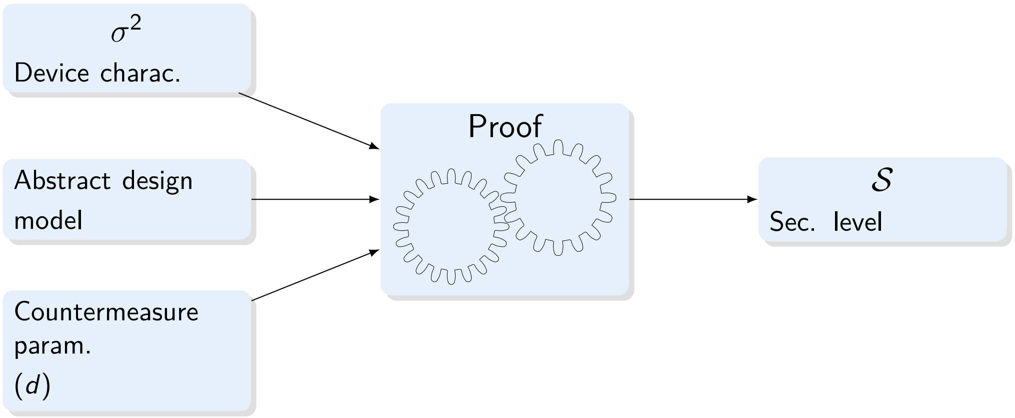
Security Proofs



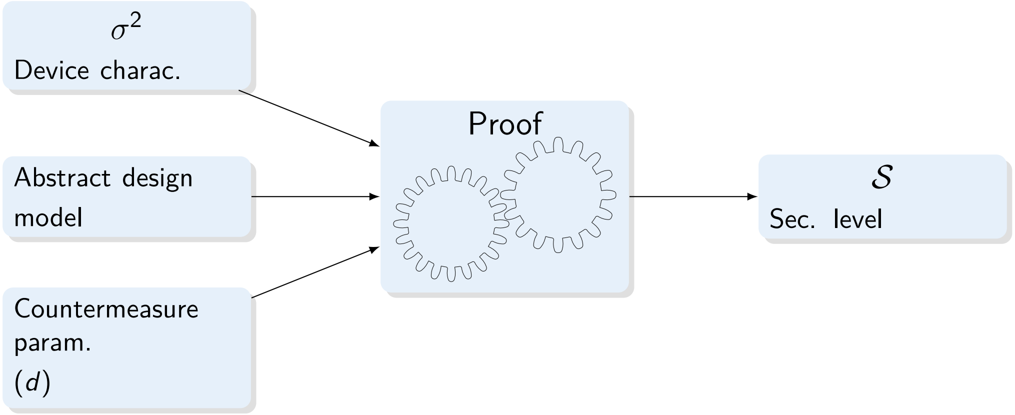
Security Proofs



Security Proofs



Security Proofs



"Any SCA attack requires at least $\mathcal{S}$ queries"

Main Ingredient: Security Reductions

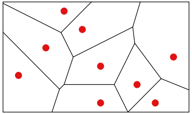


Figure: The set of all possible attacks : (adversary, leakages).

Reduction: "any attack from a given class is less powerful than the red-dot attack of the region".

Main Ingredient: Security Reductions

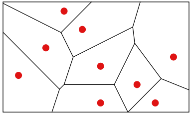


Figure: The set of all possible attacks : (adversary, leakages).

Reduction: "any attack from a given class is less powerful than the red-dot attack of the region".

