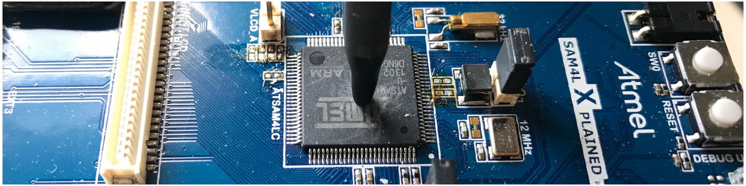


Prouff & Rivain's Security Proof of Masking, Revisited

Tight Bounds in the Noisy Leakage Model

Loïc Masure   François-Xavier Standaert

CRYPTO 2023, Santa Barbara, August 21st

https://eprint.iacr.org/2023/883

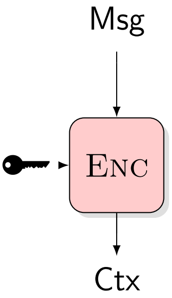
European Research Council
Established by the European Commission

GROUPE CRYPTO

UCLouvain

Table of Contents

Context : Side-Channel Analysis (SCA)

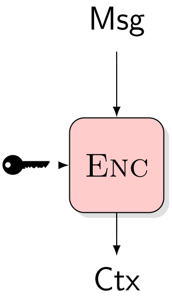


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

"Cryptographic algorithms don't run on paper,

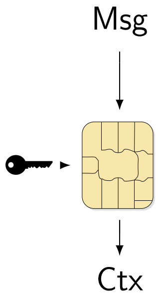


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

“Cryptographic algorithms don’t run on paper, they run on physical devices”

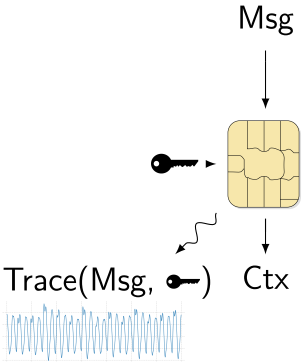


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

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



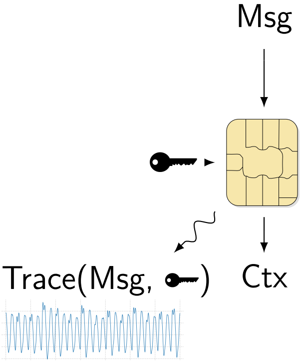
: N bits

Black-box cryptanalysis: 2^N

Trace : power, EM, acoustics, runtime, . . .

Context : Side-Channel Analysis (SCA)

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



: N bits

Black-box cryptanalysis: 2^N

Side-Channel Analysis: $2^n \cdot \frac{N}{n}, n \ll N$

Trace : power, EM, acoustics, runtime, ...

The Counter-Measure: Masking

Masking, aka *MPC on silicon*: linear secret sharing over a finite field $(\mathbb{F}, \star, \cdot)$

Y (secret)

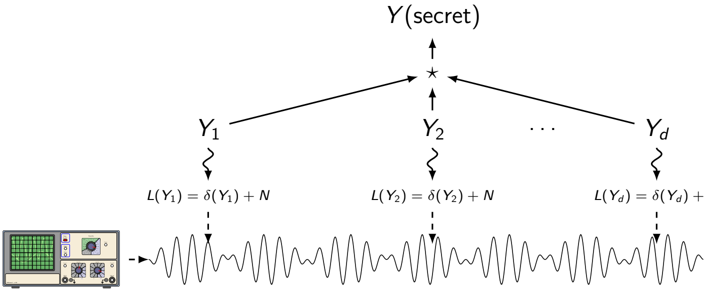
The Counter-Measure: Masking

Masking, aka *MPC on silicon*: linear secret sharing over a finite field $(\mathbb{F}, \star, \cdot)$

$$\begin{tikzcd}
 & & Y\,(\text{secret}) & & \\
 & & \star \arrow[u] & & \\
Y_1 \arrow[urr] & & Y_2 \arrow[u] & \cdots & Y_d \arrow[ull]
\end{tikzcd}$$

The Counter-Measure: Masking

Masking, aka *MPC on silicon*: linear secret sharing over a finite field $(\mathbb{F}, \star, \cdot)$



Masking amplifies noise [1]

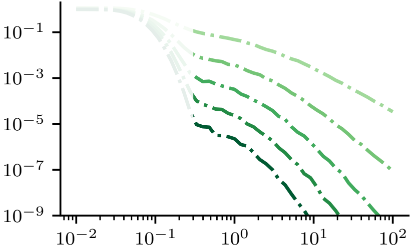


Figure: $\mathrm{MI}(Y; Trace)$ vs. σ^2, $2 \leq d \leq 6$

Cst gap between each curve (log scale)

$\iff$

exponential security w.r.t. #shares d

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

[1] Chari et al., "Towards Sound Approaches to Counteract Power-Analysis Attacks"

Masking amplifies noise [1]

