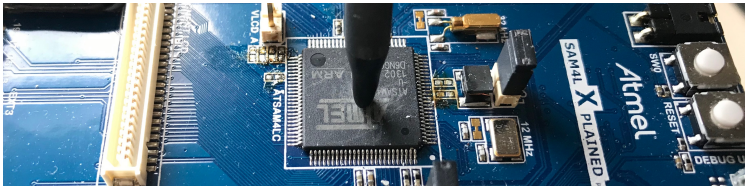


A Decade of Masking Security Proofs

Loïc Masure

WRACH, 23 Avril 2025, Roscoff

cnrs LIRMM UNIVERSITÉ DE MONTPELLIER

Agenda

Context: SCA & Security Evaluation

Masking

- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

Tight Reduction

Conclusion

Content

Context: SCA & Security Evaluation

Masking

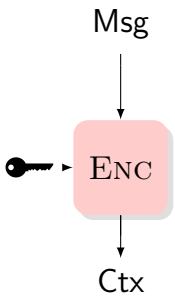
- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

Tight Reduction

Conclusion

Context : Side-Channel Analysis (SCA)

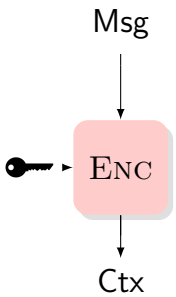


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

"Cryptographic algorithms don't run on paper,

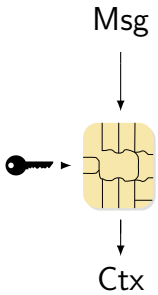


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

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

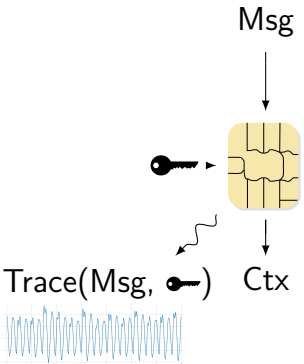


: N bits

Black-box cryptanalysis: 2^N

Context : Side-Channel Analysis (SCA)

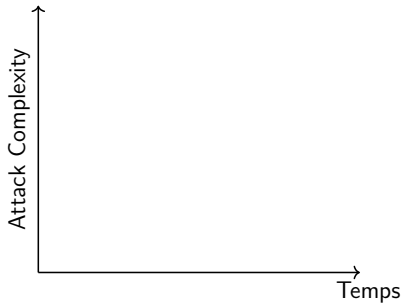
"Cryptographic algorithms don't run on paper, they run on physical devices"



: N bits

Black-box cryptanalysis: 2^N

Evaluate Security against Side-Channel Attacks

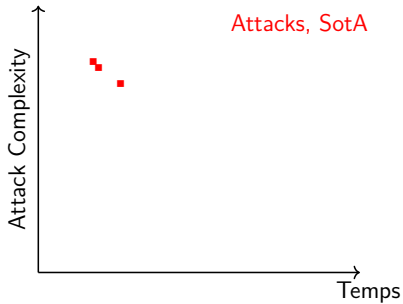


a

Attack approach (industry):

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks

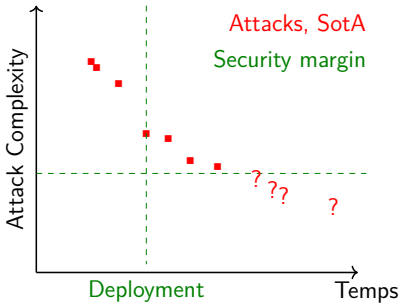


a

Attack approach (industry):
Current security level ✓

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



a

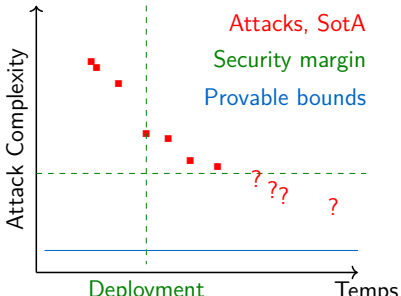
Attack approach (industry):

Current security level ✓

Future improvement → reevaluation ✗

[a] Shamelessly stolen to O. Bronchain

Evaluate Security against Side-Channel Attacks



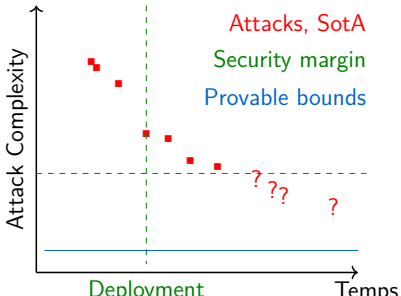
a

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

Context: SCA & Security Evaluation

Masking

- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

Tight Reduction

Conclusion

Content

Context: SCA & Security Evaluation

Masking

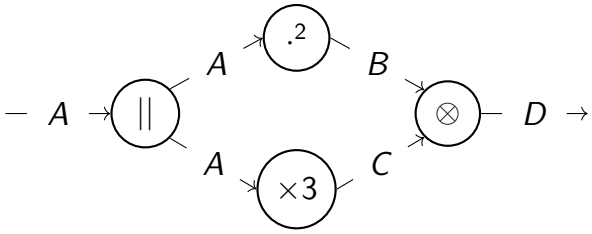
- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

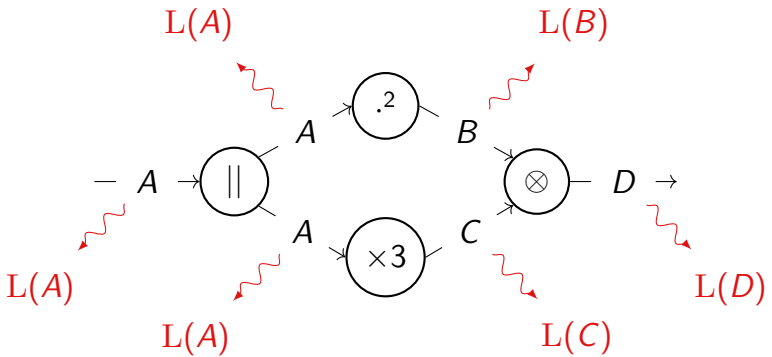
Tight Reduction

Conclusion

Statement of the Problem

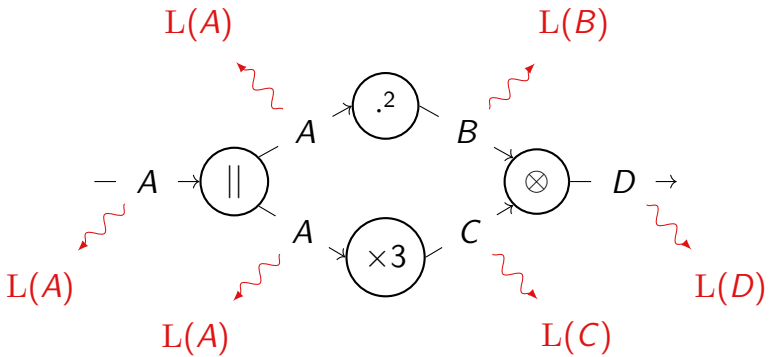


Statement of the Problem



For each wire X, a leakage function $\mathrm{L}(X)$ is revealed to the adversary.

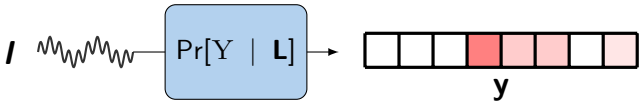
Statement of the Problem



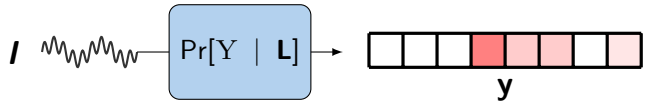
For each wire X, a leakage function $\mathrm{L}(X)$ is revealed to the adversary.

How informative **L** about A?