Data-processing inequality & Simulatability: If two attacks $\mathcal{A}, \mathcal{B}$ are such that $\mathcal{A} = \mathcal{S}(\mathcal{B})$, then $\mathit{Success}(\mathcal{A}) \leq \mathit{Success}(\mathcal{B})$. Hence,

$$\max_{\mathcal{A} \in \mathcal{A}} \mathit{Success}(\mathcal{A}) \leq \max_{\mathcal{B} \in \mathcal{S}(\mathcal{A})} \mathit{Success}(\mathcal{B}).$$

Content

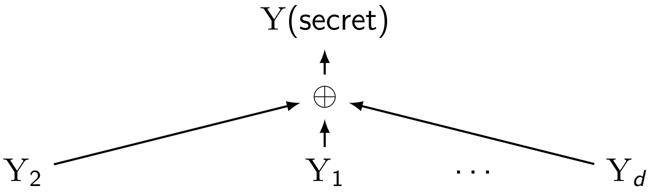
Masking: what is that ?

Masking, a.k.a. *MPC on silicon*:[12] secret sharing over a finite field $(\mathbb{F}, \oplus, \otimes)$

$$\mathrm{Y}(\text{secret})$$

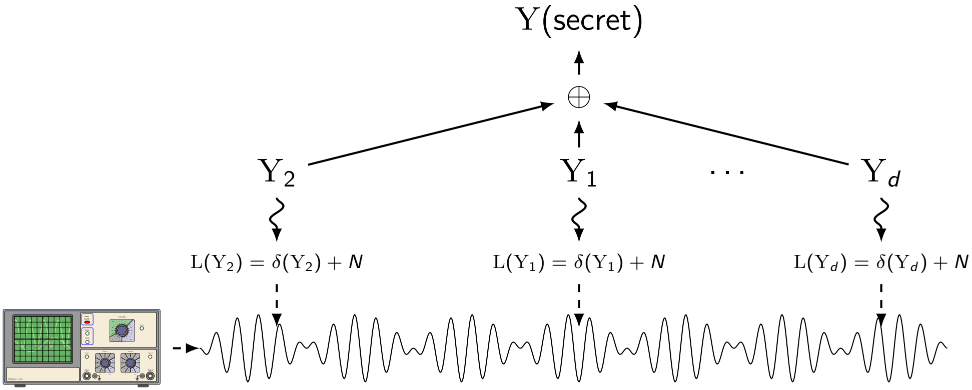
Masking: what is that ?

Masking, a.k.a. *MPC on silicon*:[12] secret sharing over a finite field $(\mathbb{F}, \oplus, \otimes)$



Masking: what is that ?

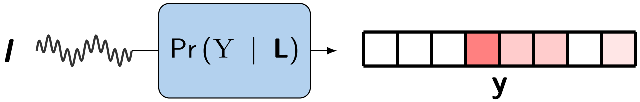
Masking, a.k.a. *MPC on silicon*:[1,2] secret sharing over a finite field $(\mathbb{F}, \oplus, \otimes)$



[1] Chari et al., "Towards Sound Approaches to Counteract Power-Analysis Attacks".
[2] Goubin and Patarin, "DES and Differential Power Analysis (The "Duplication" Method)".

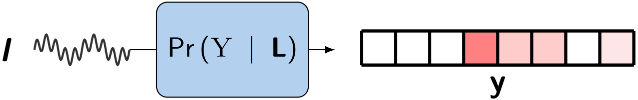
The Noisy Leakage Model

In this model, for each intermediate computation, the adversary gets a probability distribution about its operands:

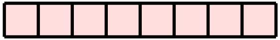


The Noisy Leakage Model

In this model, for each intermediate computation, the adversary gets a probability distribution about its operands:

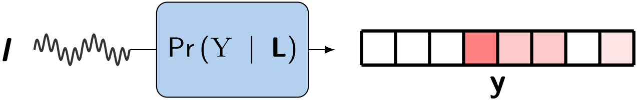


If, the adversary gets:

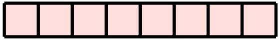


The Noisy Leakage Model

In this model, for each intermediate computation, the adversary gets a probability distribution about its operands:



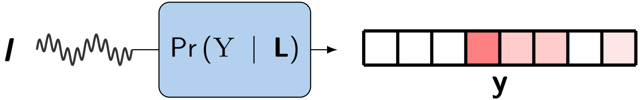
If, the adversary gets:



Very noisy
Sensitive computation unpredictable

The Noisy Leakage Model

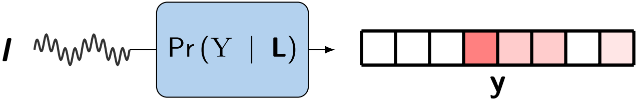
In this model, for each intermediate computation, the adversary gets a probability distribution about its operands:



If, the adversary gets:

The Noisy Leakage Model

In this model, for each intermediate computation, the adversary gets a probability distribution about its operands:



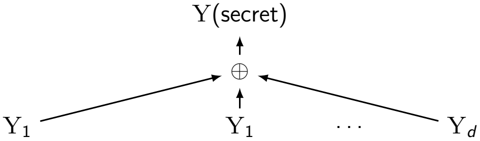
If, the adversary gets:

Low-noise
Exact prediction of the sensitive computation

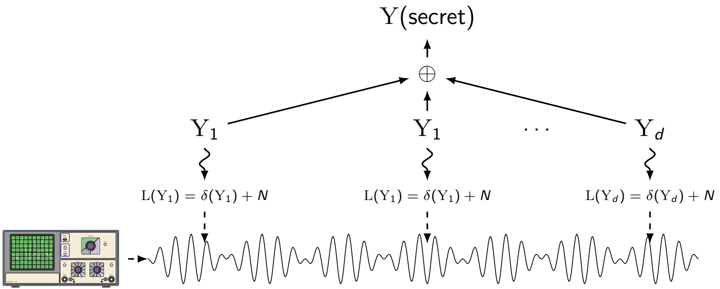
The Effect of Masking

Y(secret)