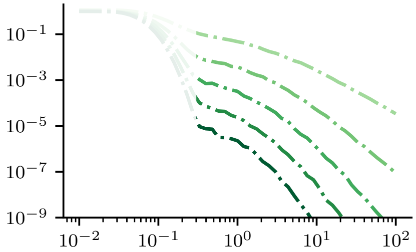
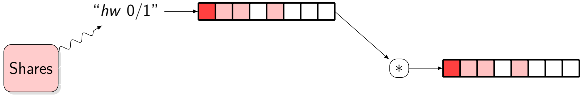


Figure: MI $(Y; Trace)$ vs. σ^2, $2 \leq d \leq 6$

Explanation: Masking $\iff$ convolution



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

[1] Chari et al., "Towards Sound Approaches to Counteract Power-Analysis Attacks"

Masking amplifies noise [1]

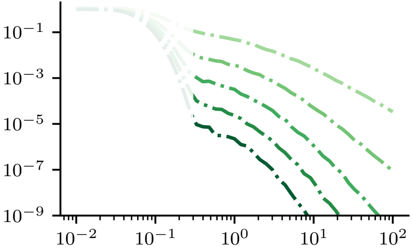
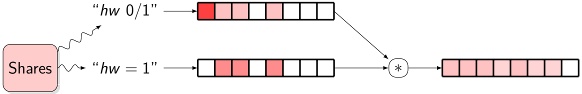


Figure: MI $(Y; Trace)$ vs. σ^2, $2 \leq d \leq 6$

Explanation: Masking $\Longleftrightarrow$ convolution



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

[1] Chari et al., "Towards Sound Approaches to Counteract Power-Analysis Attacks"

Masking amplifies noise [1]

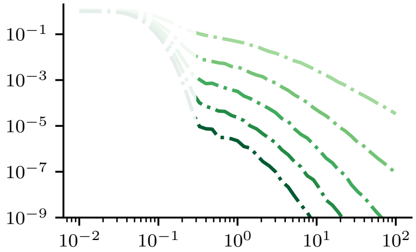
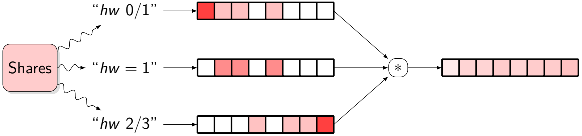


Figure: MI $(Y; Trace)$ vs. σ^2, $2 \leq d \leq 6$

Explanation: Masking $\iff$ convolution



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

[1] Chari et al., “Towards Sound Approaches to Counteract Power-Analysis Attacks”

Leakage from encoding $\longrightarrow$ leakage from computations

So far we have considered one secret leaking from one encoding ...

[2] Ishai, Sahai, and Wagner, "Private Circuits: Securing Hardware against Probing Attacks"; Rivain and Prouff, "Provably Secure Higher-Order Masking of AES"

Leakage from encoding $\longrightarrow$ leakage from computations

So far we have considered one secret leaking from one encoding ...
Actually, secrets processed by (leaky) computations $\implies$ **masking scheme**

[2] Ishai, Sahai, and Wagner, "Private Circuits: Securing Hardware against Probing Attacks"; Rivain and Prouff, "Provably Secure Higher-Order Masking of AES"

Leakage from encoding $\longrightarrow$ leakage from computations

So far we have considered one secret leaking from one encoding . . .
Actually, secrets processed by (leaky) computations $\implies$ **masking scheme**

Rivain-Prouff / I.S.W. scheme [2]

[2] Ishai, Sahai, and Wagner, "Private Circuits: Securing Hardware against Probing Attacks"; Rivain and Prouff, "Provably Secure Higher-Order Masking of AES"

Leakage from encoding $\longrightarrow$ leakage from computations

So far we have considered one secret leaking from one encoding . . .
Actually, secrets processed by (leaky) computations $\implies$ **masking scheme**

Rivain-Prouff / I.S.W. scheme [2]

- Linear operations: trivial shared computation

[2] Ishai, Sahai, and Wagner, "Private Circuits: Securing Hardware against Probing Attacks"; Rivain and Prouff, "Provably Secure Higher-Order Masking of AES"

Leakage from encoding $\longrightarrow$ leakage from computations

So far we have considered one secret leaking from one encoding ...
Actually, secrets processed by (leaky) computations $\Longrightarrow$ **masking scheme**

Rivain-Prouff / I.S.W. scheme [2]

- Linear operations: trivial shared computation
- Non-linear (Sbox): polynomial interpolation

[2] Ishai, Sahai, and Wagner, "Private Circuits: Securing Hardware against Probing Attacks"; Rivain and Prouff, "Provably Secure Higher-Order Masking of AES"

Leakage from encoding $\longrightarrow$ leakage from computations

So far we have considered one secret leaking from one encoding ...
Actually, secrets processed by (leaky) computations $\Longrightarrow$ **masking scheme**

Rivain-Prouff / I.S.W. scheme [2]

- Linear operations: trivial shared computation
- Non-linear (Sbox): polynomial interpolation

$\to$ Sequence of (linear) additions and multiplications

[2] Ishai, Sahai, and Wagner, "Private Circuits: Securing Hardware against Probing Attacks"; Rivain and Prouff, "Provably Secure Higher-Order Masking of AES"

