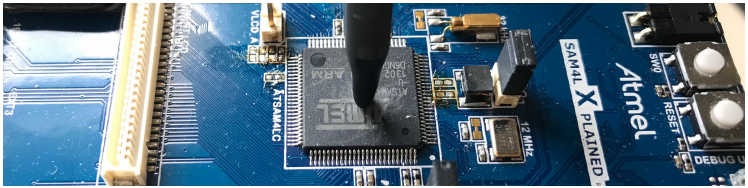


Computing over masked data with provable security

Loïc Masure (loic.masure@lirmm.fr)

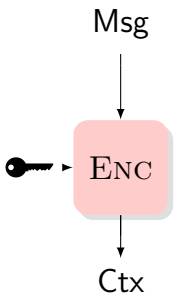
Séminaire ECO, Montpellier, 3 Septembre 2024

cnrs LIRMM UNIVERSITÉ DE MONTPELLIER

Agenda

Content

Context : Side-Channel Analysis (SCA)

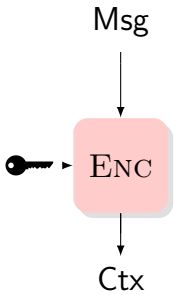


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

"Cryptographic algorithms don't run on paper,

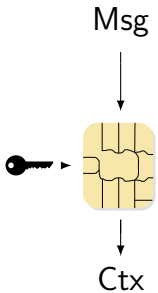


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

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

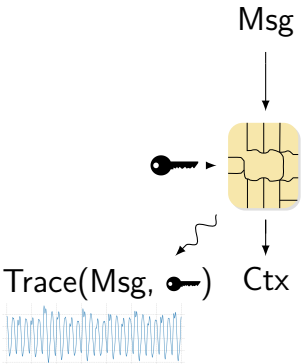


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

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

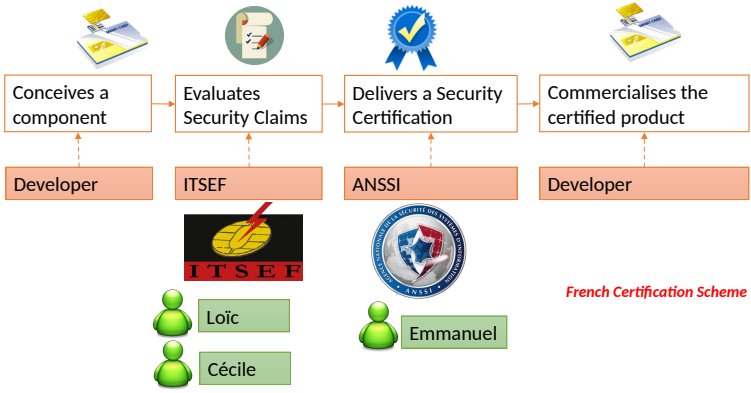


: N bits

Black-box cryptanalysis: 2^N

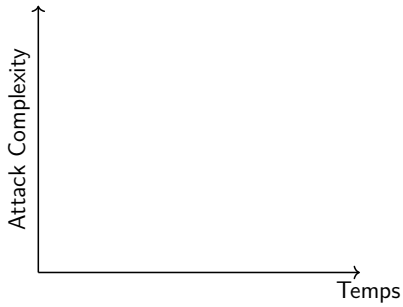
Content

Certification against SCA



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

Evaluate Security against Side-Channel Attacks

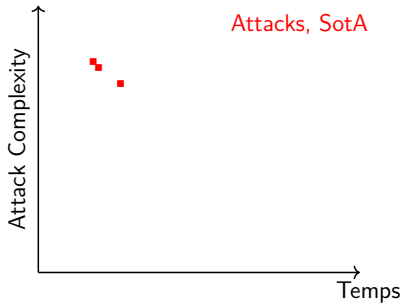


a

Attack approach (industry):

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks

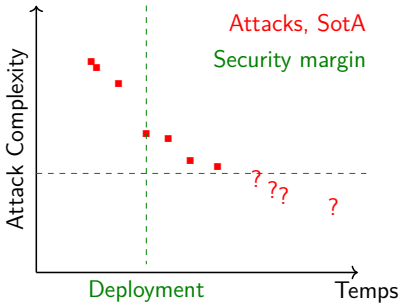


a

Attack approach (industry):
Current security level ✓

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



a

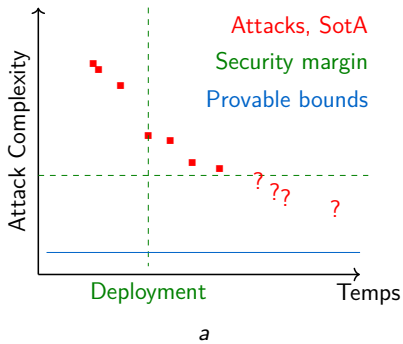
Attack approach (industry):

Current security level ✓

Future improvement → reevaluation ✗

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



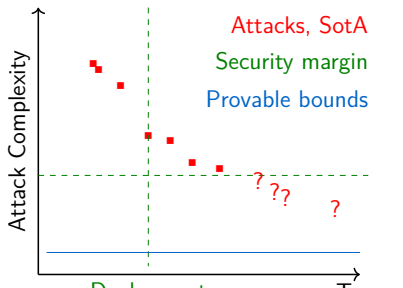
a

Attack approach (industry):
- Current security level ✓
- 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 ✓
- Future improvement → reevaluation ✗

Approach by *proofs* (academia):
- Rigorous approach ✓
- Potentially conservative ✗

[a] Shamelessly stolen to O. Bronchain

Today's agenda: evaluation by proofs

Content

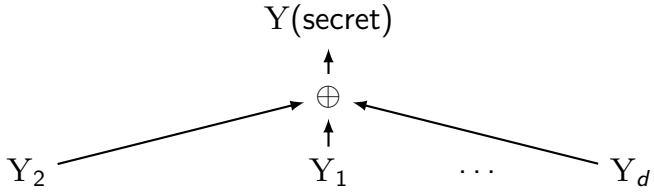
Masking: what is that ?

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

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

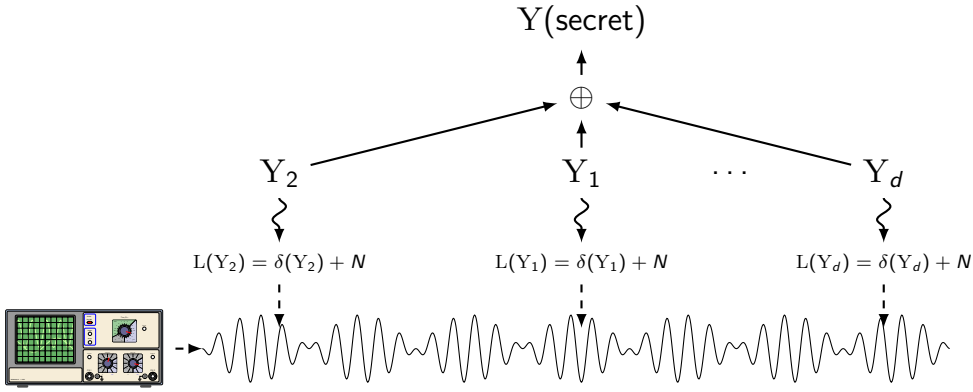
Masking: what is that ?

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 $(\mathbb{F}, \oplus, \otimes)$



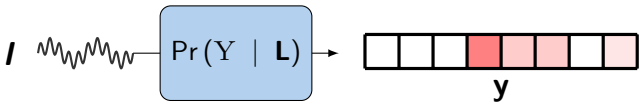
[1] Chari et al., "Towards Sound Approaches to Counteract Power-Analysis Attacks".