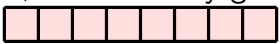
The Noisy Leakage Model



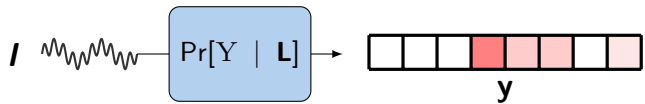
The Noisy Leakage Model



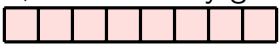
If, the adversary gets:



The Noisy Leakage Model

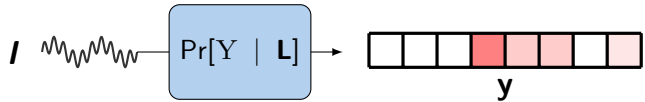


If, the adversary gets:



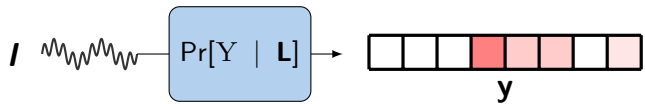
Very noisy leakage
Y indistinguishable from blind guess

The Noisy Leakage Model



If, the adversary gets:

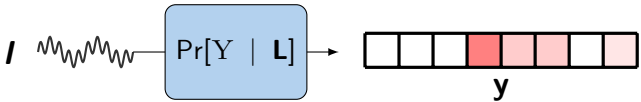
The Noisy Leakage Model



If, the adversary gets:

Low-noise leakage
Exact prediction for Y

The Noisy Leakage Model

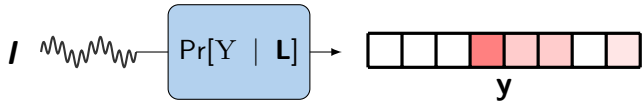


δ-NOISY ADVERSARY

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

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

The Noisy Leakage Model



δ-NOISY ADVERSARY

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

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

Main assumption: every observed leakage is δ-noisy

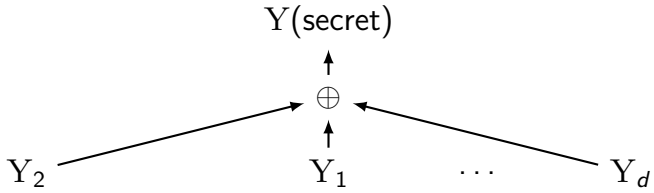
Masking: what is that ?

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

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

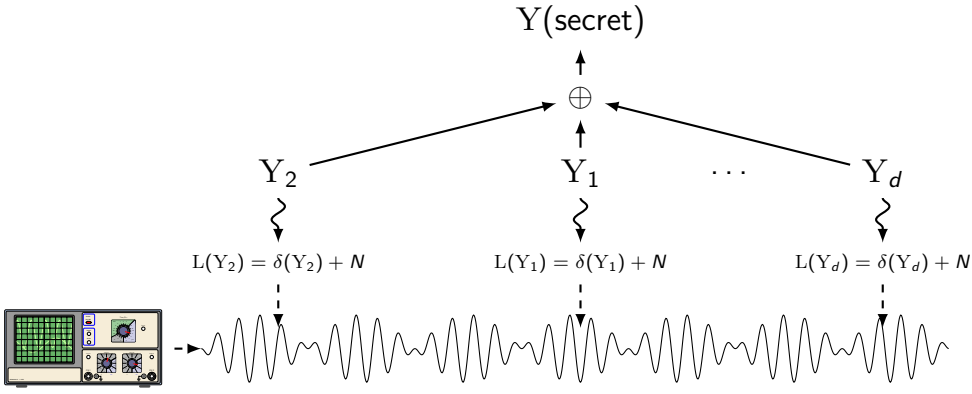
Masking: what is that ?

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



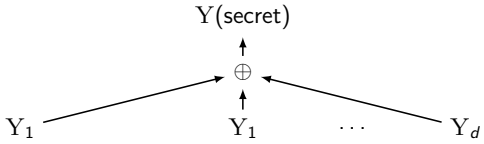
[1] Chari et al., "Towards Sound Approaches to Counteract Power-Analysis Attacks".