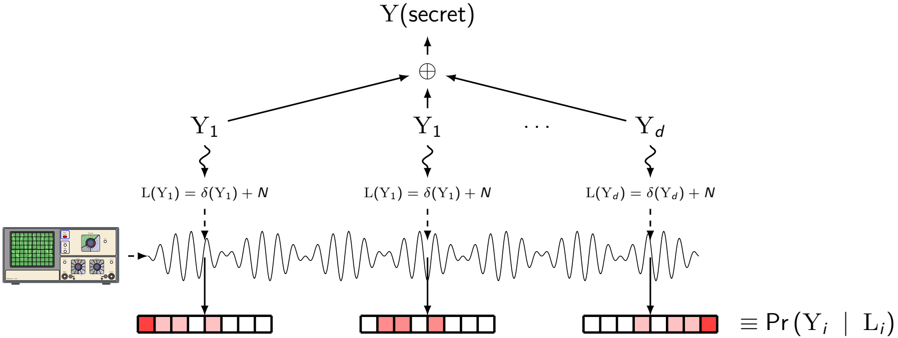
The Effect of Masking



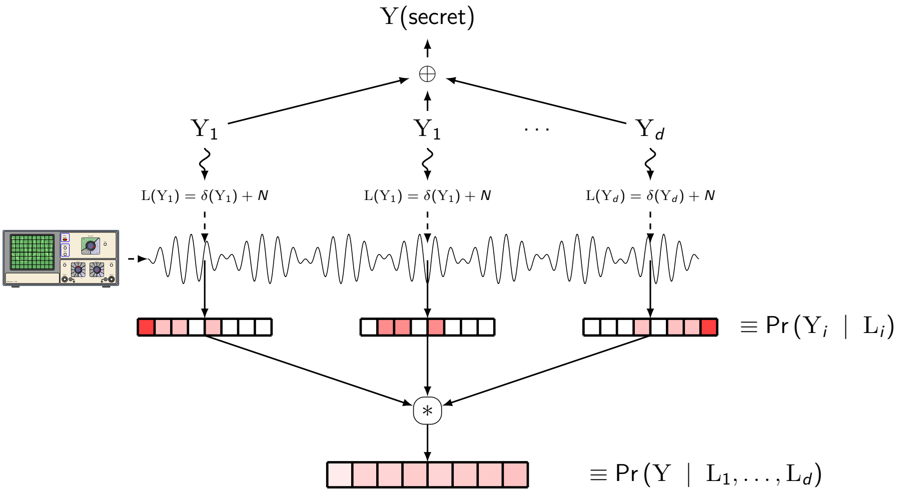
The Effect of Masking



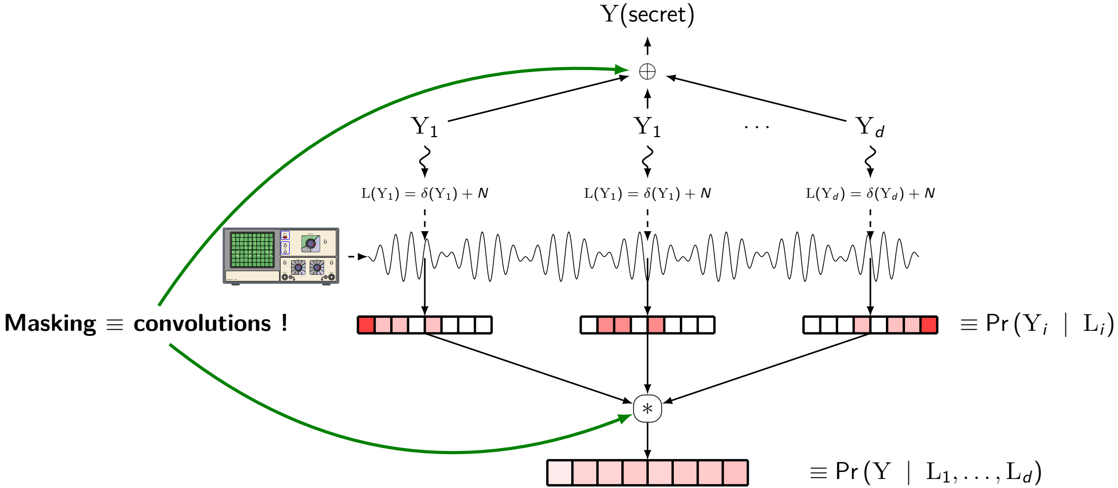
The Effect of Masking



The Effect of Masking



The Effect of Masking



Convolution = Noise Amplification

Simulation, for $\mathbb{F}_{2^n}$: $L(Y_i) = hw(Y_i) + \mathcal{N}(0; \sigma^2)$, hw = Hamming weight

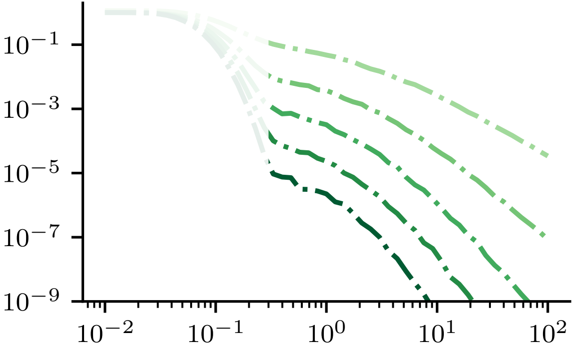
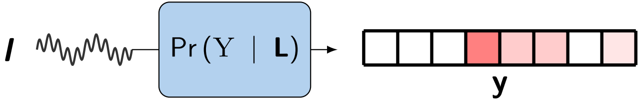


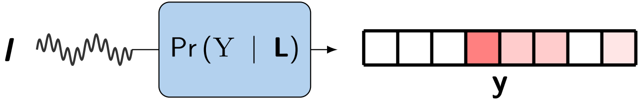
Figure: $\mathrm{MI}\left(\mathrm{Y}; \mathbf{L}\right)$ vs. σ^2, $2 \leq d \leq 6$