[2] Goubin and Patarin, "DES and Differential Power Analysis (The "Duplication" Method)".

Content

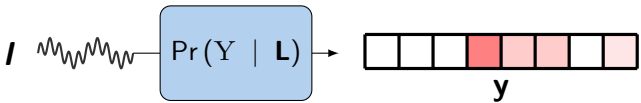
The Noisy Leakage Model

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

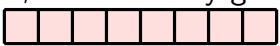


The Noisy Leakage Model

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

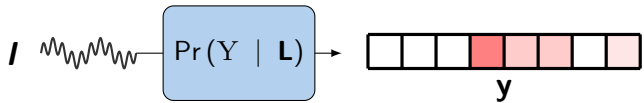


If, the adversary gets:

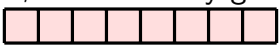


The Noisy Leakage Model

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



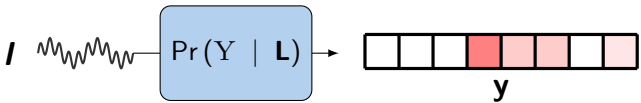
If, the adversary gets:



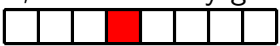
Very noisy
Sensitive computation unpredictable

The Noisy Leakage Model

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

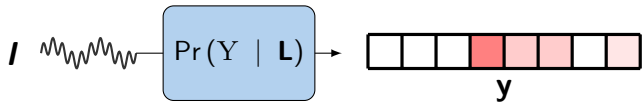


If, the adversary gets:



The Noisy Leakage Model

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



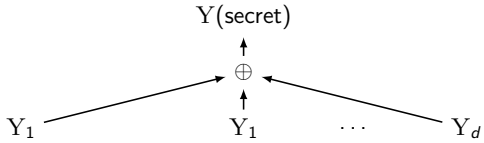
If, the adversary gets:

Low-noise
Exact prediction of the sensitive computation

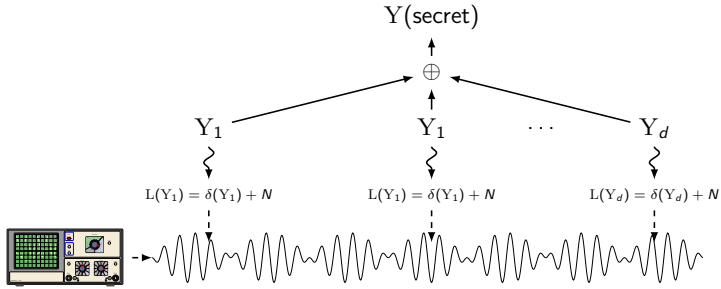
The Effect of Masking

$Y(\text{secret})$

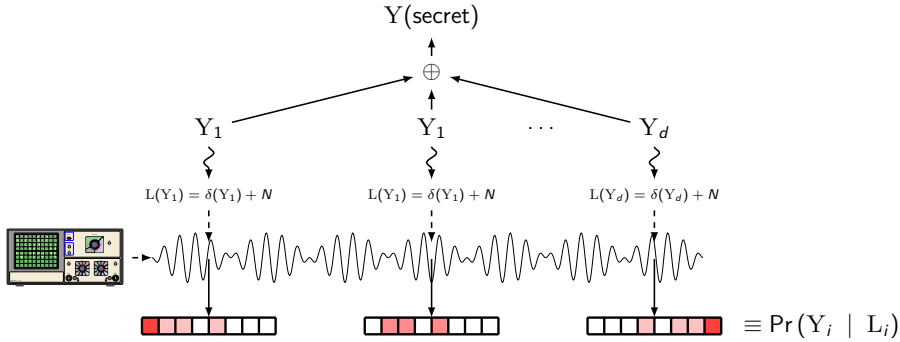
The Effect of Masking



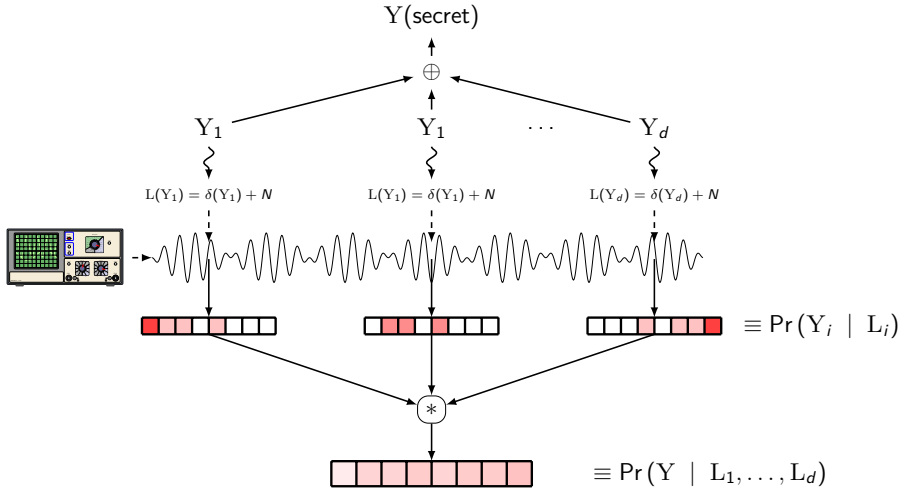
The Effect of Masking



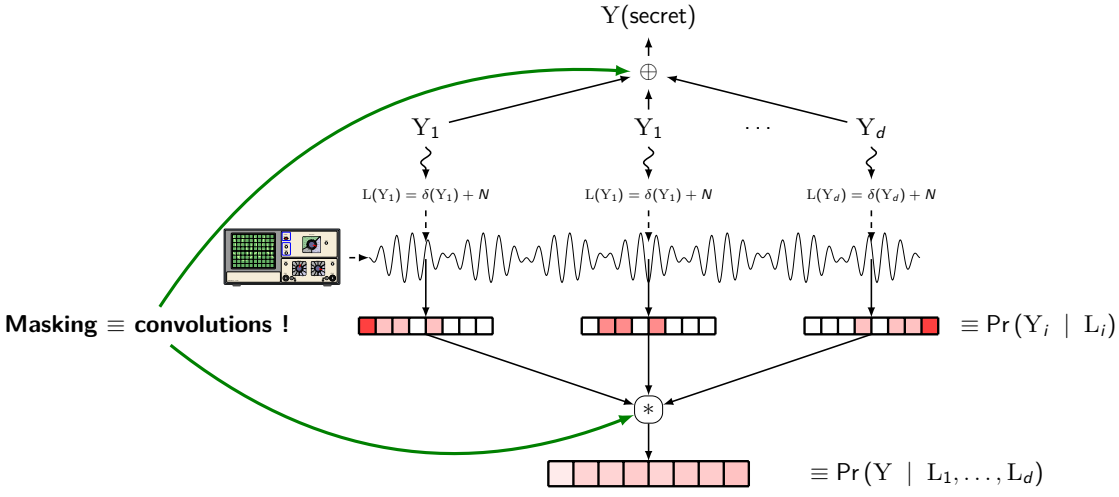
The Effect of Masking



The Effect of Masking



The Effect of Masking



Security on a Single Encoding

Theorem (Mrs. Gerber's Lemma[3])

Given $\mathrm{Y} = \mathrm{Y}_1 \oplus \ldots \oplus \mathrm{Y}_d$*, and each* Y_i *with (indep.) side information* $\mathrm{L}_1, \ldots, \mathrm{L}_d$*, then for* $\eta^{-1} = 2\log(2)$*:*

[3] Béguinot et al., "Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings".