Multiplication over secret sharing

A

B

Multiplication over secret sharing

$$\begin{array}{cc|cccc} & & & & \mathbf{A} & \\ & & A_0 & A_1 & \dots & A_d \\ \hline & B_0 & & & & \\ \mathbf{B} & B_1 & & & & \\ & \vdots & & & & \\ & B_d & & & & \end{array}$$

Multiplication over secret sharing

$$
\begin{array}{c|cccc}
 & & & \mathbf{A} & \\
 & A_0 & A_1 & \dots & A_d \\
B_0 & A_0 \cdot B_0 & A_1 \cdot B_0 & \dots & A_d \cdot B_0 \\
B_1 & A_0 \cdot B_1 & A_1 \cdot B_1 & \dots & A_d \cdot B_1 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
B_d & A_0 \cdot B_d & A_1 \cdot B_d & \dots & A_d \cdot B_d
\end{array}
$$

B

1.Cross-products

Multiplication over secret sharing

$$
\begin{array}{c|ccccc}
 & & & \mathbf{A} & & \\
 & A_0 & A_1 & \dots & A_d & \\
B_0 & A_0 \cdot B_0 & A_1 \cdot B_0 - {\color{blue}R_{0,1}} & \dots & A_d \cdot B_0 - {\color{green}R_{0,d}} & \\
B_1 & A_0 \cdot B_1 + {\color{blue}R_{0,1}} & A_1 \cdot B_1 & \dots & A_d \cdot B_1 - {\color{red}R_{1,d}} & \text{2. Refreshing} \\
\mathbf{B} \quad \vdots & \vdots & \vdots & \ddots & \vdots & \\
B_d & A_0 \cdot B_d + {\color{green}R_{0,d}} & A_1 \cdot B_d + {\color{red}R_{1,d}} & \dots & A_d \cdot B_d &
\end{array}
$$

Multiplication over secret sharing

$$
\begin{array}{c|cccccc|l}
 & & & \mathbf{A} & & & & \\
 & & A_0 & A_1 & \dots & A_d & & \\
 & B_0 & A_0 \cdot B_0 & A_1 \cdot B_0 - {\color{blue}R_{0,1}} & \dots & A_d \cdot B_0 - {\color{green}R_{0,d}} & & \\
\mathbf{B} & B_1 & A_0 \cdot B_1 + {\color{blue}R_{0,1}} & A_1 \cdot B_1 & \dots & A_d \cdot B_1 - {\color{red}R_{1,d}} & & \text{3. Compression} \\
 & \vdots & \vdots & \vdots & \ddots & \vdots & & \\
 & B_d & A_0 \cdot B_d + {\color{green}R_{0,d}} & A_1 \cdot B_d + {\color{red}R_{1,d}} & \dots & A_d \cdot B_d & & \\
 & & \Sigma_0 & \Sigma_1 & \dots & \Sigma_d & &
\end{array}
$$

Multiplication over secret sharing

$$\begin{array}{c|ccccc|c}
 & & & \mathbf{A} & & & \\
 & & A_0 & A_1 & \dots & A_d & \\
 & B_0 & A_0 \cdot B_0 & A_1 \cdot B_0 - R_{0,1} & \dots & A_d \cdot B_0 - R_{0,d} & \\
\mathbf{B} & B_1 & A_0 \cdot B_1 + R_{0,1} & A_1 \cdot B_1 & \dots & A_d \cdot B_1 - R_{1,d} & \text{3. Compression} \\
 & \vdots & \vdots & \vdots & \ddots & \vdots & \\
 & B_d & A_0 \cdot B_d + R_{0,d} & A_1 \cdot B_d + R_{1,d} & \dots & A_d \cdot B_d & \\
\downarrow & & \sum_0 & \sum_1 & \dots & \sum_d & \downarrow
\end{array}$$

The $\sum_i$ form a secure sharing of $A \cdot B$ against a *d-probing* adversary

Multiplication over secret sharing

$$
\begin{array}{cccccc}
 & & & \mathbf{A} & & \\
 & & A_0 & A_1 & \cdots & A_d \\
 & B_0 & A_0 \cdot B_0 & A_1 \cdot B_0 - R_{0,1} & \cdots & A_d \cdot B_0 - R_{0,d} \\
\mathbf{B} & B_1 & A_0 \cdot B_1 + R_{0,1} & A_1 \cdot B_1 & \cdots & A_d \cdot B_1 - R_{1,d} \\
 & \vdots & \vdots & \vdots & \ddots & \vdots \\
 & B_d & A_0 \cdot B_d + R_{0,d} & A_1 \cdot B_d + R_{1,d} & \cdots & A_d \cdot B_d \\
 & & \sum_0 & \sum_1 & \cdots & \sum_d
\end{array}
$$

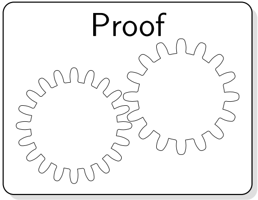
3. Compression

The $\sum_i$ form a secure sharing of $A \cdot B$ against a *d-probing* adversary

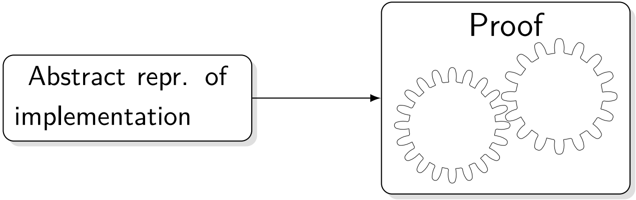
Probing model

A t-probing adversary can reveal a subset of t intermediate calculations. The target is secure if the subset is independent of the secret.