Content

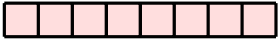
Recall on Noisy Leakage Model



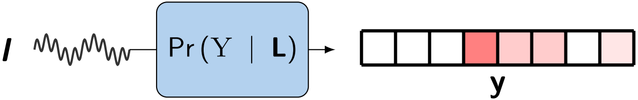
Recall on Noisy Leakage Model



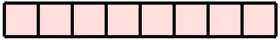
If, the adversary gets:



Recall on Noisy Leakage Model

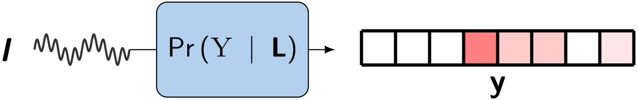


If, the adversary gets:



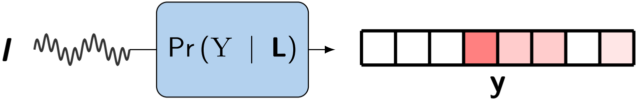
Very noisy leakage
Y indistinguishable from blind guess

Recall on Noisy Leakage Model

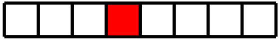


If, the adversary gets:

Recall on Noisy Leakage Model



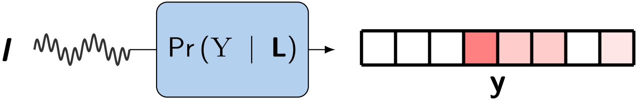
If, the adversary gets:



Low-noise leakage

Exact prediction for Y

Recall on Noisy Leakage Model



δ-noisy adversary

Any intermediate computation Y leaks $\mathrm{L}(\mathrm{Y})$ such that:

$$\mathsf{SD}(\mathrm{Y};\mathrm{L}) = \mathop{\mathbb{E}}_{\mathrm{L}}\left[TV\left(\underbrace{\cdots}_{\Pr(\mathrm{Y} \mid \mathrm{L})}, \underbrace{\cdots}_{\Pr(\mathrm{Y})} \right) \right] \leq \delta$$

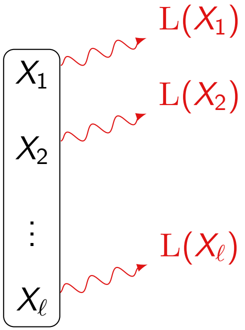
Security Proof for a Circuit

Consider a circuit with ℓ intermediate computations:

$$\begin{pmatrix} X_1 \\ X_2 \\ \vdots \\ X_\ell \end{pmatrix}$$

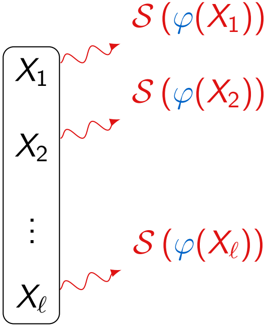
Security Proof for a Circuit

Consider a circuit with ℓ δ-noisy intermediate computations:



Security Proof for a Circuit

Consider a circuit with ℓ δ-noisy intermediate computations:



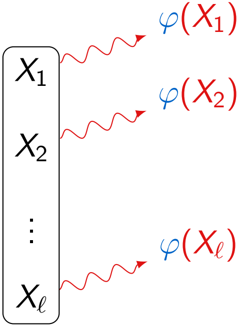
LEMMA (SIMULATABILITY)

The leakage function L *can be simulated from a random probing adversary:* $\varphi(x)$ *exactly reveals* x *with probability* $\epsilon = 1 - \sum_l \min_x \Pr(\mathrm{L}(x) = l) \leq \delta \cdot |\mathbb{F}|$.[a]

[a] Duc, Dziembowski, and Faust, "Unifying Leakage Models: From Probing Attacks to Noisy Leakage".

Security Proof for a Circuit

Consider a circuit with ℓ δ-noisy intermediate computations:



We may reduce to an adversary observing $\varphi(X)$ instead of $\mathcal{S}(\varphi(X))$ (Data Processing Inequality)

Security against a Random Probing Adversary

To succeed, at least d out of ℓ wires must be revealed to the adversary:

$$\Pr(\text{Adv. learns sth}) \leq \Pr(\text{At least } d \text{ wires revealed})$$

[3]Boucheron, Lugosi, and Massart, *Concentration Inequalities: A Nonasymptotic Theory of Independence*, P.24, and Ex. 2.11.