Security on a Single Encoding

Theorem (Mrs. Gerber's Lemma[3])

Given $\mathrm{Y} = \mathrm{Y}_1 \oplus \ldots \oplus \mathrm{Y}_d$*, and each* Y_i *with (indep.) side information* $\mathrm{L}_1, \ldots, \mathrm{L}_d$*, then for* $\eta^{-1} = 2\log(2)$*:*

$$\mathsf{MI}(\mathrm{Y}; \mathbf{L}) \leq \prod_{i=1}^{d} \frac{\mathsf{MI}(\mathrm{Y}_i; \mathrm{L}_i)}{\eta} + \mathcal{O}\left(\prod_{i=1}^{d} \mathsf{MI}(\mathrm{Y}_i; \mathrm{L}_i)^2 \right) \quad \textit{in } \mathbb{F}_{2^n}$$

[3] Béguinot et al., "Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings".

Security on a Single Encoding

Theorem (Mrs. Gerber's Lemma[3]*)*

Given $\mathrm{Y} = \mathrm{Y}_1 \oplus \ldots \oplus \mathrm{Y}_d$*, and each* Y_i *with (indep.) side information* $\mathrm{L}_1, \ldots, \mathrm{L}_d$*, then for* $\eta^{-1} = 2\log(2)$*:*

$$\mathsf{MI}(\mathrm{Y}; \mathbf{L}) \leq \prod_{i=1}^{d} \frac{\mathsf{MI}(\mathrm{Y}_i; \mathrm{L}_i)}{\eta} + \mathcal{O}\left(\prod_{i=1}^{d} \mathsf{MI}(\mathrm{Y}_i; \mathrm{L}_i)^2 \right) \quad \textit{in } \mathbb{F}_{2^n}$$

$\rightarrow$ Security $\propto \frac{1}{\mathsf{MI}(\mathrm{Y};\mathbf{L})} \implies$ increases **exponentially fast** with d ✓

[3] Béguinot et al., "Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings".

Security on a Single Encoding

Theorem (Mrs. Gerber's Lemma[3]*)*

Given $\mathrm{Y} = \mathrm{Y}_1 \oplus \ldots \oplus \mathrm{Y}_d$*, and each* Y_i *with (indep.) side information* $\mathrm{L}_1, \ldots, \mathrm{L}_d$*, then for* $\eta^{-1} = 2\log(2)$*:*

$$\mathsf{MI}(\mathrm{Y}; \mathbf{L}) \leq \prod_{i=1}^{d} \frac{\mathsf{MI}(\mathrm{Y}_i; \mathrm{L}_i)}{\eta} + \mathcal{O}\left(\prod_{i=1}^{d} \mathsf{MI}(\mathrm{Y}_i; \mathrm{L}_i)^2 \right) \quad \textit{in } \mathbb{F}_{2^n}$$

$\rightarrow$ Security $\propto \frac{1}{\mathsf{MI}(\mathrm{Y};\mathbf{L})} \implies$ increases **exponentially fast** with d ✓

$\rightarrow$ Independent of the adversary ✓

[3] Béguinot et al., "Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings".

Convolution = Noise Amplification

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

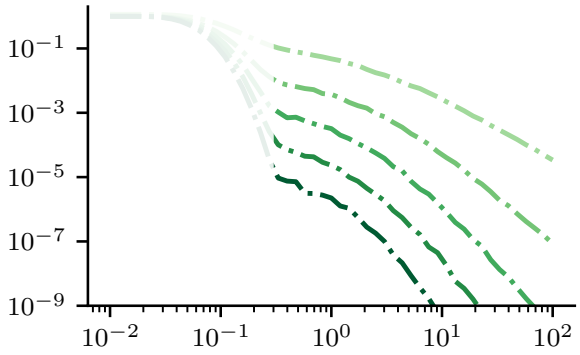


Figure: $\mathrm{MI}(\mathrm{Y}; \mathbf{L})$ vs. σ^2, $2 \leq d \leq 6$

Content

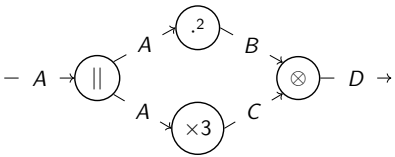
The Composition Paradigm

Idea to make a masked circuit

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

The Composition Paradigm

Idea to make a masked circuit

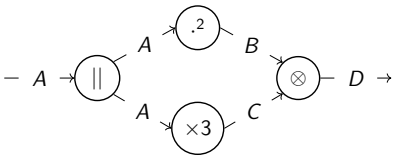


- View your algorithm as a circuit

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

The Composition Paradigm

Idea to make a masked circuit

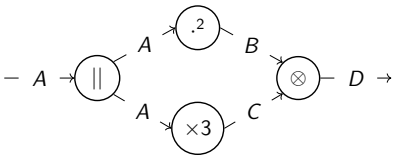


· View your algorithm as a circuit
→ Made of `not`, `and` gates [4]

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

The Composition Paradigm

Idea to make a masked circuit

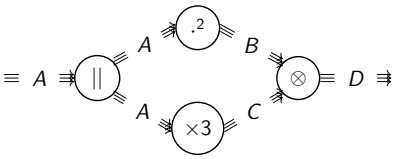


- View your algorithm as a circuit
  → Made of `not`, `and` gates [4]
  → Made of $\oplus, \otimes$ gates [5]

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

The Composition Paradigm

Idea to make a masked circuit

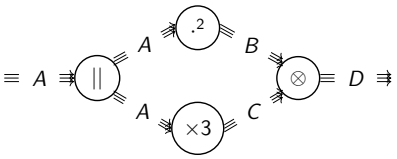


- View your algorithm as a circuit
  - → Made of `not`, `and` gates [4]
  - → Made of $\oplus, \otimes$ gates [5]
- Replace each gate by a masked *gadget*

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

The Composition Paradigm

Idea to make a masked circuit



- View your algorithm as a circuit
  → Made of `not`, `and` gates [4]
  → Made of $\oplus, \otimes$ gates [5]
- Replace each gate by a masked *gadget*
- Et voilà !

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

Desired Properties

Definition (t-privacy)

Any tuple of t intermediate values $\perp$ secrets

[6] Not $\iff$, see Bordes, "Security of symmetric primitives and their implementations", Example 5.5

Desired Properties

Definition (t-privacy)

Any tuple of t intermediate values $\perp$ secrets

Definition (Simulatability)

A set of probes $\mathcal{P}$ in a circuit $\mathbb{C}$ can be simulated with the input shares $\mathcal{I}$ if there exists an algorithm $\mathcal{S}$ (the *simulator*) such that

$$\mathcal{P} \overset{d}{=} \mathcal{S}(\mathcal{I})$$

[6] Not $\iff$, see Bordes, "Security of symmetric primitives and their implementations", Example 5.5

Desired Properties

Definition (t-privacy)

Any tuple of t intermediate values $\perp$ secrets

Definition (Simulatability)

A set of probes $\mathcal{P}$ in a circuit $\mathbb{C}$ can be simulated with the input shares $\mathcal{I}$ if there exists an algorithm $\mathcal{S}$ (the *simulator*) such that

$$\mathcal{P} \overset{d}{=} \mathcal{S}(\mathcal{I})$$

Definition (t-non-interference (NI))

$\mathbb{C}$ is t-NI if *any* set of t probes is simulatable by *at most* t shares of each input

[6] Not $\iff$, see Bordes, "Security of symmetric primitives and their implementations", Example 5.5

Desired Properties

Definition (t-privacy)

Any tuple of t intermediate values $\perp$ secrets

Definition (Simulatability)