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

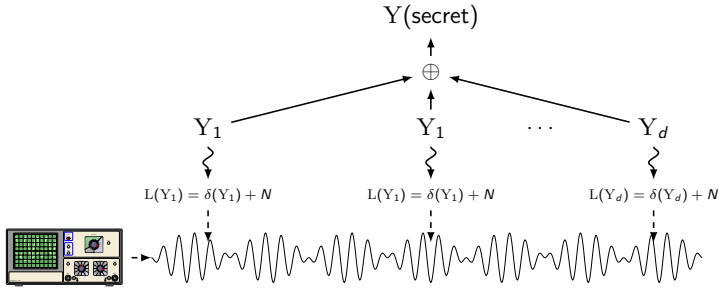
The Effect of Masking

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

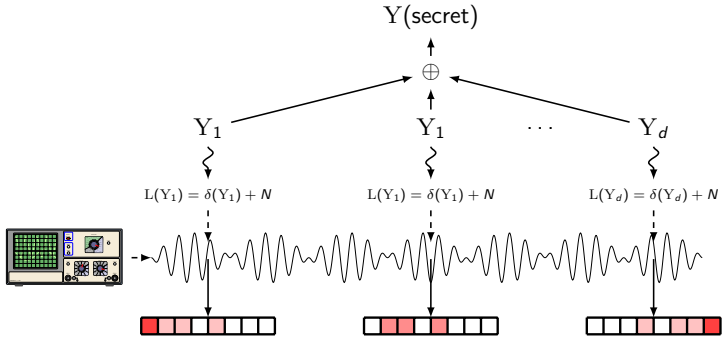
The Effect of Masking



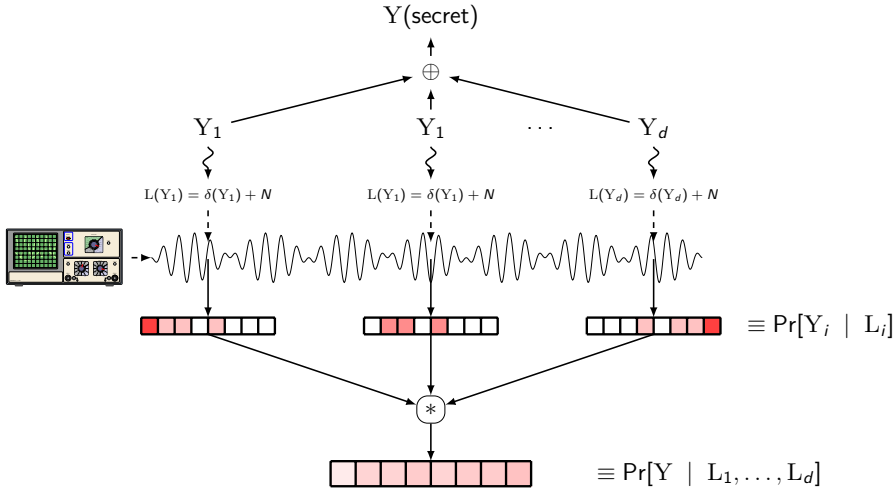
The Effect of Masking



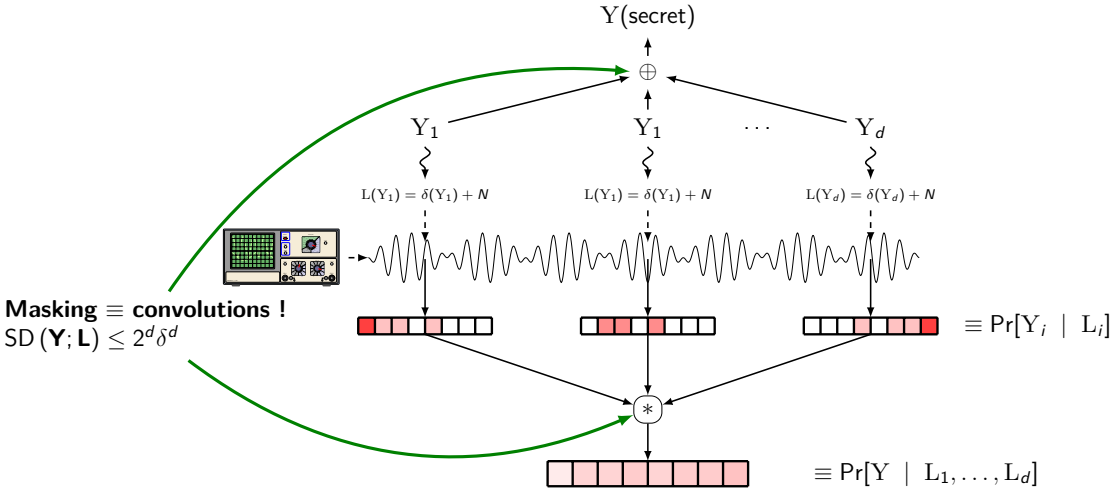
The Effect of Masking



The Effect of Masking



The Effect of Masking



Content

Context: SCA & Security Evaluation

Masking

- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

Tight Reduction

Conclusion

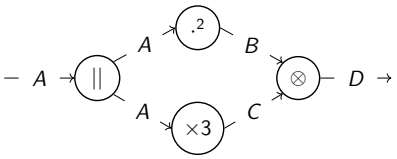
Computing over Masked Secrets

Idea to make a masked circuit

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

Computing over Masked Secrets

Idea to make a masked circuit

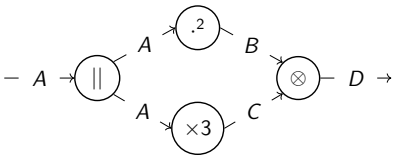


- View your algorithm as a circuit

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

Computing over Masked Secrets

Idea to make a masked circuit

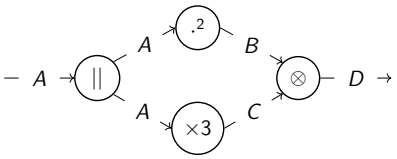


· View your algorithm as a circuit
→ Made of `not`, `and` gates [3]

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

Computing over Masked Secrets

Idea to make a masked circuit

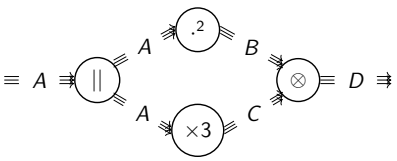


- View your algorithm as a circuit
  → Made of `not`, `and` gates [3]
  → Made of $\oplus, \otimes$ gates [4]

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

Computing over Masked Secrets

Idea to make a masked circuit

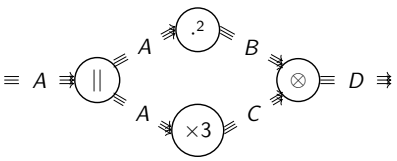


- View your algorithm as a circuit
  - → Made of `not`, `and` gates [3]
  - → Made of $\oplus, \otimes$ gates [4]
- Replace each gate by a masked *gadget*

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

Computing over Masked Secrets

Idea to make a masked circuit



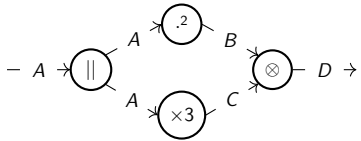
- View your algorithm as a circuit
  → Made of `not`, `and` gates [3]
  → Made of $\oplus, \otimes$ gates [4]
- Replace each gate by a masked *gadget*
- Et voilà !**

For now, let's assume the whole circuit to be *probing secure*: every subset of $d-1$ wires is independent from the secret.

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

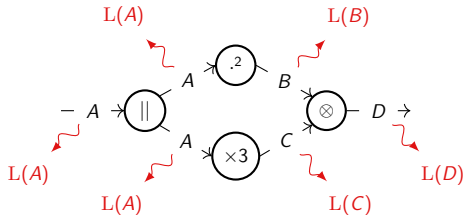
Security Proof for a Gadget

Consider a gadget with ℓ intermediate computations:



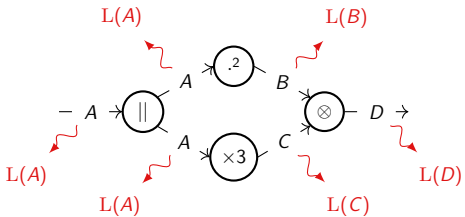
Security Proof for a Gadget

Consider a gadget with ℓ δ-noisy intermediate computations:



Security Proof for a Gadget

Consider a gadget with ℓ δ-noisy intermediate computations:

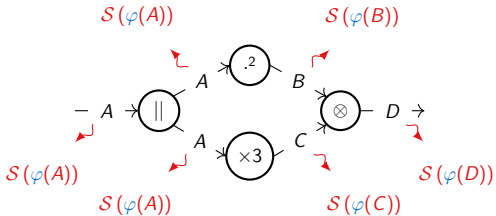


Data-processing Inequality

If for any x the leakage function $\mathrm{L}(x)$

Security Proof for a Gadget

Consider a gadget with ℓ δ-noisy intermediate computations:

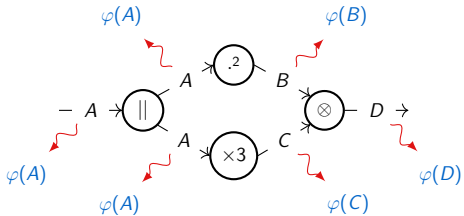


Data-processing Inequality

If for any x the leakage function $\mathrm{L}(x)$ may be expressed as $\mathcal{S}(\varphi(x))$,

Security Proof for a Gadget

Consider a gadget with ℓ δ-noisy intermediate computations:



Data-processing Inequality

If for any x the leakage function $\mathrm{L}(x)$ may be expressed as $\mathcal{S}(\varphi(x))$, then: advantage from $\mathrm{L}(x) \leq$ advantage from $\varphi(x)$

Reduction from Noisy Leakage to Random Probing

Lemma (Simulatability by Random Probing)

The leakage function L *can be simulated from a random probing adversary:* $\varphi(x)$ *reveals* x *with probability* $\epsilon = 1 - \sum_l \min_x \Pr[\mathrm{L}(x) = l] \leq \delta \cdot |\mathbb{F}|$.[5]

Random probing model: easier to analyze for leakage from computations

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

Security against a Random Probing Adversary

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

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

[6] 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[6])

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

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

[6] 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:

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

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:

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

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

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

Main Challenge

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

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

Main challenge: get rid of the three factors d, $|\mathsf{C}|$, and $|\mathbb{F}|$

Main Challenge

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

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

Main challenge: get rid of the three factors d, $|\mathsf{C}|$, and $|\mathbb{F}|$

- d: Abdel's thesis

Main Challenge

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

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

Main challenge: get rid of the three factors d, $|\mathsf{C}|$, and $|\mathbb{F}|$

- d: Abdel's thesis
- $|\mathsf{C}|$: this talk (a bit) and Melissa's talk (more in depth)

Main Challenge

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

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

Main challenge: get rid of the three factors d, $|\mathsf{C}|$, and $|\mathbb{F}|$

- d: Abdel's thesis
- $|\mathsf{C}|$: this talk (a bit) and Melissa's talk (more in depth)
- $|\mathbb{F}|$: this talk (a bit, work in progress)

Main Challenge

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

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

Main challenge: get rid of the three factors d, $|\mathsf{C}|$, and $|\mathbb{F}|$

- d: Abdel's thesis
- $|\mathsf{C}|$: this talk (a bit) and Melissa's talk (more in depth)
- $|\mathbb{F}|$: this talk (a bit, work in progress)

A few numbers:

$$d(2, 3, 4, ..., 16) \ll |\mathsf{C}|(\approx 10^3, 10^5), |\mathbb{F}|(256, 2^{23}, 2^{50})$$

Content

Context: SCA & Security Evaluation

Masking

- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

Tight Reduction

Conclusion

Setting

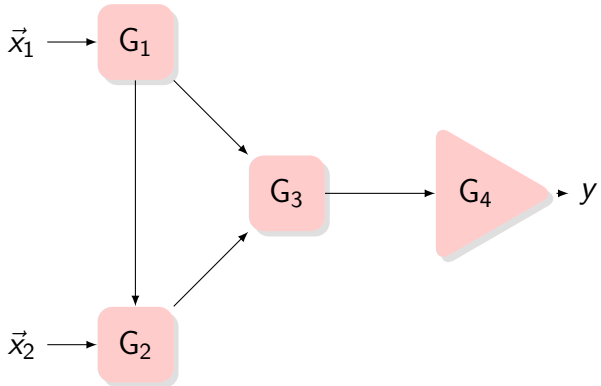


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget.