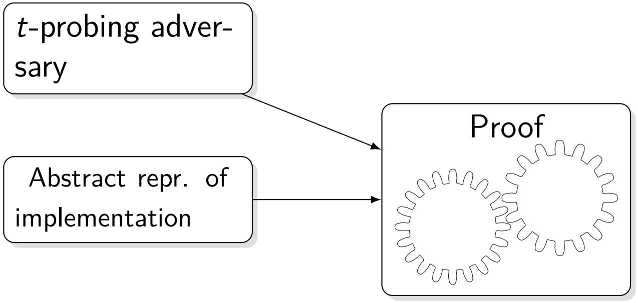
Proving Security in the Probing Model



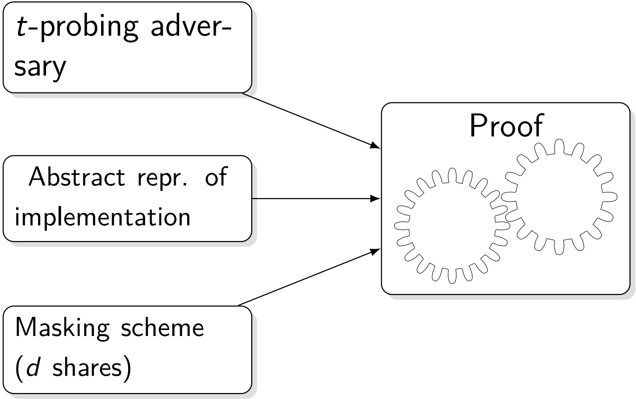
Proving Security in the Probing Model



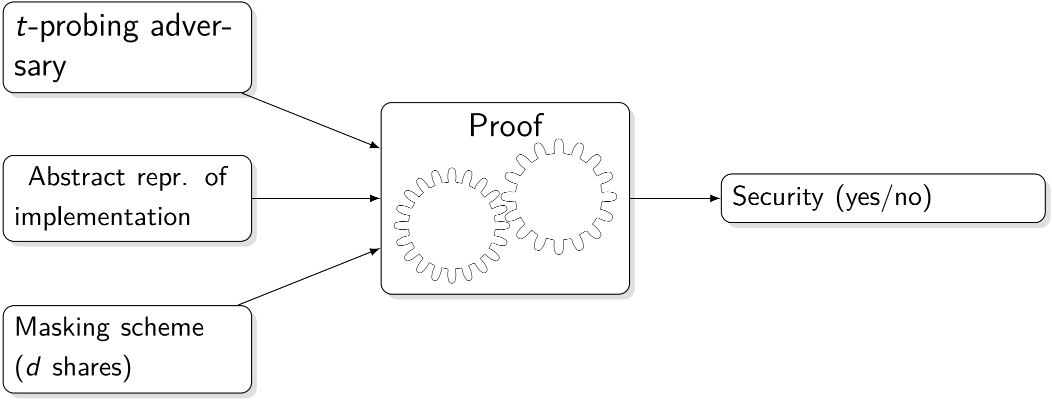
Proving Security in the Probing Model



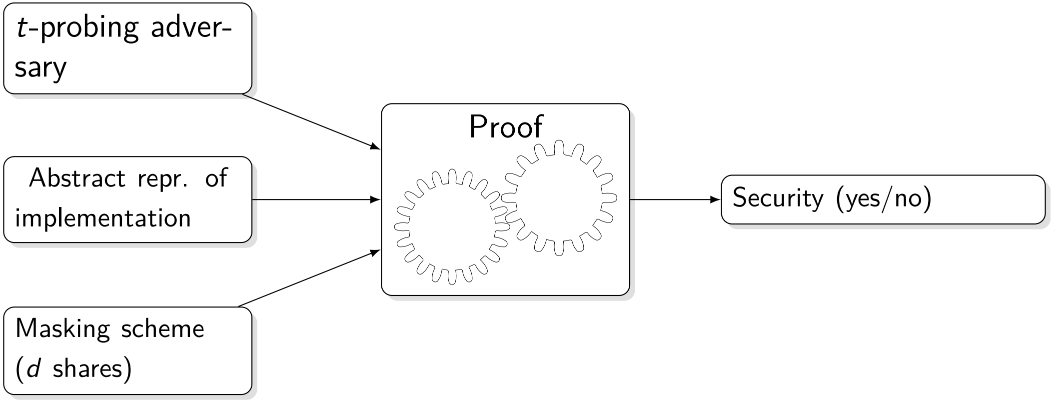
Proving Security in the Probing Model



Proving Security in the Probing Model



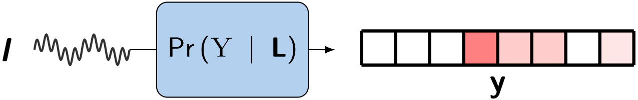
Proving Security in the Probing Model



Very practical to verify (using formal verification tools), but unrealistic adversary

The Noisy Leakage Model

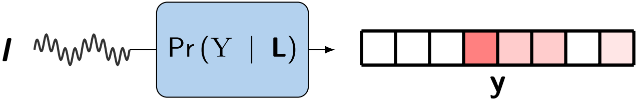
In this model, for each intermediate computation, the adversary gets a probability distribution about its operands:



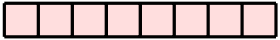
[3] D: Kullback - Leibler (KL) divergence, total variation, Euclidean norm, ...