A set of probes $\mathcal{P}$ in a circuit $\mathbb{C}$ can be simulated with the input shares $\mathcal{I}$ if there exists an algorithm $\mathcal{S}$ (the *simulator*) such that

$$\mathcal{P} \overset{d}{=} \mathcal{S}(\mathcal{I})$$

Definition (t-non-interference (NI))

$\mathbb{C}$ is t-NI if *any* set of t probes is simulatable by *at most* t shares of each input

For a circuit with d shares, d-NI $\implies$ d-privacy[6]

[6] Not $\iff$, see Bordes, "Security of symmetric primitives and their implementations", Example 5.5

Desired Properties

Definition (t-privacy)

Any tuple of t intermediate values $\perp$ secrets

Definition (Simulatability)

A set of probes $\mathcal{P}$ in a circuit $\mathbb{C}$ can be simulated with the input shares $\mathcal{I}$ if there exists an algorithm $\mathcal{S}$ (the *simulator*) such that

$$\mathcal{P} \overset{d}{=} \mathcal{S}(\mathcal{I}) \iff \mathcal{P}\perp \text{ all inputs except } \mathcal{I}$$

Definition (t-non-interference (NI))

$\mathbb{C}$ is t-NI if *any* set of t probes is simulatable by *at most* t shares of each input

For a circuit with d shares, d-NI $\implies$ d-privacy[6]

[6] Not $\iff$, see Bordes, "Security of symmetric primitives and their implementations", Example 5.5

The Composability Issue

✗NI is not always composable[7]

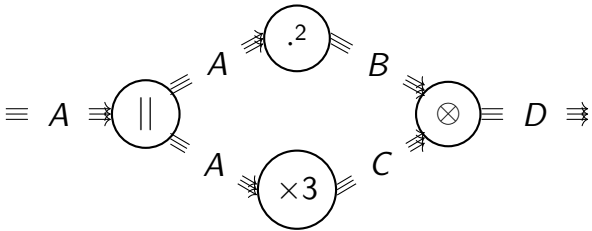


Figure: Two probes on D may depend on three probes of A !

[7] Coron et al., "Higher-Order Side Channel Security and Mask Refreshing".

The Composability Issue

✗NI is not always composable[7]

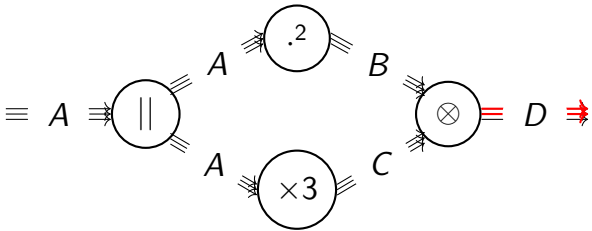


Figure: Two probes on D may depend on three probes of A !

[7] Coron et al., "Higher-Order Side Channel Security and Mask Refreshing".

The Composability Issue

✗NI is not always composable[7]

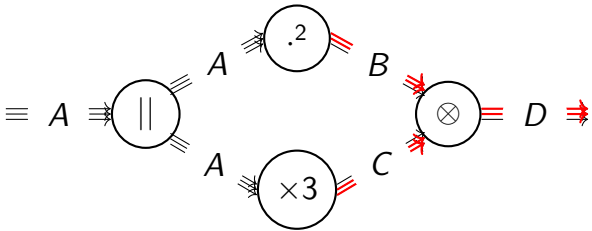


Figure: Two probes on D may depend on three probes of A !

[7] Coron et al., "Higher-Order Side Channel Security and Mask Refreshing".

The Composability Issue

✗NI is not always composable[7]

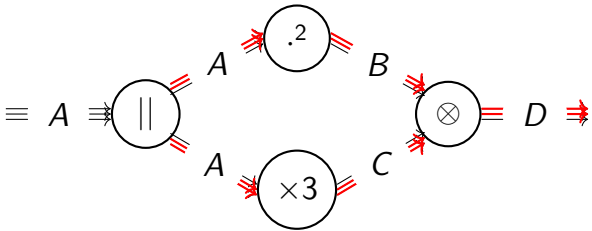


Figure: Two probes on D may depend on three probes of A !

[7] Coron et al., "Higher-Order Side Channel Security and Mask Refreshing".

The Composability Issue

✗NI is not always composable[7]

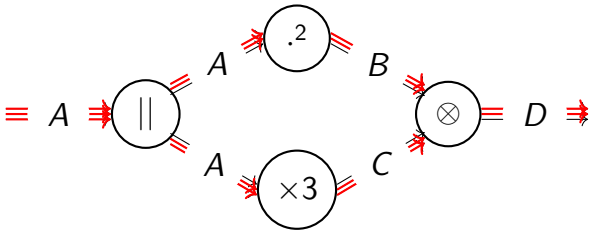


Figure: Two probes on D may depend on three probes of A !

[7] Coron et al., "Higher-Order Side Channel Security and Mask Refreshing".

Strong Non-Interference[9]

Definition (t-Strong Non-Interference)

A gadget is t-SNI if any set of t_1 internal probes and t_2 output probes can be simulated with t_1 shares of each input sharing, and

$$t = t_1 + t_2$$

$\rightarrow$ SNI is composable ✓

$\rightarrow$ SNI $\implies$ NI $\implies$ privacy

Other composable notions: SNIu, PINI[8], robust probing, glitch-extended, ...

[8] Cassiers and Standaert, "Trivially and Efficiently Composing Masked Gadgets With Probe Isolating Non-Interference".

[9] Barthe et al., "Strong Non-Interference and Type-Directed Higher-Order Masking".

Masked addition gadget

Inputs:

$$\begin{aligned}[\![A]\!] &= (A_1, \ldots, A_d) \\ [\![B]\!] &= (B_1, \ldots, B_d)\end{aligned}$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \oplus \left(\sum_i B_i\right)$$

Masked addition gadget

Inputs:

$$[\![A]\!] = (A_1, \ldots, A_d)$$
$$[\![B]\!] = (B_1, \ldots, B_d)$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \oplus \left(\sum_i B_i\right)$$

SecAdd algorithm:

$$\begin{aligned} C_1 &= A_1 \oplus B_1 \\ &\vdots \\ C_d &= A_d \oplus B_d \end{aligned}$$

Masked addition gadget

Inputs:

$$[\![A]\!] = (A_1, \ldots, A_d)$$
$$[\![B]\!] = (B_1, \ldots, B_d)$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \oplus \left(\sum_i B_i\right)$$

SecAdd algorithm:

$$C_1 = A_1 \oplus B_1$$
$$\vdots$$
$$C_d = A_d \oplus B_d$$

- NI, but not SNI ✗

Masked addition gadget

Inputs:

$$[\![A]\!] = (A_1, \ldots, A_d)$$
$$[\![B]\!] = (B_1, \ldots, B_d)$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \oplus \left(\sum_i B_i\right)$$

SecAdd algorithm:

$$\begin{aligned} C_1 &= A_1 \oplus B_1 \\ &\vdots \\ C_d &= A_d \oplus B_d \end{aligned}$$

- NI, but not SNI ✗
- t-NI + t-SNI refresh $\implies$ t-SNI ✓

Masked addition gadget

Inputs:

$$[\![A]\!] = (A_1, \ldots, A_d)$$
$$[\![B]\!] = (B_1, \ldots, B_d)$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \oplus \left(\sum_i B_i\right)$$

SecAdd algorithm:

$$\begin{aligned} C_1 &= A_1 \oplus B_1 \\ &\vdots \\ C_d &= A_d \oplus B_d \end{aligned}$$