Setting

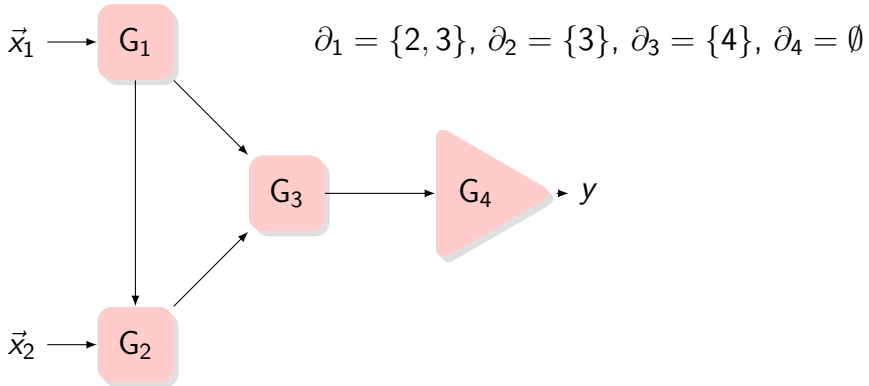


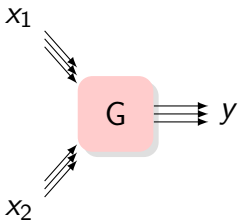
Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget.

∂_i: set of all subsequent gadgets linked to G_i

Strong Non-Interference[8]

Definition (t-Strong Non-Interference)

A gadget G is t-SNI



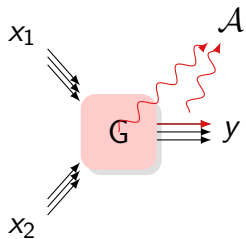
[7] Must be connected to different gadgets ✓

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

Strong Non-Interference[8]

Definition (t-Strong Non-Interference)

A gadget G is t-SNI if any set W^{G} of internal probes and any set J^{G} of output probes such that $\left|W^{\mathsf{G}}\right| + \left|J^{\mathsf{G}}\right| \leq t$



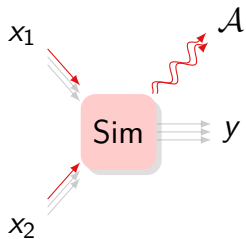
[7] Must be connected to different gadgets ✓

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

Strong Non-Interference[8]

Definition (t-Strong Non-Interference)

A gadget G is t-SNI if any set W^{G} of internal probes and any set J^{G} of output probes such that $\left|W^{\mathsf{G}}\right| + \left|J^{\mathsf{G}}\right| \leq t$ can be simulated with at most $\left|I^{\mathsf{G}}\right| \leq \left|W^{\mathsf{G}}\right|$ shares of each input sharing



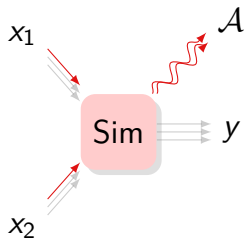
[7] Must be connected to different gadgets ✓

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

Strong Non-Interference[8]

Definition (t-Strong Non-Interference)

A gadget G is t-SNI if any set W^{G} of internal probes and any set J^{G} of output probes such that $\left|W^{\mathsf{G}}\right| + \left|J^{\mathsf{G}}\right| \leq t$ can be simulated with at most $\left|I^{\mathsf{G}}\right| \leq \left|W^{\mathsf{G}}\right|$ shares of each input sharing



→ Composable : circ. SNI iff all gadgets SNI
→ SNI $\implies$ probing security
→ Extends to multiple outputs[7]

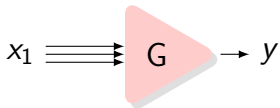
[7] Must be connected to different gadgets ✓

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

Non-Interference with Public Outputs[10]

Definition (t-NIo)

A gadget is t-NIo

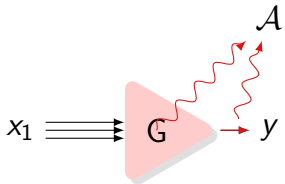


[9] Coron et al., *High-order Polynomial Comparison and Masking Lattice-based Encryption*
[10] Barthe et al., "Masking the GLP Lattice-Based Signature Scheme at Any Order".

Non-Interference with Public Outputs[10]

Definition (t-NIo)

A gadget is t-NIo if any set of $t_1 \leq t$ internal probes and the output

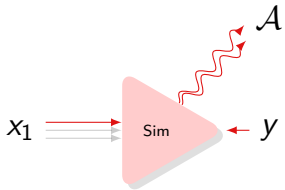


[9] Coron et al., *High-order Polynomial Comparison and Masking Lattice-based Encryption*
[10] Barthe et al., "Masking the GLP Lattice-Based Signature Scheme at Any Order".

Non-Interference with Public Outputs[10]

Definition (t-NIo)

A gadget is t-NIo if any set of $t_1 \leq t$ internal probes and the output can be jointly simulated from the output and at most t_1 input shares

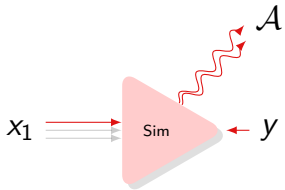


[9] Coron et al., *High-order Polynomial Comparison and Masking Lattice-based Encryption*
[10] Barthe et al., "Masking the GLP Lattice-Based Signature Scheme at Any Order".

Non-Interference with Public Outputs[10]

Definition (t-NIo)

A gadget is t-NIo if any set of $t_1 \leq t$ internal probes and the output can be jointly simulated from the output and at most t_1 input shares



$\rightarrow$ Output assumed to be public anyway
$\rightarrow$ Built from strong Refreshing [9]

[9] Coron et al., *High-order Polynomial Comparison and Masking Lattice-based Encryption*
[10] Barthe et al., "Masking the GLP Lattice-Based Signature Scheme at Any Order".

Composition Theorem

Theorem

Assume: (1) Each output gadget $(d-1)$*-Nlo;*

Composition Theorem

Theorem

Assume: (1) Each output gadget $(d-1)$*-NIo; (2) Each internal gadget* t_i*-SNI;*

Composition Theorem

Theorem

Assume: (1) Each output gadget $(d-1)$*-NIo; (2) Each internal gadget* t_i*-SNI; (3) Each copy gadget connected to different gadgets;*

Composition Theorem

Theorem

Assume: (1) Each output gadget $(d-1)$-NIo; (2) Each internal gadget t_i-SNI; (3) Each copy gadget connected to different gadgets; then, C is secure with proba $\geq 1-\eta$ such that:

$$\eta \leq \sum_{\substack{i=1 \\ G_i \text{ not output}}}^{|C|} \left(e \cdot \frac{|G_i| + \sum_{j \in \partial_i} |G_j|}{t_i + 1} \cdot \epsilon \right)^{t_i+1}.$$

Composition Theorem

Theorem

Assume: (1) Each output gadget $(d-1)$-NIo; (2) Each internal gadget t_i-SNI; (3) Each copy gadget connected to different gadgets; then, C is secure with proba $\geq 1-\eta$ such that:

$$\eta \leq \sum_{\substack{i=1 \\ G_i \text{ not output}}}^{|\mathsf{C}|} \left(e \cdot \frac{|G_i| + \sum_{j \in \partial_i} |G_j|}{t_i + 1} \cdot \epsilon \right)^{t_i+1}.$$

Corollary

The d-share ISW compiler is $|\mathsf{C}| \cdot (\mathcal{O}(d) \cdot |\mathbb{F}| \cdot \delta)^d$-noisy leakage secure

Proof Sketch

Apply SNI simulator gadget-wise, in reversed order, until complete or failure

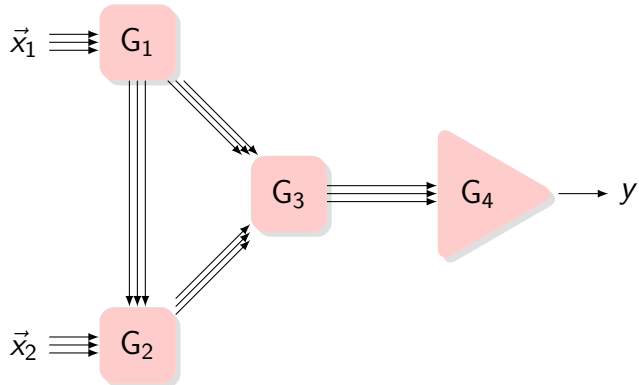


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Apply SNI simulator gadget-wise, in reversed order, until complete or failure