Security against a Random Probing Adversary

To succeed, at least d out of ℓ wires must be revealed to the adversary:

$$\Pr(\text{Adv. learns sth}) \leq \Pr(\text{At least } d \text{ wires revealed})$$

THEOREM (CHERNOFF CONCENTRATION INEQUALITY[3])

If ℓ wires, each independently revealed with proba. ϵ:

$$\Pr(\textit{At least } d \textit{ wires revealed}) \leq \left(\frac{e \cdot \ell \cdot \epsilon}{d}\right)^d$$

[3] Boucheron, Lugosi, and Massart, *Concentration Inequalities: A Nonasymptotic Theory of Independence*, P.24, and Ex. 2.11.

Putting all Together

In our context, $\ell \leq \mathcal{O}\left(d^2\right)$, and $\epsilon \leq \delta \cdot |\mathbb{F}|$:

Theorem (Security Bound)

For a single computation with $\ell \leq \mathcal{O}\left(d^2\right)$ gates:

$$\mathsf{SD}(k; \mathbf{L}) \leq (\mathcal{O}(d) \cdot \delta \cdot |\mathbb{F}|)^d$$

Putting all Together

In our context, $\ell \leq \mathcal{O}\left(d^2\right)$, and $\epsilon \leq \delta \cdot |\mathbb{F}|$:

Theorem (Security Bound)

For a single computation with $\ell \leq \mathcal{O}\left(d^2\right)$ gates:

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \left(\mathcal{O}\left(d\right) \cdot \delta \cdot |\mathbb{F}|\right)^d$$

For the whole circuit $\mathbb{C}$, (work in progress),

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \left(\mathcal{O}\left(|\mathbb{C}| d\right) \cdot \delta \cdot |\mathbb{F}|\right)^d$$

Putting all Together

In our context, $\ell \leq \mathcal{O}\left(d^2\right)$, and $\epsilon \leq \delta \cdot |\mathbb{F}|$:

Theorem (Security Bound)

For a single computation with $\ell \leq \mathcal{O}\left(d^2\right)$ gates:

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \left(\mathcal{O}\left(d\right) \cdot \delta \cdot |\mathbb{F}|\right)^d$$

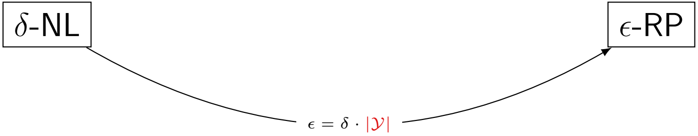
For the whole circuit $\mathbb{C}$, (work in progress),

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq |\mathbb{C}| \left(\mathcal{O}\left(d\right) \cdot \delta \cdot |\mathbb{F}|\right)^d$$