- NI, but not SNI ✗
- t-NI + t-SNI refresh $\implies$ t-SNI ✓
- Generalization: share-wise application of any affine map

Masked multiplication gadget

Inputs:

$$\begin{aligned}[\![A]\!] &= (A_1, \ldots, A_d) \\ [\![B]\!] &= (B_1, \ldots, B_d)\end{aligned}$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \otimes \left(\sum_i B_i\right)$$

Masked multiplication gadget

Inputs:

$$\begin{aligned}[\![A]\!] &= (A_1, \ldots, A_d)\\ [\![B]\!] &= (B_1, \ldots, B_d)\end{aligned}$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \otimes \left(\sum_i B_i\right)$$

BadMult algorithm:

$$\begin{aligned}C_1 = &(A_1 \otimes B_1) \oplus (A_1 \otimes B_2) \oplus (A_1 \otimes B_3)\\ C_2 = &(A_2 \otimes B_1) \oplus (A_2 \otimes B_2) \oplus (A_2 \otimes B_3)\\ C_3 = &(A_3 \otimes B_1) \oplus (A_3 \otimes B_2) \oplus (A_3 \otimes B_3)\end{aligned}$$

Correct, but not 2-NI. Why ?

Masked multiplication gadget

Inputs:

$$[\![A]\!] = (A_1, \ldots, A_d)$$
$$[\![B]\!] = (B_1, \ldots, B_d)$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \otimes \left(\sum_i B_i\right)$$

BadMult algorithm:

$$\begin{aligned} C_1 &= (A_1 \otimes B_1) \oplus (A_1 \otimes B_2) \oplus (A_1 \otimes B_3) \\ C_2 &= (A_2 \otimes B_1) \oplus (A_2 \otimes B_2) \oplus (A_2 \otimes B_3) \\ C_3 &= (A_3 \otimes B_1) \oplus (A_3 \otimes B_2) \oplus (A_3 \otimes B_3) \end{aligned}$$

Correct, but not 2-NI. Why ?

Masked multiplication gadget

Inputs:

$$[\![A]\!] = (A_1, \ldots, A_d)$$
$$[\![B]\!] = (B_1, \ldots, B_d)$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \otimes \left(\sum_i B_i\right)$$

SecMult algorithm:

$$C_1 = (A_1 \otimes B_1) \oplus (A_1 \otimes B_2 \oplus R_1) \oplus (A_1 \otimes B_3 \oplus R_2)$$
$$C_2 = (A_2 \otimes B_1 \ominus R_1) \oplus (A_2 \otimes B_2) \oplus (A_2 \otimes B_3 \oplus R_3)$$
$$C_3 = (A_3 \otimes B_1 \ominus R_2) \oplus (A_3 \otimes B_2 \ominus R_3) \oplus (A_3 \otimes B_3)$$

· SecMult is $(d-1)$-SNI ✓

Masked multiplication gadget

Inputs:

$$[\![A]\!] = (A_1, \ldots, A_d)$$
$$[\![B]\!] = (B_1, \ldots, B_d)$$

Output:

$$[\![C]\!] = (C_1, \ldots, C_d)$$

such that

$$\sum_i C_i = \left(\sum_i A_i\right) \otimes \left(\sum_i B_i\right)$$

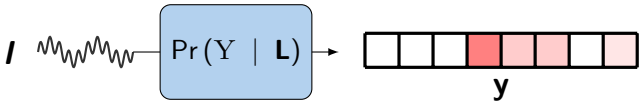
SecMult algorithm:

$$C_1 = (A_1 \otimes B_1) \oplus (A_1 \otimes B_2 \oplus R_1) \oplus (A_1 \otimes B_3 \oplus R_2)$$
$$C_2 = (A_2 \otimes B_1 \ominus R_1) \oplus (A_2 \otimes B_2) \oplus (A_2 \otimes B_3 \oplus R_3)$$
$$C_3 = (A_3 \otimes B_1 \ominus R_2) \oplus (A_3 \otimes B_2 \ominus R_3) \oplus (A_3 \otimes B_3)$$

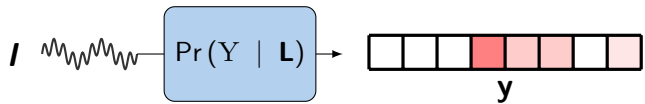
- SecMult is $(d-1)$-SNI ✓
- If $[\![B]\!] = (1, 0, \ldots, 0)$, then $\text{SecMult}([\![A]\!], [\![B]\!]) = \text{Refresh}([\![A]\!])$ ✓

Content

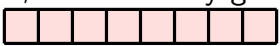
Recall on Noisy Leakage Model



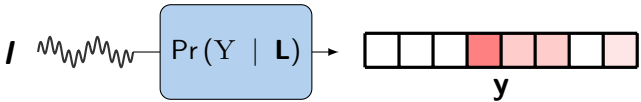
Recall on Noisy Leakage Model



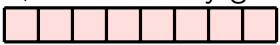
If, the adversary gets:



Recall on Noisy Leakage Model

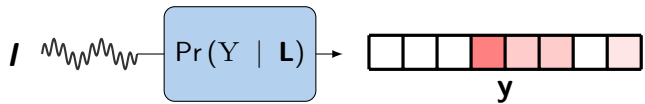


If, the adversary gets:



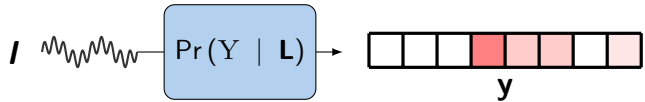
Very noisy leakage
Y indistinguishable from blind guess

Recall on Noisy Leakage Model



If, the adversary gets:

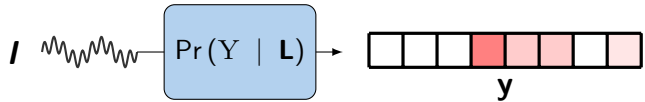
Recall on Noisy Leakage Model



If, the adversary gets:

Low-noise leakage
Exact prediction for Y

Recall on Noisy Leakage Model



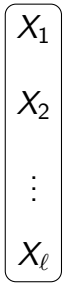
δ-NOISY ADVERSARY

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

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

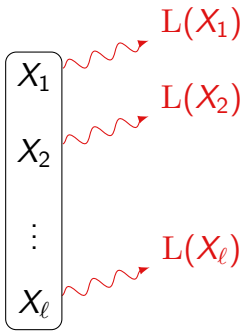
Security Proof for a Gadget

Consider a gadget with ℓ intermediate computations:



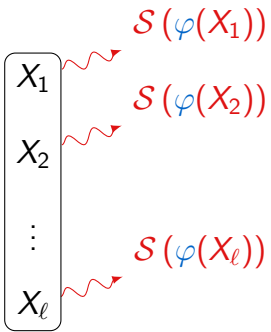
Security Proof for a Gadget

Consider a gadget with ℓ δ-noisy intermediate computations:



Security Proof for a Gadget

Consider a gadget with ℓ δ-noisy intermediate computations:

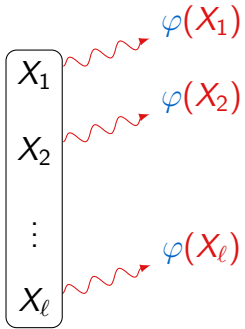


Lemma (Simulatability by RP)
The leakage function L *can be simulated from a random probing adversary:* $\varphi(x)$ *exactly reveals* x *with probability* $\epsilon = 1 - \sum_l \min_x \Pr(\mathrm{L}(x) = l) \leq \delta \cdot |\mathbb{F}|$.[a]