The Noisy Leakage Model

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



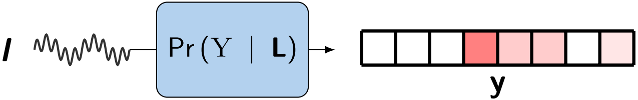
If, the adversary gets:



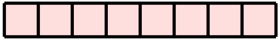
[3] D: KL divergence, total variation, Euclidean norm, ...

The Noisy Leakage Model

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



If, the adversary gets:

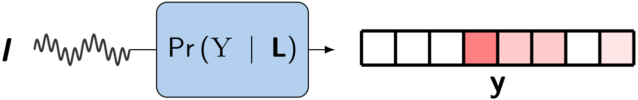


Very noisy
Sensitive computation unpredictable

[3] D: KL divergence, total variation, Euclidean norm, ...

The Noisy Leakage Model

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

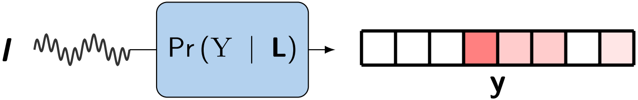


If, the adversary gets:

[3] D: KL divergence, total variation, Euclidean norm, ...

The Noisy Leakage Model

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



If, the adversary gets:

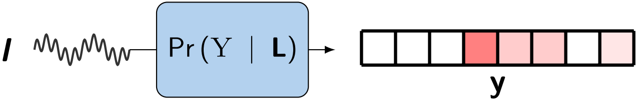
Low-noise

Exact prediction of the sensitive computation

[3] D: KL divergence, total variation, Euclidean norm, ...

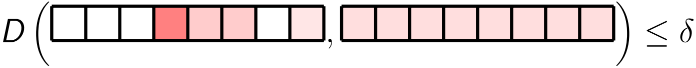
The Noisy Leakage Model

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



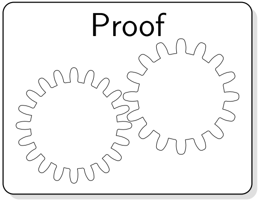
δ-NOISY ADVERSARY

All the p.m.f.s accessed by the adversary are δ-close[3] to the uniform:

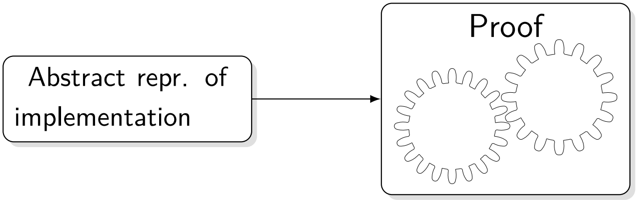


[3] D: KL divergence, total variation, Euclidean norm, ...