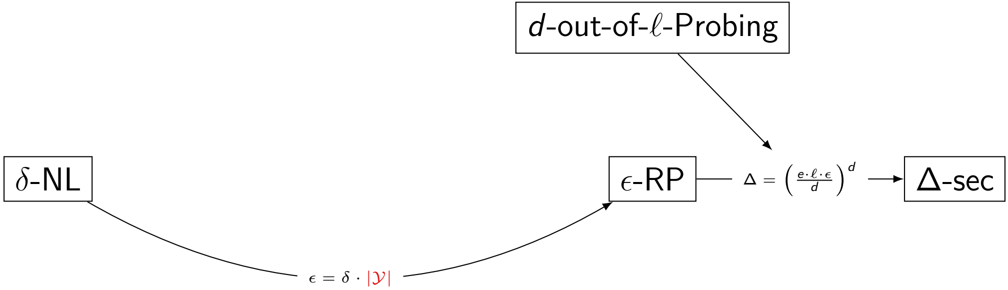
Wrap-Up of the Proof

δ-NL

Wrap-Up of the Proof



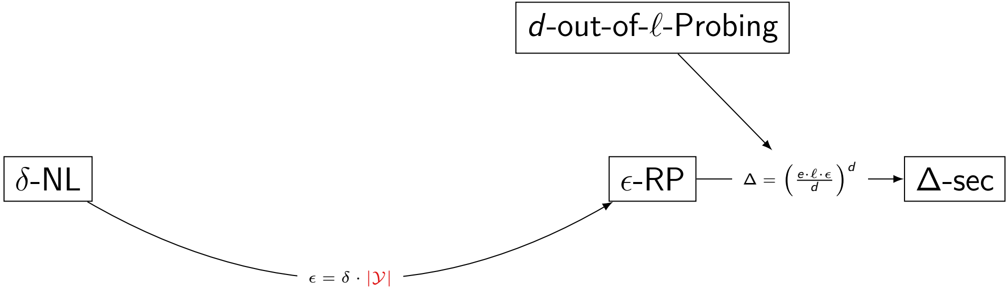
Wrap-Up of the Proof



[4] Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence".

Wrap-Up of the Proof

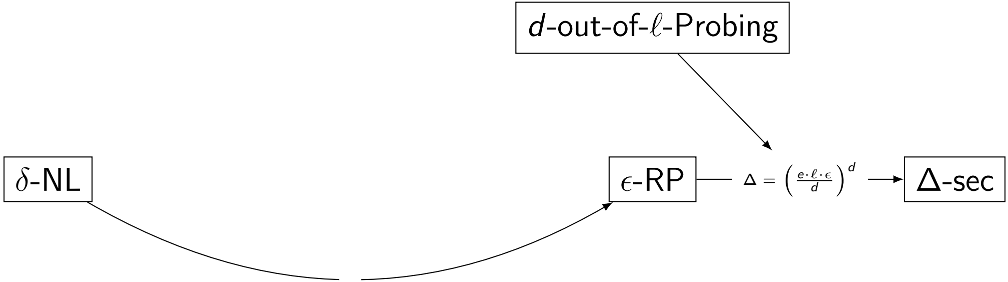
Bad *leakage rate* $\approx d \cdot |\mathbb{F}|$ ✗...



[4] Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence".

Wrap-Up of the Proof

Bad *leakage rate* $\approx d \cdot |\mathbb{F}|$ ✗... but new perspectives[4] ✓



[4] Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence".

Perspectives

- Improving the reduction from Noisy Leakages to Random Probing

[5] Belaïd, Rivain, and Taleb, "On the Power of Expansion: More Efficient Constructions in the Random Probing Model".

Perspectives

- Improving the reduction from Noisy Leakages to Random Probing
- New constructions with leakage rates indep. of d[5]

[5] Belaïd, Rivain, and Taleb, “On the Power of Expansion: More Efficient Constructions in the Random Probing Model”.

Perspectives

- Improving the reduction from Noisy Leakages to Random Probing
- New constructions with leakage rates indep. of d[5]
- Masking PQC, *e.g.*, Kyber:

[5]Belaïd, Rivain, and Taleb, "On the Power of Expansion: More Efficient Constructions in the Random Probing Model".

Perspectives

- Improving the reduction from Noisy Leakages to Random Probing
- New constructions with leakage rates indep. of d[5]
- Masking PQC, *e.g.*, Kyber:
  - ⋆ Unefficient masking through decomposition into circuit ✗

[5] Belaïd, Rivain, and Taleb, "On the Power of Expansion: More Efficient Constructions in the Random Probing Model".

Perspectives

- Improving the reduction from Noisy Leakages to Random Probing
- New constructions with leakage rates indep. of d[5]
- Masking PQC, *e.g.*, Kyber:
  - ⋆ Unefficient masking through decomposition into circuit ✗
  - ⋆ Needs bigger gadgets with other paradigm: pre-computation tables ✓

[5] Belaïd, Rivain, and Taleb, "On the Power of Expansion: More Efficient Constructions in the Random Probing Model".