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

Security Proof for a Gadget

Consider a gadget with ℓ δ-noisy intermediate computations:



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

Proof of the Core Lemma (I)

Assume there exists such a simulator $\mathcal{S}$,

Proof of the Core Lemma (I)

Assume there exists such a simulator $\mathcal{S}$, we need to construct it for all inputs:

$$\begin{aligned} \Pr\left(\mathcal{S}\left(x\right) = l\right) &= \ldots, \text{ for all } x \\ \Pr\left(\mathcal{S}\left(\bot\right) = l\right) &= \ldots \end{aligned}$$

Constraints:

Proof of the Core Lemma (I)

Assume there exists such a simulator $\mathcal{S}$, we need to construct it for all inputs:

$$\begin{aligned} \Pr\left(\mathcal{S}\left(x\right) = l\right) &= \ldots, \text{ for all } x \\ \Pr\left(\mathcal{S}\left(\bot\right) = l\right) &= \ldots \end{aligned}$$

Constraints:

$\rightarrow$ For all input x, $\Pr\left(\mathcal{S}\left(x\right)\right)$ should be a p.m.f. $(2 \cdot |\mathbb{F}|$ (in)equations)

Proof of the Core Lemma (I)

Assume there exists such a simulator $\mathcal{S}$, we need to construct it for all inputs:

$$\begin{aligned} \Pr\left(\mathcal{S}\left(x\right) = l\right) &= \ldots, \text{ for all } x \\ \Pr\left(\mathcal{S}\left(\perp\right) = l\right) &= \ldots \end{aligned}$$

Constraints:

$\rightarrow$ For all input x, $\Pr\left(\mathcal{S}\left(x\right)\right)$ should be a p.m.f. $(2 \cdot |\mathbb{F}|$ (in)equations)

$\rightarrow$ For the input $\perp$, $\Pr\left(\mathcal{S}\left(\perp\right)\right)$ should be a p.m.f. (2 (in)equations)

Proof of the Core Lemma (I)

Assume there exists such a simulator $\mathcal{S}$, we need to construct it for all inputs:

$$\begin{aligned} \Pr\left(\mathcal{S}\left(x\right) = l\right) &= \ldots, \text{ for all } x \\ \Pr\left(\mathcal{S}\left(\bot\right) = l\right) &= \ldots \end{aligned}$$

Constraints:

$\rightarrow$ For all input x, $\Pr\left(\mathcal{S}\left(x\right)\right)$ should be a p.m.f. $(2 \cdot |\mathbb{F}|$ (in)equations)

$\rightarrow$ For the input $\bot$, $\Pr\left(\mathcal{S}\left(\bot\right)\right)$ should be a p.m.f. (2 (in)equations)

$\rightarrow$ For any x, l, $\Pr\left(\mathcal{S}\left(\varphi(x)\right) = l\right) = \Pr\left(\mathrm{L}(x) = l\right)$ $(|\mathbb{F}| \times |\mathcal{L}|$ equations)

Proof of the Core Lemma (II)

Let us start from the last constraint. For any x and any l:

$$\Pr\left(\mathrm{L}(x) = l\right) \;=\; \Pr\left(\mathcal{S}\left(\varphi(x)\right) = l\right)$$

Proof of the Core Lemma (II)

Let us start from the last constraint. For any x and any l:

$$\begin{aligned}\Pr\left(\mathrm{L}(x) = l\right) &= \Pr\left(\mathcal{S}\left(\varphi(x)\right) = l\right) \\ &= \Pr\left(\varphi(x) = x\right) \cdot \Pr\left(\mathcal{S}\left(x\right) = l\right) + \Pr\left(\varphi(x) = \bot\right) \cdot \Pr\left(\mathcal{S}\left(\bot\right) = l\right)\end{aligned}$$

Proof of the Core Lemma (II)

Let us start from the last constraint. For any x and any l:

$$\begin{aligned}
\Pr\left(\mathrm{L}(x) = l\right) &= \Pr\left(\mathcal{S}\left(\varphi(x)\right) = l\right) \\
&= \Pr\left(\varphi(x) = x\right) \cdot \Pr\left(\mathcal{S}\left(x\right) = l\right) + \Pr\left(\varphi(x) = \bot\right) \cdot \Pr\left(\mathcal{S}\left(\bot\right) = l\right) \\
&= \epsilon \cdot \Pr\left(\mathcal{S}\left(x\right) = l\right) + (1 - \epsilon) \cdot \Pr\left(\mathcal{S}\left(\bot\right) = l\right)
\end{aligned}$$

Proof of the Core Lemma (II)

Let us start from the last constraint. For any x and any l:

$$\begin{aligned}\Pr\left(\mathrm{L}(x)=l\right) &= \Pr\left(\mathcal{S}\left(\varphi(x)\right)=l\right)\\ &= \Pr\left(\varphi(x)=x\right)\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+\Pr\left(\varphi(x)=\bot\right)\cdot\Pr\left(\mathcal{S}\left(\bot\right)=l\right)\\ &= \epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+(1-\epsilon)\cdot\Pr\left(\mathcal{S}\left(\bot\right)=l\right)\end{aligned}$$

Hence,

$$0 \leq \Pr\left(\mathcal{S}\left(\bot\right)=l\right) = \frac{\overbrace{\Pr\left(\mathrm{L}(x)=l\right)-\epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)}^{\text{Should not depend on } X}}{1-\epsilon}$$

Proof of the Core Lemma (II)

Let us start from the last constraint. For any x and any l:

$$\begin{aligned}\Pr\left(\mathrm{L}(x)=l\right) &= \Pr\left(\mathcal{S}\left(\varphi(x)\right)=l\right)\\ &= \Pr\left(\varphi(x)=x\right)\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+\Pr\left(\varphi(x)=\bot\right)\cdot\Pr\left(\mathcal{S}\left(\bot\right)=l\right)\\ &= \epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+(1-\epsilon)\cdot\Pr\left(\mathcal{S}\left(\bot\right)=l\right)\end{aligned}$$

Hence,

$$0 \leq \Pr\left(\mathcal{S}\left(\bot\right)=l\right) = \frac{\overbrace{\Pr\left(\mathrm{L}(x)=l\right)-\epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)}^{\text{Should not depend on } X}}{1-\epsilon} = \frac{\pi(l)}{1-\epsilon} \quad (1)$$

Proof of the Core Lemma (II)

Let us start from the last constraint. For any x and any l:

$$\begin{aligned}\Pr\left(\mathrm{L}(x)=l\right) &= \Pr\left(\mathcal{S}\left(\varphi(x)\right)=l\right)\\ &= \Pr\left(\varphi(x)=x\right)\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+\Pr\left(\varphi(x)=\bot\right)\cdot\Pr\left(\mathcal{S}\left(\bot\right)=l\right)\\ &= \epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+(1-\epsilon)\cdot\Pr\left(\mathcal{S}\left(\bot\right)=l\right)\end{aligned}$$

Hence,

$$0 \leq \Pr\left(\mathcal{S}\left(\bot\right)=l\right) = \frac{\overbrace{\Pr\left(\mathrm{L}(x)=l\right)-\epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)}^{\text{Should not depend on } X}}{1-\epsilon} = \frac{\pi(l)}{1-\epsilon} \quad (1)$$

$$0 \leq \Pr\left(\mathcal{S}\left(x\right)=l\right) = \frac{\Pr\left(\mathrm{L}(x)=l\right)-\pi(l)}{\epsilon} \quad (2)$$

Proof of the Core Lemma (II)