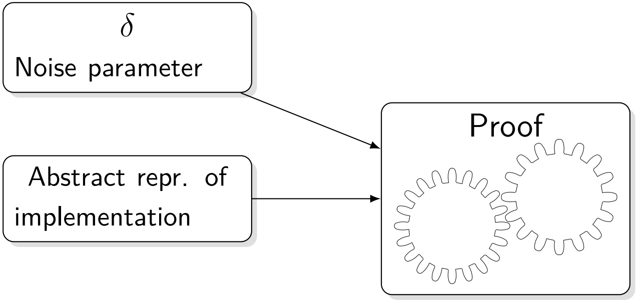
Proving the Masking Security



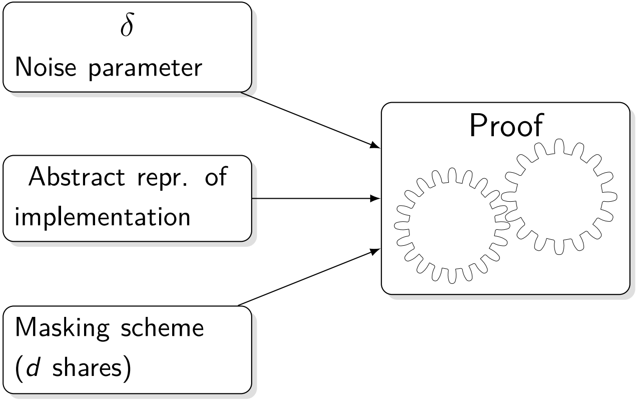
Proving the Masking Security



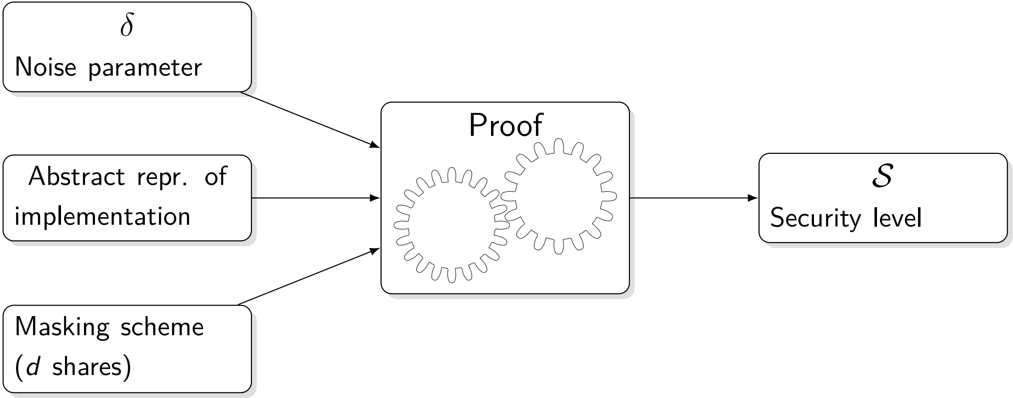
Proving the Masking Security



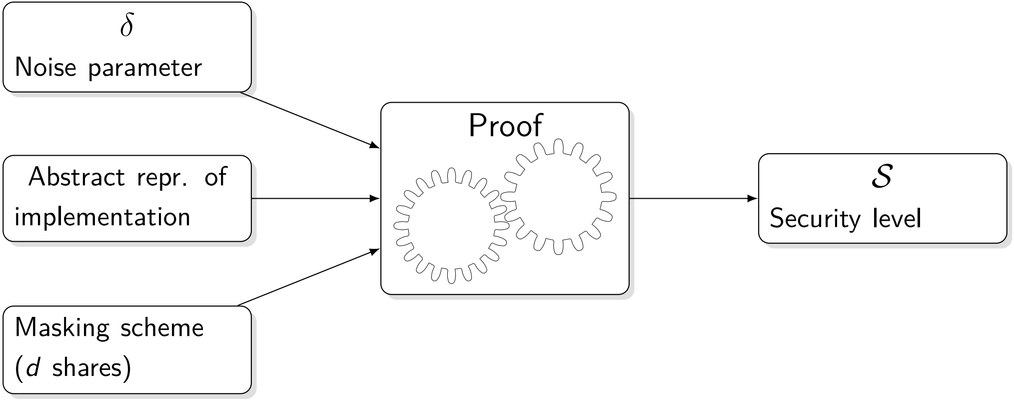
Proving the Masking Security



Proving the Masking Security

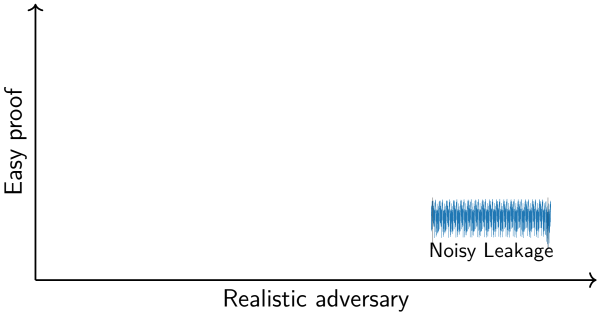


Proving the Masking Security



"Any attack requires $\mathcal{S}$ queries "

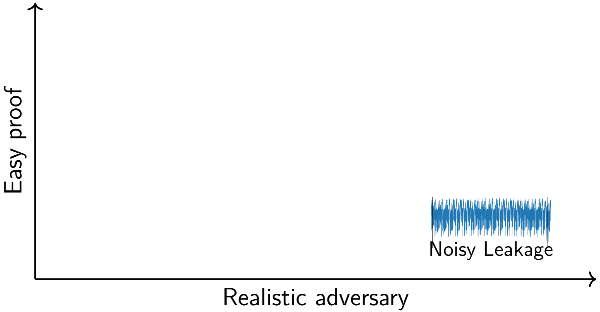
The Link between both Models



The Link between both Models

"Any successful adversary requires $\mathcal{S} = \Omega\left(\left(\frac{1}{\delta d |\mathbb{F}|}\right)^d\right)$ queries"

$\rightarrow$ Direct proof, with significant artifacts, with restricting assumptions[4]

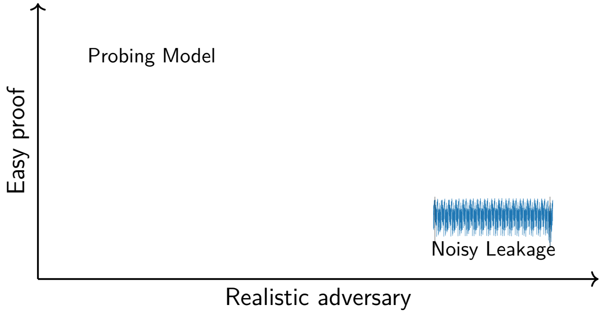


[4] Prouff and Rivain, "Masking against Side-Channel Attacks: A Formal Security Proof".