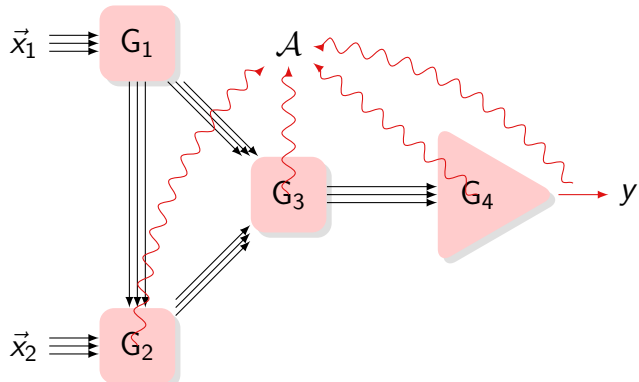


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Apply SNI simulator gadget-wise, in reversed order, until complete or failure

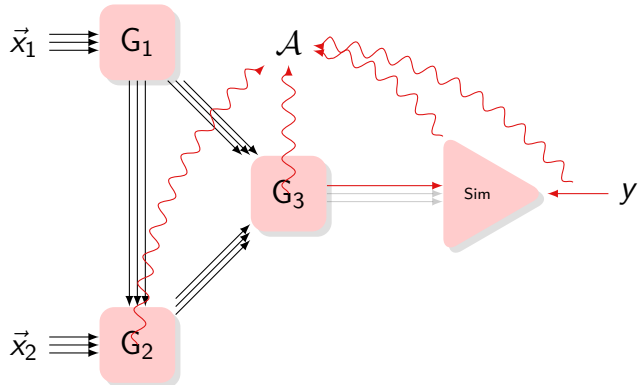


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Apply SNI simulator gadget-wise, in reversed order, until complete or failure

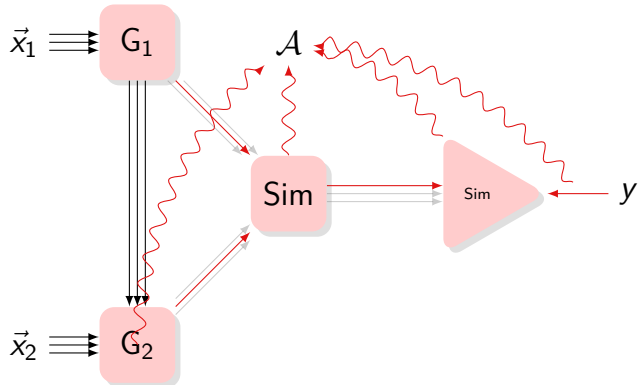


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Apply SNI simulator gadget-wise, in reversed order, until complete or failure

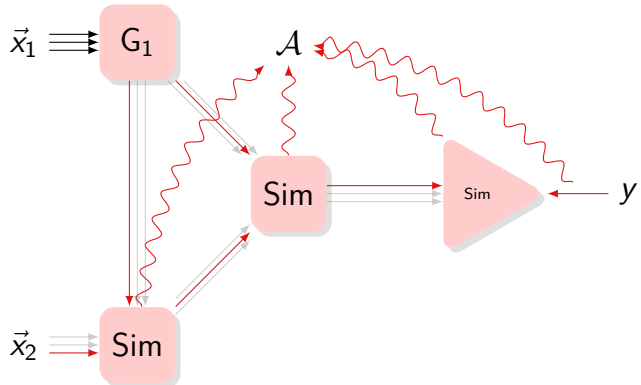


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Apply SNI simulator gadget-wise, in reversed order, until complete or failure

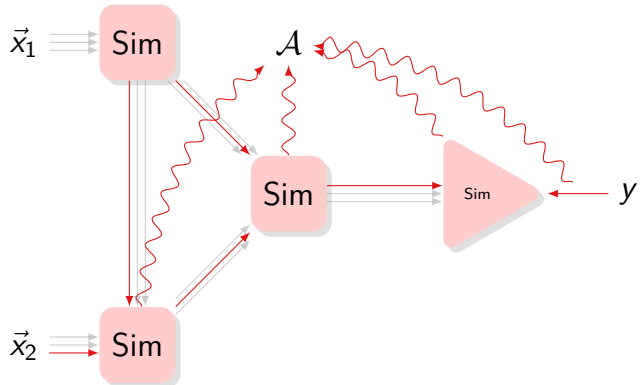


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Failure may happen (simulation with abort)

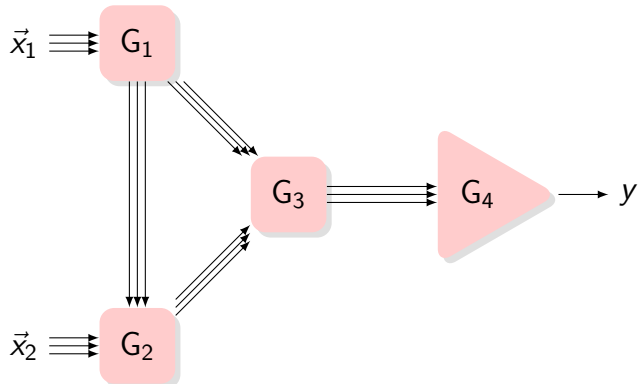


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Failure may happen (simulation with abort)

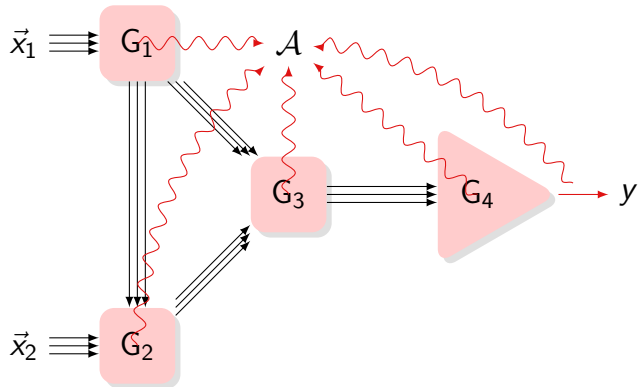


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Failure may happen (simulation with abort)

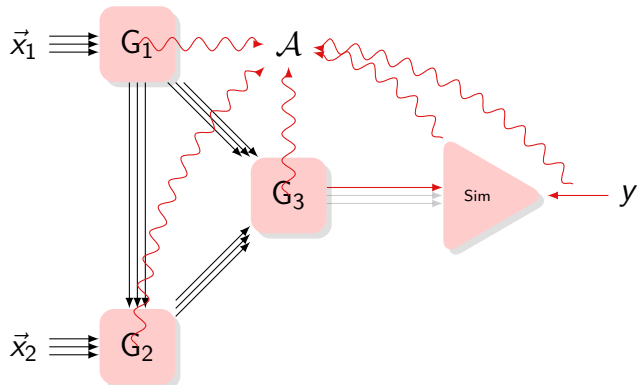


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Failure may happen (simulation with abort)

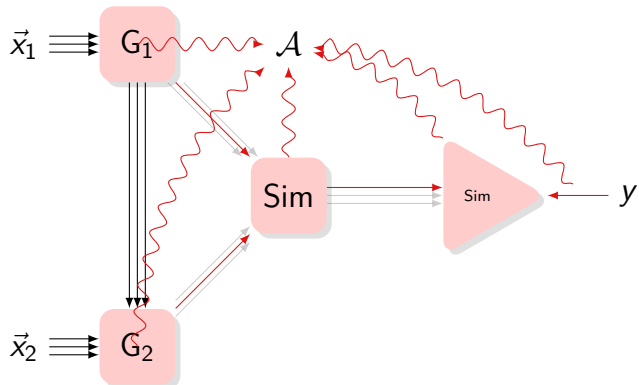


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Failure may happen (simulation with abort)