Let us start from the last constraint. For any x and any l:

$$\begin{aligned}\Pr\left(\mathrm{L}(x)=l\right) &= \Pr\left(\mathcal{S}\left(\varphi(x)\right)=l\right)\\ &= \Pr\left(\varphi(x)=x\right)\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+\Pr\left(\varphi(x)=\perp\right)\cdot\Pr\left(\mathcal{S}\left(\perp\right)=l\right)\\ &= \epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)+(1-\epsilon)\cdot\Pr\left(\mathcal{S}\left(\perp\right)=l\right)\end{aligned}$$

Hence,

$$0 \leq \Pr\left(\mathcal{S}\left(\perp\right)=l\right) = \frac{\overbrace{\Pr\left(\mathrm{L}(x)=l\right)-\epsilon\cdot\Pr\left(\mathcal{S}\left(x\right)=l\right)}^{\text{Should not depend on } x}}{1-\epsilon} = \frac{\pi(l)}{1-\epsilon} \quad (1)$$

$$0 \leq \Pr\left(\mathcal{S}\left(x\right)=l\right) = \frac{\Pr\left(\mathrm{L}(x)=l\right)-\pi(l)}{\epsilon} \quad (2)$$

Is there any ϵ such that $\geq$ and $\geq$ are valid?

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid?

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (1), and (2), we get

$$0 \leq \pi(l) \leq \Pr(\mathrm{L}(x) = l) \text{ for any } x$$

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (1), and (2), we get

$$0 \leq \pi(l) \leq \Pr\left(\mathrm{L}(x) = l\right) \text{ for any } x$$

In other words,

$$0 \leq \pi(l) \leq \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (1), and (2), we get

$$0 \leq \pi(l) \leq \Pr\left(\mathrm{L}(x) = l\right) \text{ for any } x$$

In other words,

$$0 \leq \pi(l) \leq \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Furthermore, summing (1) over l, by definition of probability distributions,

$$\sum_l \pi(l) = \underbrace{\sum_l \Pr\left(\mathrm{L}(x) = l\right)}_{=1} - \epsilon \cdot \underbrace{\sum_l \Pr\left(\mathcal{S}(x) = l\right)}_{=1}$$

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (1), and (2), we get

$$0 \leq \pi(l) \leq \Pr\left(\mathrm{L}(x) = l\right) \text{ for any } x$$

In other words,

$$0 \leq \pi(l) \leq \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Furthermore, summing (1) over l, by definition of probability distributions,

$$\sum_l \pi(l) = \underbrace{\sum_l \Pr\left(\mathrm{L}(x) = l\right)}_{=1} - \epsilon \cdot \underbrace{\sum_l \Pr\left(\mathcal{S}(x) = l\right)}_{=1} = 1 - \epsilon$$

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (1), and (2), we get

$$0 \leq \pi(l) \leq \Pr\left(\mathrm{L}(x) = l\right) \text{ for any } x$$

In other words,

$$0 \leq \pi(l) \leq \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Furthermore, summing (1) over l, by definition of probability distributions,

$$\sum_l \pi(l) = \underbrace{\sum_l \Pr\left(\mathrm{L}(x) = l\right)}_{=1} - \epsilon \cdot \underbrace{\sum_l \Pr\left(\mathcal{S}(x) = l\right)}_{=1} = 1 - \epsilon$$

Hence,

$$\epsilon = 1 - \sum_l \pi(l) \geq 1 - \sum_l \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (1), and (2), we get

$$0 \leq \pi(l) \leq \Pr\left(\mathrm{L}(x) = l\right) \text{ for any } x$$

In other words,

$$0 \leq \pi(l) \leq \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Furthermore, summing (1) over l, by definition of probability distributions,

$$\sum_l \pi(l) = \underbrace{\sum_l \Pr\left(\mathrm{L}(x) = l\right)}_{=1} - \epsilon \cdot \underbrace{\sum_l \Pr\left(\mathcal{S}(x) = l\right)}_{=1} = 1 - \epsilon$$

Hence, to have the smallest ϵ,

$$\epsilon = 1 - \sum_l \pi(l) = 1 - \sum_l \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Proof of the Core Lemma (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (1), and (2), we get

$$0 \leq \pi(l) \leq \Pr\left(\mathrm{L}(x) = l\right) \text{ for any } x$$

In other words,

$$0 \leq \pi(l) \leq \min_x \Pr\left(\mathrm{L}(x) = l\right)$$

Furthermore, summing (1) over l, by definition of probability distributions,

$$\sum_l \pi(l) = \underbrace{\sum_l \Pr\left(\mathrm{L}(x) = l\right)}_{=1} - \epsilon \cdot \underbrace{\sum_l \Pr\left(\mathcal{S}(x) = l\right)}_{=1} = 1 - \epsilon$$

Hence, to have the smallest ϵ,

$$\epsilon = 1 - \sum_l \pi(l) = 1 - \sum_l \min_x \Pr\left(\mathrm{L}(x) = l\right) \leq \delta \cdot |\mathbb{F}| \quad (\textbf{Q11}\text{: prove it})$$

Security against a Random Probing Adversary

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

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

[10] 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)

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

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

[10] 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)

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

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

Q11: Prove the inequality from a particular case of Chernoff inequality[10]

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

Putting all Together

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

Theorem (Security Bound)

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

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \mathcal{O}\left(\left(7e \cdot d \cdot \delta \cdot |\mathbb{F}|\right)^d\right)$$

[11] t-Region-probing secure: NI, with t probes from *each* gadget

Putting all Together

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

Theorem (Security Bound)

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

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \mathcal{O}\left(\left(7e \cdot d \cdot \delta \cdot |\mathbb{F}|\right)^d\right)$$

For the whole circuit $\mathbb{C}$,

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \mathcal{O}\left(\left(7e \cdot |\mathbb{C}| \cdot d \cdot \delta \cdot |\mathbb{F}|\right)^d\right)$$

[11] t-Region-probing secure: NI, with t probes from *each* gadget

Putting all Together

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

Theorem (Security Bound)

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

$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \mathcal{O}\left(\left(7e \cdot d \cdot \delta \cdot |\mathbb{F}|\right)^d\right)$$

For the whole circuit $\mathbb{C}$, $d/2$-region probing[11] security implies

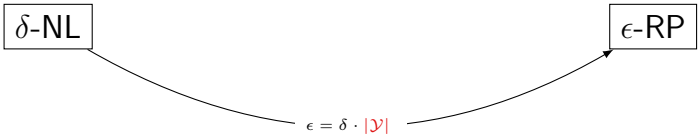
$$\mathsf{SD}\left(k; \mathbf{L}\right) \leq \mathcal{O}\left(|\mathbb{C}| \left(7e \cdot d \cdot \delta \cdot |\mathbb{F}|\right)^{d/2}\right)$$