The Link between both Models

"Any successful adversary requires $\mathcal{S} = \Omega\left(\left(\frac{1}{\delta d |\mathbb{F}|}\right)^d\right)$ queries"

$\rightarrow$ Direct proof, with significant artifacts, with restricting assumptions[4]

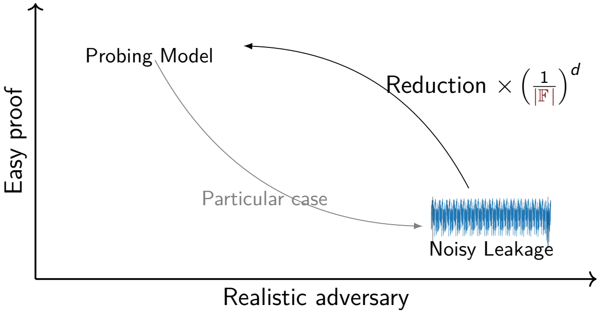


[4] Prouff and Rivain, "Masking against Side-Channel Attacks: A Formal Security Proof".

The Link between both Models

"Any successful adversary requires $\mathcal{S} = \Omega\left(\left(\frac{1}{\delta d |\mathbb{F}|}\right)^d\right)$ queries"

$\rightarrow$ Reduction, with significant artifacts, without restricting assumptions[4]



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

Our Work

"Any successful adversary requires $\mathcal{S} = \Omega\left(\left(\frac{1}{\delta d}\right)^{d}\right)$ queries"

Direct proof, without significant artifacts, with restricting assumptions[5]

[5] Almost identical to the ones of Prouff & Rivain

First Improvement: the Noise Amplification Bound

One bottleneck in P&R's proof is the bound over *one* encoding

First Improvement: the Noise Amplification Bound

One bottleneck in P&R's proof is the bound over *one* encoding

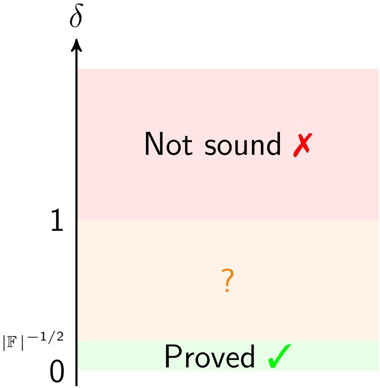
$$\mathrm{EN}\left(Secret; Leaky\ \ Encoding\right) \leq \left(\delta \cdot \sqrt{|\mathbb{F}|}\right)^{d}$$

Two issues with EN:

$\rightarrow$ Field-size dependent

$\rightarrow$ Does not extend well to leakage over computations

$\rightarrow$



First Improvement: the Noise Amplification Bound

One bottleneck in P&R's proof is the bound over *one* encoding

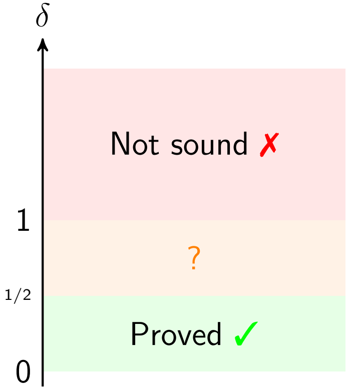
$$\mathrm{SD}\left(\mathit{Secret}; \mathit{Leaky\ \ Encoding}\right) \leq (\delta \cdot 2)^{d}$$

One issue with SD: [6]

$\rightarrow$ Not Field-size dependent

$\rightarrow$ Does not extend well to leakage over computations

$\rightarrow$

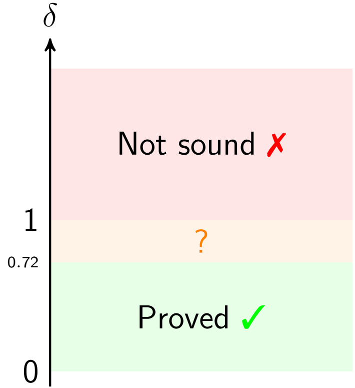


[6] Dziembowski, Faust, and Skórski, "Optimal Amplification of Noisy Leakages"

First Improvement: the Noise Amplification Bound

One bottleneck in P&R's proof is the bound over *one* encoding

$$\mathrm{MI}\left(Secret; Leaky\ \ Encoding\right) \leq 0.72 \cdot \left(\frac{\delta}{0.72}\right)^{d}$$



New bounds for MI: [6]

→ Not Field-size dependent

→ **This paper**: Extends well to leakage over computations

→

[6] Béguinot *et al.*, COSADE 2023, following Masure *et al.* at CARDIS'23 and Ito *et al.* at CCS'23)

Second Improvement: Refined Reduction to Uniform

The noise amplification bound only holds if the underlying secret is *uniform*
Required to get independent shares $\rightarrow$ reduction to random walks

Second Improvement: Refined Reduction to Uniform

The noise amplification bound only holds if the underlying secret is *uniform*
Required to get independent shares $\rightarrow$ reduction to random walks

In some non-linear computations, secret is not uniform, *e.g.*, $\mathrm{Y} \mapsto \mathrm{Y}^3$
How to deal with it?

Second Improvement: Refined Reduction to Uniform

The noise amplification bound only holds if the underlying secret is *uniform*
Required to get independent shares $\to$ reduction to random walks

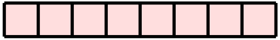
In some non-linear computations, secret is not uniform, *e.g.*, $\mathrm{Y} \mapsto \mathrm{Y}^3$
How to deal with it?