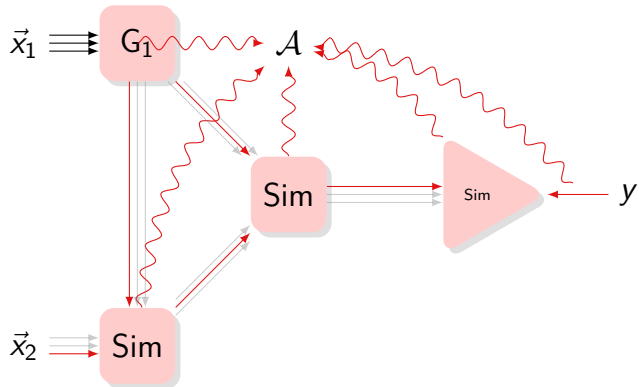


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

Proof Sketch

Failure may happen (simulation with abort)

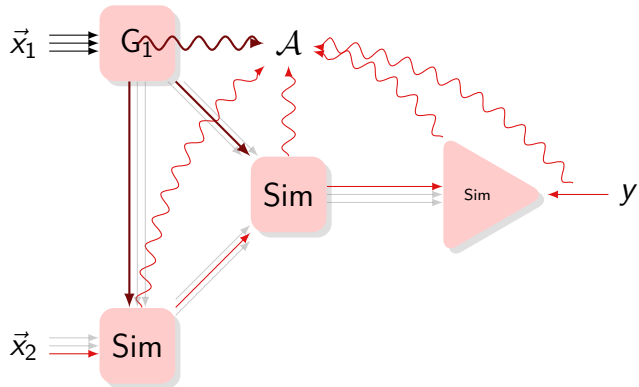


Figure: G_1: SNI copy gadget, G_2, G_3: SNI gadgets, G_4: NIo gadget. $\partial_1 = \{2, 3\}$, $\partial_2 = \{3\}$, $\partial_3 = \{4\}$, $\partial_4 = \emptyset$

How Often Does It Fail?

Let bad_i: "simulation failure at step i". This implies:

[11] If G_j is an NIo output gadget, this is also verified.

How Often Does It Fail?

Let bad_i: "simulation failure at step i". This implies:

$\rightarrow$ t_i-SNI assumption of G_i not verified: $\left|W^{G_i}\right| + \sum_{j \in \partial_i} \left|J_j^{G_i}\right| \geq t_i$

[11] If G_j is an NIo output gadget, this is also verified.

How Often Does It Fail?

Let bad_i: "simulation failure at step i". This implies:

$\rightarrow$ t_i-SNI assumption of G_i not verified: $\left|W^{G_i}\right| + \sum_{j \in \partial_i} \left|J_j^{G_i}\right| \geq t_i$

$\rightarrow$ $\forall j > i$, t_j-SNI assumption of G_j verified, thereby $\left|J_j^{G_i}\right| = \left|I_i^{G_j}\right| \leq \left|W^{G_j}\right|$[11]

[11] If G_j is an NIo output gadget, this is also verified.

How Often Does It Fail?

Let bad_i: "simulation failure at step i". This implies:

$\rightarrow$ t_i-SNI assumption of G_i not verified: $\left|W^{G_i}\right| + \sum_{j \in \partial_i} \left|J_j^{G_i}\right| \geq t_i$

$\rightarrow$ $\forall j > i$, t_j-SNI assumption of G_j verified, thereby $\left|J_j^{G_i}\right| = \left|I_i^{G_j}\right| \leq \left|W^{G_j}\right|$[11]

Hence,

$$\Pr[\mathsf{bad}_i] \leq \Pr\left[\left|W^{G_i}\right| + \sum_{j \in \partial_i} \left|W^{G_j}\right| \geq t_i\right]$$

Using the union bound:

$$\eta = \sum_{\substack{i=1 \\ G_i \text{not output}}}^{|\mathsf{C}|} \Pr[\mathsf{bad}_i]$$

[11] If G_j is an NIo output gadget, this is also verified.

Concluding the Proof

Using Chernoff:

$$\Pr\left[\left|W^{G_i}\right| + \sum_{j\in\partial_i}\left|W^{G_j}\right| > t_i\right] = \Pr\left[\left|W^{G_i} \cup \left(\bigcup_{j\in\partial_i} W^{G_j}\right)\right| \geq t_i + 1\right]$$
$$\leq \left(e \cdot \frac{|G_i| + \sum_{j\in\partial_i}|G_j|}{t_i + 1} \cdot \epsilon\right)^{t_i+1}.$$

Comparison with Previous Works

So far, trade-off was needed (see next talk):

$\rightarrow$ Duc *et al.*:[12] $|\mathsf{C}| \cdot (\mathcal{O}(d) \cdot |\mathbb{F}| \cdot \delta)^{d/2}$

$\rightarrow$ Belaïd *et al.*:[13] $|\mathsf{C}| \cdot (\mathcal{O}(1) \cdot |\mathbb{F}| \cdot \delta)^{\approx d/3}$

$\rightarrow$ Next talk: tighter and more generic way to compose

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

[13] Taleb, "Secure and Verified Cryptographic Implementations in the Random Probing Model. (Implémentations cryptographiques sûres et vérifiées dans le modèle random probing)".

Content

Context: SCA & Security Evaluation

Masking

- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

Tight Reduction

Conclusion

Noisy-to-Random Reduction

Lemma (Simulatability by Random Probing[14]*)*

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

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

Noisy-to-Random Reduction

Lemma (Simulatability by Random Probing[14]*)*

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

$\rightarrow$ Tight w.r.t. $|\mathbb{F}|$ ✗

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

Noisy-to-Random Reduction

Lemma (Simulatability by Random Probing[14]*)*

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

→ Tight w.r.t. $|\mathbb{F}|$ ✗

→ Holds for any $x \in \mathbb{F}$ $\iff$ holds for any arbitrarily distributed r.v. $X \leftarrow\!\!\$\ \mathbb{F}$

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

Noisy-to-Random Reduction

Lemma (Simulatability by Random Probing[14]*)*

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

→ Tight w.r.t. $|\mathbb{F}|$ ✗

→ Holds for any $x \in \mathbb{F}$ $\iff$ holds for any arbitrarily distributed r.v. $X \leftarrow\!\!\$\ \mathbb{F}$

→ Equivalently, holds at the scale of the whole circuit, for *any* joint distribution $X_1, \ldots, X_\ell$ of the wires ✓✓

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

Noisy-to-Random Reduction

Lemma (Simulatability by Random Probing[14]*)*

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

→ Tight w.r.t. $|\mathbb{F}|$ ✗

→ Holds for any $x \in \mathbb{F}$ $\iff$ holds for any arbitrarily distributed r.v. $X \leftarrow\!\!\$\ \mathbb{F}$

→ Equivalently, holds at the scale of the whole circuit, for *any* joint distribution $X_1, \ldots, X_\ell$ of the wires ✓✓

Is it too much ?

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

The Average Random Probing Model

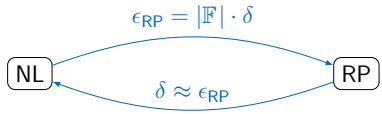
The Average Random Probing Model

NL

RP

[14] Blue: Duc, Dziembowski, and Faust, "Unifying Leakage Models: From Probing Attacks to Noisy Leakage",
Green: Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited",
Brown: Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence"

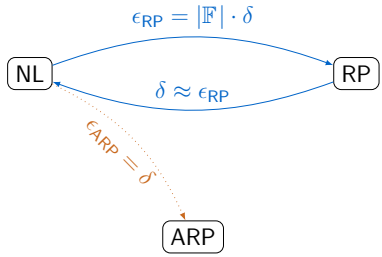
The Average Random Probing Model



[14] Blue: Duc, Dziembowski, and Faust, "Unifying Leakage Models: From Probing Attacks to Noisy Leakage",
Green: Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited",
Brown: Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence"

The Average Random Probing Model

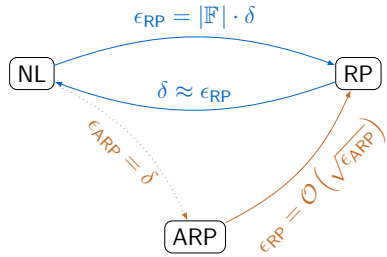
- **ARP** (EC'24): $\varphi(x) = x$ with proba. ϵ_x



[14] Blue: Duc, Dziembowski, and Faust, "Unifying Leakage Models: From Probing Attacks to Noisy Leakage",
Green: Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited",
Brown: Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence"