[11] t-Region-probing secure: NI, with t probes from *each* gadget

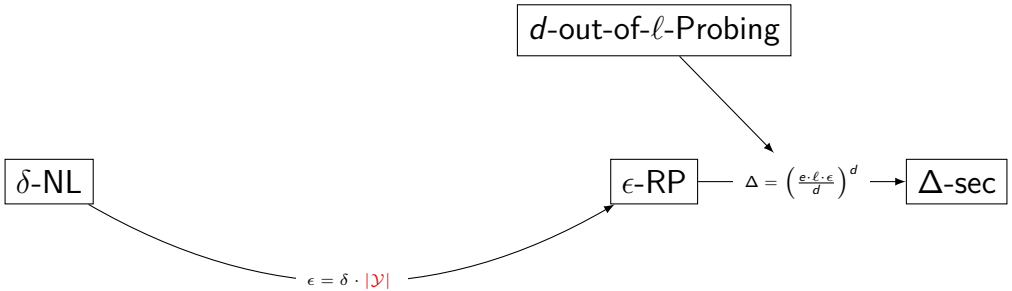
Wrap-Up of the Proof

δ-NL

Wrap-Up of the Proof

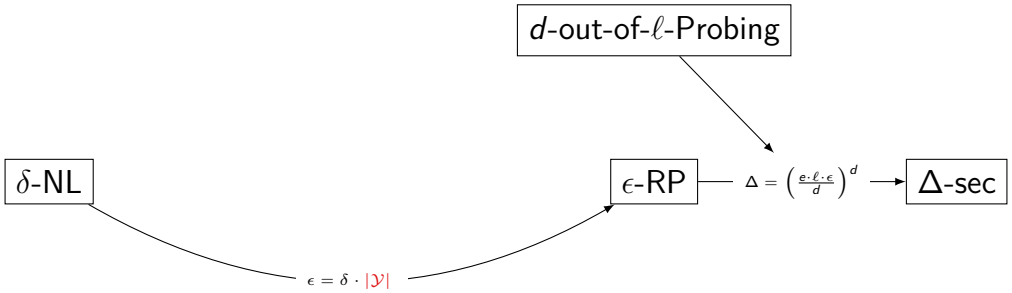


Wrap-Up of the Proof



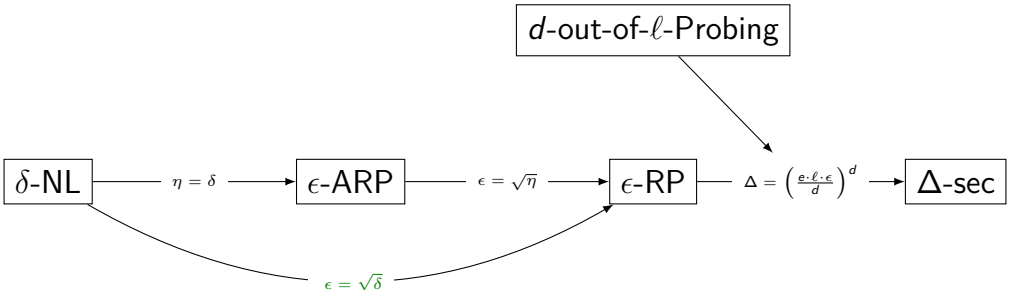
Wrap-Up of the Proof

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



Wrap-Up of the Proof

Bad *leakage rate* $\approx d \cdot |\mathbb{F}|$ ✗... but new reduction through *Average probing*[12] ✓



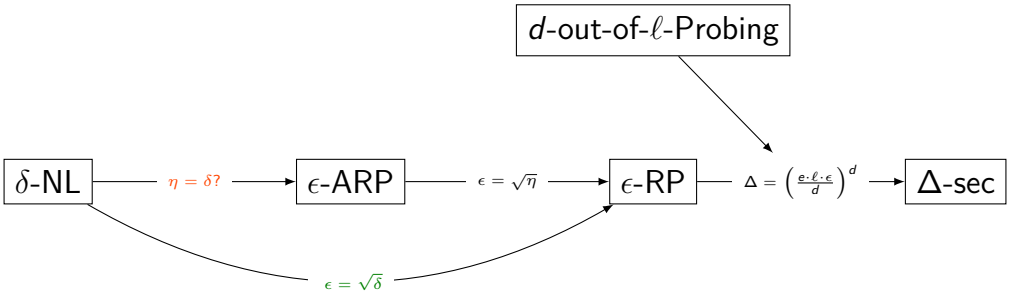
[12] Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence".

[13] Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited".

Wrap-Up of the Proof

Bad *leakage rate* $\approx d \cdot |\mathbb{F}|$ ✗... but new reduction through *Average probing*[12] ✓

Problem: Gap with the definition of ARP[13] ✗



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

[13] Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited".

Perspectives

- Fixing the reduction through Average Probing (work in progress)

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

Perspectives

- Fixing the reduction through Average Probing (work in progress)
- New constructions with leakage rates indep. of d[14]

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

Perspectives

- Fixing the reduction through Average Probing (work in progress)
- New constructions with leakage rates indep. of d[14]
- Masking PQC, *e.g.*, Kyber:

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

Perspectives

- Fixing the reduction through Average Probing (work in progress)
- New constructions with leakage rates indep. of d[14]
- Masking PQC, *e.g.*, Kyber:
  - ⋆ Unefficient masking through decomposition into circuit ✗

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

Perspectives

- Fixing the reduction through Average Probing (work in progress)
- New constructions with leakage rates indep. of d[14]
- Masking PQC, *e.g.*, Kyber:
  - ⋆ Unefficient masking through decomposition into circuit ✗
  - ⋆ Needs bigger gadgets with other paradigm: pre-computation tables ✓

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

Perspectives

- Fixing the reduction through Average Probing (work in progress)
- New constructions with leakage rates indep. of d[14]
- 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 ✗

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

Perspectives

- Fixing the reduction through Average Probing (work in progress)
- New constructions with leakage rates indep. of d[14]
- 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 ✗
  - ⋆ Masking-friendly schemes, *e.g.*, Raccoon ? ✓

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

Pointers

Interested ?

- Coron's keynote at CARDIS 23 on masking lattice-based cryptography
- Cassiers' keynote at COSADE 23 on masking composability
- Nicolas Bordes' thesis with nice examples of probing notions.

References I

Barthe, G. et al. "Strong Non-Interference and Type-Directed Higher-Order Masking". In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS '16. Vienna, Austria: Association for Computing Machinery, 2016, pp. 116129. ISBN: 9781450341394. DOI: 10.1145/2976749.2978427. URL: https://doi.org/10.1145/2976749.2978427.

References II

Béguinot, J. et al. "Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings". In: *Constructive Side-Channel Analysis and Secure Design - 14th International Workshop, COSADE 2023, Munich, Germany, April 3-4, 2023, Proceedings*. Ed. by E. B. Kavun and M. Pehl. Vol. 13979. Lecture Notes in Computer Science. Springer, 2023, pp. 86–104. DOI: 10.1007/978-3-031-29497-6_5. URL: https://doi.org/10.1007/978-3-031-29497-6_5.

References III

- 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.
- Bordes, N. "Security of symmetric primitives and their implementations". Theses. Université Grenoble Alpes [2020-....], Dec. 2021. URL: https://theses.hal.science/tel-03675249.

References IV

- 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.
- 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 V

- Cassiers, G. and F.-X. Standaert. "Trivially and Efficiently Composing Masked Gadgets With Probe Isolating Non-Interference". In: *IEEE Transactions on Information Forensics and Security* 15 (2020), pp. 2542–2555. DOI: 10.1109/TIFS.2020.2971153.
- 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.

References VI

- Coron, J. et al. "Higher-Order Side Channel Security and Mask Refreshing". In: *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*. Ed. by S. Moriai. Vol. 8424. Lecture Notes in Computer Science. Springer, 2013, pp. 410–424. DOI: 10.1007/978-3-662-43933-3_21. URL: https://doi.org/10.1007/978-3-662-43933-3_21.
- 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 VII

 Dziembowski, S., S. Faust, and M. Skorski. "Noisy Leakage Revisited". In: *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 II*. Ed. by E. Oswald and M. Fischlin. Vol. 9057. Lecture Notes in Computer Science. Springer, 2015, pp. 159–188. DOI: 10.1007/978-3-662-46803-6_6. URL: https://doi.org/10.1007/978-3-662-46803-6_6.

References VIII

 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.

References IX

 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 X

 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.