In previous works: generic (crude) reduction "non-uniform $\to$ uniform" $(\times|\mathbb{F}|)$

Second Improvement: Refined Reduction to Uniform

The noise amplification bound only holds if the underlying secret is *uniform*
Required to get independent shares $\rightarrow$ reduction to random walks

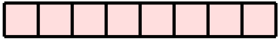
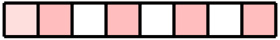
In some non-linear computations, secret is not uniform, *e.g.*, $\mathrm{Y} \mapsto \mathrm{Y}^3$
How to deal with it?

In previous works: generic (crude) reduction "non-uniform $\rightarrow$ uniform" $(\times|\mathbb{F}|)$
Our observation: If $\mathrm{Y} =$ ,

Second Improvement: Refined Reduction to Uniform

The noise amplification bound only holds if the underlying secret is *uniform*
Required to get independent shares $\rightarrow$ reduction to random walks

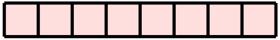
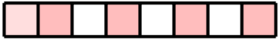
In some non-linear computations, secret is not uniform, *e.g.*, $\mathrm{Y} \mapsto \mathrm{Y}^3$
How to deal with it?

In previous works: generic (crude) reduction "non-uniform $\rightarrow$ uniform" $(\times|\mathbb{F}|)$
Our observation: If $\mathrm{Y} =$ , then $\mathrm{Y}^3 \approx$ 
Y^3 not that far from uniform $\implies$ specific (refined) reduction

Second Improvement: Refined Reduction to Uniform

The noise amplification bound only holds if the underlying secret is *uniform*
Required to get independent shares $\rightarrow$ reduction to random walks

In some non-linear computations, secret is not uniform, *e.g.*, $\mathrm{Y} \mapsto \mathrm{Y}^3$
How to deal with it?

In previous works: generic (crude) reduction "non-uniform $\rightarrow$ uniform" ($\times |\mathbb{F}|$)
Our observation: If $\mathrm{Y} =$ , then $\mathrm{Y}^3 \approx$ 
Y^3 not that far from uniform $\implies$ specific (refined) reduction

Pros: reasonable quasi-constant factor overhead
Cons: requires monomial SBoxes (ok for AES, not for DES)

Conclusion

Conclusion

→ We improve previous amplification-based bounds (EC'13, EC'15, C'19) in complementary directions

Conclusion

→ We improve previous amplification-based bounds (EC'13, EC'15, C'19) in complementary directions

→ We do not claim that the superiority of proofs by reductions is over

Conclusion

→ We improve previous amplification-based bounds (EC'13, EC'15, C'19) in complementary directions

→ We do not claim that the superiority of proofs by reductions is over

→ We also confirm that some (field-size) factors coming from proof reductions are indeed artifacts (see some bonus in the paper)

Conclusion

→ We improve previous amplification-based bounds (EC'13, EC'15, C'19) in complementary directions

→ We do not claim that the superiority of proofs by reductions is over

→ We also confirm that some (field-size) factors coming from proof reductions are indeed artifacts (see some bonus in the paper)

Future works:

- Relaxing the assumptions of direct proofs?
- Direct proofs for other masking schemes, *e.g.* table-based?

Thanks!

References I

- 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 II

Dziembowski, S., S. Faust, and M. Skórski. "Optimal Amplification of Noisy Leakages". In: *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part II*. Ed. by E. Kushilevitz and T. Malkin. Vol. 9563. Lecture Notes in Computer Science. Springer, 2016, pp. 291–318. DOI: 10.1007/978-3-662-49099-0_11. URL: https://doi.org/10.1007/978-3-662-49099-0_11.

References III

Ishai, Y., A. Sahai, and D. A. Wagner. "Private Circuits: Securing Hardware against Probing Attacks". In: *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*. Ed. by D. Boneh. Vol. 2729. Lecture Notes in Computer Science. Springer, 2003, pp. 463–481. DOI: 10.1007/978-3-540-45146-4_27. URL: https://doi.org/10.1007/978-3-540-45146-4_27.

References IV

Prouff, E. and M. Rivain. "Masking against Side-Channel Attacks: A Formal Security Proof". In: *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings.* Ed. by T. Johansson and P. Q. Nguyen. Vol. 7881. Lecture Notes in Computer Science. Springer, 2013, pp. 142–159. ISBN: 978-3-642-38347-2. DOI: 10.1007/978-3-642-38348-9_9. URL: https://doi.org/10.1007/978-3-642-38348-9_9.

References V

Rivain, M. and E. Prouff. "Provably Secure Higher-Order Masking of AES". In: *Cryptographic Hardware and Embedded Systems, CHES 2010, 12th International Workshop, Santa Barbara, CA, USA, August 17-20, 2010. Proceedings*. Ed. by S. Mangard and F. Standaert. Vol. 6225. Lecture Notes in Computer Science. Springer, 2010, pp. 413–427. DOI: 10.1007/978-3-642-15031-9_28. URL: https://doi.org/10.1007/978-3-642-15031-9_28.