The Average Random Probing Model

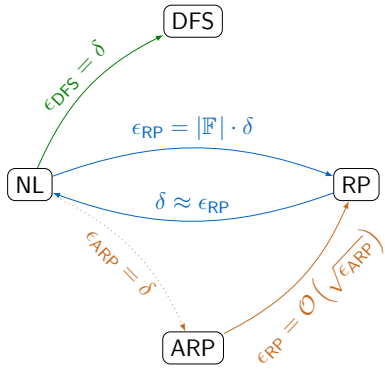
- **ARP** (EC'24): $\varphi(x) = x$ with proba. ϵ_x



[14] Blue: Duc, Dziembowski, and Faust, "Unifying Leakage Models: From Probing Attacks to Noisy Leakage",
Green: Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited",
Brown: Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence"

The Average Random Probing Model

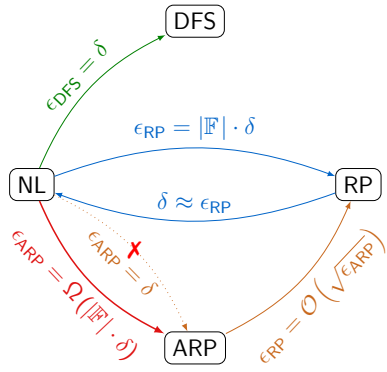
- **ARP** (EC'24): $\varphi(x) = x$ with proba. ϵ_x
- **DFS-ARP** (EC'15): $\varphi(x)$ reveals x with proba. ϵ_x, *and* some internal randomness



[14] Blue: Duc, Dziembowski, and Faust, "Unifying Leakage Models: From Probing Attacks to Noisy Leakage",
Green: Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited",
Brown: Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence"

The Average Random Probing Model

- **ARP** (EC'24): $\varphi(x) = x$ with proba. ϵ_x
- **DFS-ARP** (EC'15): $\varphi(x)$ reveals x with proba. ϵ_x, *and* some internal randomness



[14] Blue: Duc, Dziembowski, and Faust, "Unifying Leakage Models: From Probing Attacks to Noisy Leakage",
Green: Dziembowski, Faust, and Skorski, "Noisy Leakage Revisited",
Brown: Brian, Dziembowski, and Faust, "From Random Probing to Noisy Leakages Without Field-Size Dependence"

Technical Results

Theorem (ARP-Simulability)

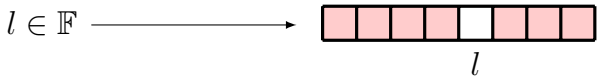
L *is simulable in the* $\{\epsilon_x\}_x$ *average random probing model iff*[15]

$$1 \leq \sum_l \min_{x' : \epsilon_{x'} < 1} \left\{ \frac{\Pr[\mathrm{L}(x') = l]}{1 - \epsilon_{x'}} \right\}$$

Remark: if ϵ_x constant, we get back the RP lemma
Proof: see appendix

[15] One needs at least one $\epsilon_x < 1$ for non-trivial simulation

The Catastrophic Channel, a.k.a., the *evil* function[16]



Equivalently:

$$\Pr[\mathrm{L}(x) = l] = \begin{cases} 0 & \text{if } x = l, \\ \frac{1}{|\mathbb{F}|-1} & \text{otherwise} \end{cases}$$

Here, $\delta = \frac{1}{|\mathbb{F}|}$, but $\epsilon = \mathop{\mathbb{E}}_{x}[\epsilon_x] \geq \frac{1}{2}$

$$\text{Hence, } \frac{\epsilon}{\delta} \geq \Omega\left(|\mathbb{F}|\right) \text{ ✗}$$

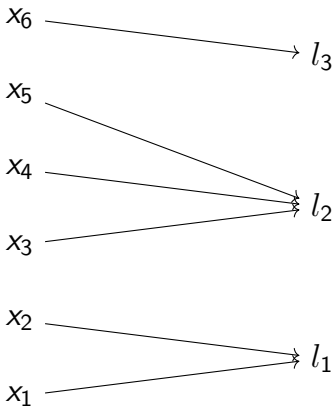
[16] Thus named by Gianluca Brian, as it appears as a worst-case in another of their works

Deterministic Leakage Functions

We can characterize the optimal simulator:

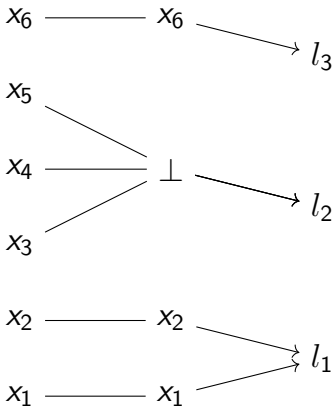
Deterministic Leakage Functions

We can characterize the optimal simulator:



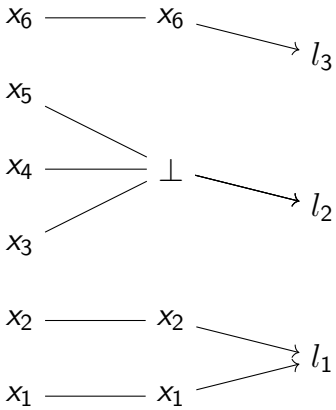
Deterministic Leakage Functions

We can characterize the optimal simulator:



Deterministic Leakage Functions

We can characterize the optimal simulator:



$$\epsilon = \mathop{\mathbb{E}}_{x}[\epsilon_x] = 1 - \frac{\max_l |\{x : \mathrm{L}(x) = l\}|}{|\mathbb{F}|}$$
$$\leq 1 - \frac{\mathop{\mathbb{E}}_{l}[|\{x : \mathrm{L}(x) = l\}|]}{|\mathbb{F}|}$$
$$= \delta$$

Content

Context: SCA & Security Evaluation

Masking

- Background & Intuitions
- Provably Secure Masking

Composition in the Random Probing Model

Tight Reduction

Conclusion

Conclusion

Research strategy in masking security proofs:

Conclusion

Research strategy in masking security proofs:

- Always good to start tackling a problem by simpler sides

Conclusion

Research strategy in masking security proofs:

- Always good to start tackling a problem by simpler sides
- Gives good intuitions

Conclusion

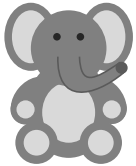
Research strategy in masking security proofs:

- Always good to start tackling a problem by simpler sides
- Gives good intuitions
- Risk: forgetting the big picture (noisy leakage)

Conclusion

Research strategy in masking security proofs:

- Always good to start tackling a problem by simpler sides
- Gives good intuitions
- Risk: forgetting the big picture (noisy leakage)



Main priority (IMHO):

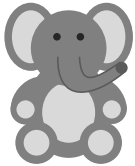
$\rightarrow$ Either improving reductions to random probing

$\rightarrow$ Or working directly in the noisy leakage

Conclusion

Research strategy in masking security proofs:

- Always good to start tackling a problem by simpler sides
- Gives good intuitions
- Risk: forgetting the big picture (noisy leakage)



Main priority (IMHO):

$\rightarrow$ Either improving reductions to random probing

$\rightarrow$ Or working directly in the noisy leakage

No easy fix currently ...

Conclusion

Research strategy in masking security proofs:

- Always good to start tackling a problem by simpler sides
- Gives good intuitions
- Risk: forgetting the big picture (noisy leakage)

Main priority (IMHO):

$\rightarrow$ Either improving reductions to random probing

$\rightarrow$ Or working directly in the noisy leakage

No easy fix currently ...

Join us in this line of research !

References I

- Barthe, G. et al. "Masking the GLP Lattice-Based Signature Scheme at Any Order". In: *J. Cryptol.* 37.1 (2024), p. 5. DOI: 10.1007/S00145-023-09485-Z. URL: https://doi.org/10.1007/s00145-023-09485-z.
- 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, 116–129. ISBN: 9781450341394. DOI: 10.1145/2976749.2978427. URL: https://doi.org/10.1145/2976749.2978427.

References II

- 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 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.
- Coron, J.-S. et al. *High-order Polynomial Comparison and Masking Lattice-based Encryption*. Cryptology ePrint Archive, Paper 2021/1615. 2021. URL: https://eprint.iacr.org/2021/1615.