Perspectives

- Improving the reduction from Noisy Leakages to Random Probing
- New constructions with leakage rates indep. of d[5]
- Masking PQC, *e.g.*, Kyber:
  - ⋆ Unefficient masking through decomposition into circuit ✗
  - ⋆ Needs bigger gadgets with other paradigm: pre-computation tables ✓
    $\Longrightarrow$ wider gap between d-probing and ϵ-RP ✗

[5] Belaïd, Rivain, and Taleb, "On the Power of Expansion: More Efficient Constructions in the Random Probing Model".

Perspectives

- Improving the reduction from Noisy Leakages to Random Probing
- New constructions with leakage rates indep. of d[5]
- Masking PQC, *e.g.*, Kyber:
  - ⋆ Unefficient masking through decomposition into circuit ✗
  - ⋆ Needs bigger gadgets with other paradigm: pre-computation tables ✓
    $\implies$ wider gap between d-probing and ϵ-RP ✗
  - ⋆ Masking-friendly schemes, *e.g.*, Raccoon ? ✓

[5] Belaïd, Rivain, and Taleb, "On the Power of Expansion: More Efficient Constructions in the Random Probing Model".

References I

Belaïd, S., M. Rivain, and A. R. Taleb. "On the Power of Expansion: More Efficient Constructions in the Random Probing Model". In: *Advances in Cryptology - EUROCRYPT 2021 - 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17-21, 2021, Proceedings, Part II*. Ed. by A. Canteaut and F. Standaert. Vol. 12697. Lecture Notes in Computer Science. Springer, 2021, pp. 313–343. DOI: 10.1007/978-3-030-77886-6_11. URL: https://doi.org/10.1007/978-3-030-77886-6_11.

Boucheron, S., G. Lugosi, and P. Massart. *Concentration Inequalities: A Nonasymptotic Theory of Independence*. Oxford University Press, 2013. ISBN: 9780191747106. URL: https://books.google.fr/books?id=O3yoAQAACAAJ.

References II

Brian, G., S. Dziembowski, and S. Faust. “From Random Probing to Noisy Leakages Without Field-Size Dependence”. In: *Advances in Cryptology - EUROCRYPT 2024 - 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zurich, Switzerland, May 26-30, 2024, Proceedings, Part IV*. Ed. by M. Joye and G. Leander. Vol. 14654. Lecture Notes in Computer Science. Springer, 2024, pp. 345–374. DOI: 10.1007/978-3-031-58737-5_13. URL: https://doi.org/10.1007/978-3-031-58737-5_13.

References III

Chari, S. et al. "Towards Sound Approaches to Counteract Power-Analysis Attacks". In: *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*. Ed. by M. J. Wiener. Vol. 1666. Lecture Notes in Computer Science. Springer, 1999, pp. 398–412. ISBN: 3-540-66347-9. DOI: 10.1007/3-540-48405-1_26. URL: https://doi.org/10.1007/3-540-48405-1_26.

Duc, A., S. Dziembowski, and S. Faust. "Unifying Leakage Models: From Probing Attacks to Noisy Leakage". In: *J. Cryptology* 32.1 (2019), pp. 151–177. DOI: 10.1007/s00145-018-9284-1. URL: https://doi.org/10.1007/s00145-018-9284-1.

References IV

Goubin, L. and J. Patarin. "DES and Differential Power Analysis (The "Duplication" Method)". In: *Cryptographic Hardware and Embedded Systems, First International Workshop, CHES'99, Worcester, MA, USA, August 12-13, 1999, Proceedings*. Ed. by Ç. K. Koç and C. Paar. Vol. 1717. Lecture Notes in Computer Science. Springer, 1999, pp. 158–172. DOI: 10.1007/3-540-48059-5_15. URL: https://doi.org/10.1007/3-540-48059-5_15.