References IV

- 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.
- 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 V


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 VI


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 VII

- 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.
- Taleb, A. R. "Secure and Verified Cryptographic Implementations in the Random Probing Model. (Implémentations cryptographiques sûres et vérifiées dans le modèle random probing)". PhD thesis. Sorbonne University, Paris, France, 2023. URL: https://tel.archives-ouvertes.fr/tel-04457258.

Reduction from Noisy Leakage to Random Probing (I)

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

Reduction from Noisy Leakage to Random Probing (I)

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

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

Constraints:

Reduction from Noisy Leakage to Random Probing (I)

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

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

Constraints:

$\rightarrow$ For all input x, $\Pr[\mathcal{S}(x)]$ should be a p.m.f.

Reduction from Noisy Leakage to Random Probing (I)

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

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

Constraints:

$\rightarrow$ For all input x, $\Pr[\mathcal{S}(x)]$ should be a p.m.f.

$\rightarrow$ For the input $\perp$, $\Pr[\mathcal{S}(\perp)]$ should be a p.m.f.

Reduction from Noisy Leakage to Random Probing (I)

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

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

Constraints:

$\rightarrow$ For all input x, $\Pr[\mathcal{S}(x)]$ should be a p.m.f.

$\rightarrow$ For the input $\perp$, $\Pr[\mathcal{S}(\perp)]$ should be a p.m.f.

$\rightarrow$ For any x, l, $\Pr[\mathcal{S}(\varphi(x)) = l] = \Pr[\mathrm{L}(x) = l]$

Reduction from Noisy Leakage to Random Probing (II)

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

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

Reduction from Noisy Leakage to Random Probing (II)

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

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

Reduction from Noisy Leakage to Random Probing (II)

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

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

Reduction from Noisy Leakage to Random Probing (II)

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

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

Hence,

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

Reduction from Noisy Leakage to Random Probing (II)

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

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

Hence,

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

Reduction from Noisy Leakage to Random Probing (II)

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

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

Hence,

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

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

Reduction from Noisy Leakage to Random Probing (II)

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

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

Hence,

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

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

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

Reduction from Noisy Leakage to RP (III)

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

In other words,

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

In other words,

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

Furthermore, summing (3) over l, by definition of probability distributions,

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

In other words,

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

Furthermore, summing (3) over l, by definition of probability distributions,

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

In other words,

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

Furthermore, summing (3) over l, by definition of probability distributions,

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

Hence,

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

In other words,

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

Furthermore, summing (3) over l, by definition of probability distributions,

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

Hence, to have the smallest ϵ,

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

Reduction to Average Random Probing (I)

For any x and any l:

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

Reduction to Average Random Probing (I)

For any x and any l:

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

Reduction to Average Random Probing (I)

For any x and any l:

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

Reduction to Average Random Probing (I)

For any x and any l:

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

Hence, provided that $\epsilon_x < 1$,

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

Reduction to Average Random Probing (I)

For any x and any l:

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

Hence, provided that $\epsilon_x < 1$,

$$0 \leq \Pr[\mathcal{S}(\bot) = l] = \frac{\overbrace{\Pr[\mathrm{L}(x) = l] - \epsilon_x \cdot \Pr[\mathcal{S}(x) = l]}^{\text{Should not depend on } X}}{1 - \epsilon_x} = \frac{\pi(l, x)}{1 - \epsilon_x} \quad (3)$$

Reduction to Average Random Probing (I)

For any x and any l:

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

Hence, provided that $\epsilon_x < 1$,

$$0 \leq \Pr[\mathcal{S}(\perp) = l] = \frac{\overbrace{\Pr[\mathrm{L}(x) = l] - \epsilon_x \cdot \Pr[\mathcal{S}(x) = l]}^{\text{Should not depend on } x}}{1 - \epsilon_x} = \frac{\pi(l, x)}{1 - \epsilon_x} \quad (3)$$

$$0 \leq \Pr[\mathcal{S}(x) = l] = \frac{\Pr[\mathrm{L}(x) = l] - \pi(l, x)}{\epsilon_x} \quad (4)$$

Reduction to Average Random Probing (I)

For any x and any l:

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

Hence, provided that $\epsilon_x < 1$,

$$0 \leq \Pr[\mathcal{S}(\perp) = l] = \frac{\overbrace{\Pr[\mathrm{L}(x) = l] - \epsilon_x \cdot \Pr[\mathcal{S}(x) = l]}^{\text{Should not depend on } x}}{1 - \epsilon_x} = \frac{\pi(l, x)}{1 - \epsilon_x} \quad (3)$$

$$0 \leq \Pr[\mathcal{S}(x) = l] = \frac{\Pr[\mathrm{L}(x) = l] - \pi(l, x)}{\epsilon_x} \quad (4)$$

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

Reduction from Noisy Leakage to RP (III)

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

So (3) gives

$$\Pr[\mathcal{S}(\perp) = l] \leq \frac{\Pr[\mathrm{L}(x) = l]}{1 - \epsilon_x} \text{ for any } x \text{ s.t. } \epsilon_x < 1$$

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

So (3) gives

$$\Pr[\mathcal{S}(\perp) = l] \leq \frac{\Pr[\mathrm{L}(x) = l]}{1 - \epsilon_x} \text{ for any } x \text{ s.t. } \epsilon_x < 1$$

In other words,

$$0 \leq \Pr[\mathcal{S}(\perp) = l] \leq \min_{x' : \epsilon_{x'} < 1} \left\{ \frac{\Pr[\mathrm{L}(x') = l]}{1 - \epsilon_{x'}} \right\}$$

Reduction from Noisy Leakage to RP (III)

Is there any ϵ such that $\geq$ and $\geq$ are valid? From (3), and (4), we get

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

So (3) gives

$$\Pr[\mathcal{S}(\perp) = l] \leq \frac{\Pr[\mathrm{L}(x) = l]}{1 - \epsilon_x} \text{ for any } x \text{ s.t. } \epsilon_x < 1$$

In other words,

$$0 \leq \Pr[\mathcal{S}(\perp) = l] \leq \min_{x' : \epsilon_{x'} < 1} \left\{ \frac{\Pr[\mathrm{L}(x') = l]}{1 - \epsilon_{x'}} \right\}$$

And (3) also gives

$$0 \leq \pi(l, x) \leq (1 - \epsilon_x) \cdot \min_{x' : \epsilon_{x'} < 1} \left\{ \frac{\Pr[\mathrm{L}(x') = l]}{1 - \epsilon_{x'}} \right\}$$

Characterization of ARP-simulable Leakages

Furthermore, summing (3) over l, by definition of probability distributions,

$$\sum_l \pi(l, x) = \underbrace{\sum_l \Pr[\mathrm{L}(x) = l]}_{=1} - \epsilon_x \cdot \underbrace{\sum_l \Pr[\mathcal{S}(x) = l]}_{=1}$$

[17] One needs at least one $\epsilon_x < 1$ for non-trivial simulation

Characterization of ARP-simulable Leakages

Furthermore, summing (3) over l, by definition of probability distributions,

$$\sum_l \pi(l, x) = \underbrace{\sum_l \Pr[\mathrm{L}(x) = l]}_{=1} - \epsilon_x \cdot \underbrace{\sum_l \Pr[\mathcal{S}(x) = l]}_{=1} = 1 - \epsilon_x$$

[17] One needs at least one $\epsilon_x < 1$ for non-trivial simulation

Characterization of ARP-simulable Leakages

Furthermore, summing (3) over l, by definition of probability distributions,

$$\sum_l \pi(l,x) = \underbrace{\sum_l \Pr[\mathrm{L}(x)=l]}_{=1} - \epsilon_x \cdot \underbrace{\sum_l \Pr[\mathcal{S}(x)=l]}_{=1} = 1-\epsilon_x$$

Hence, the following result

Theorem (ARP-Simulability)

L *is simulable in the* $\{\epsilon_x\}_x$ *average random probing model iff*[17]

$$1 \leq \sum_l \min_{x':\epsilon_{x'}<1} \left\{ \frac{\Pr[\mathrm{L}(x')=l]}{1-\epsilon_{x'}} \right\}$$

[17] One needs at least one $\epsilon_x < 1$ for non-trivial simulation