Leakage Squeezing of Order Two

Claude CARLET[1], Jean-Luc DANGER[2,3],
Sylvain GUILLEY[2,3] and Houssem MAGHREBI[2].

[1] LAGA, UMR 7539, CNRS, Department of Mathematics,
University of Paris XIII and University of Paris VIII,
2 rue de la liberté, 93 526 Saint-Denis Cedex, France.

[2] TELECOM-ParisTech, Crypto Group,
37/39 rue Dareau, 75 634 Paris Cedex 13, France.

[3] Secure-IC S.A.S., 80 avenue des Buttes de Coësmes,
35 700 Rennes, France.

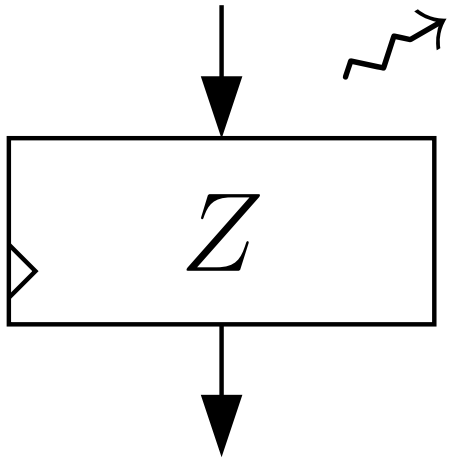
Outline

No protection... secrets are gone

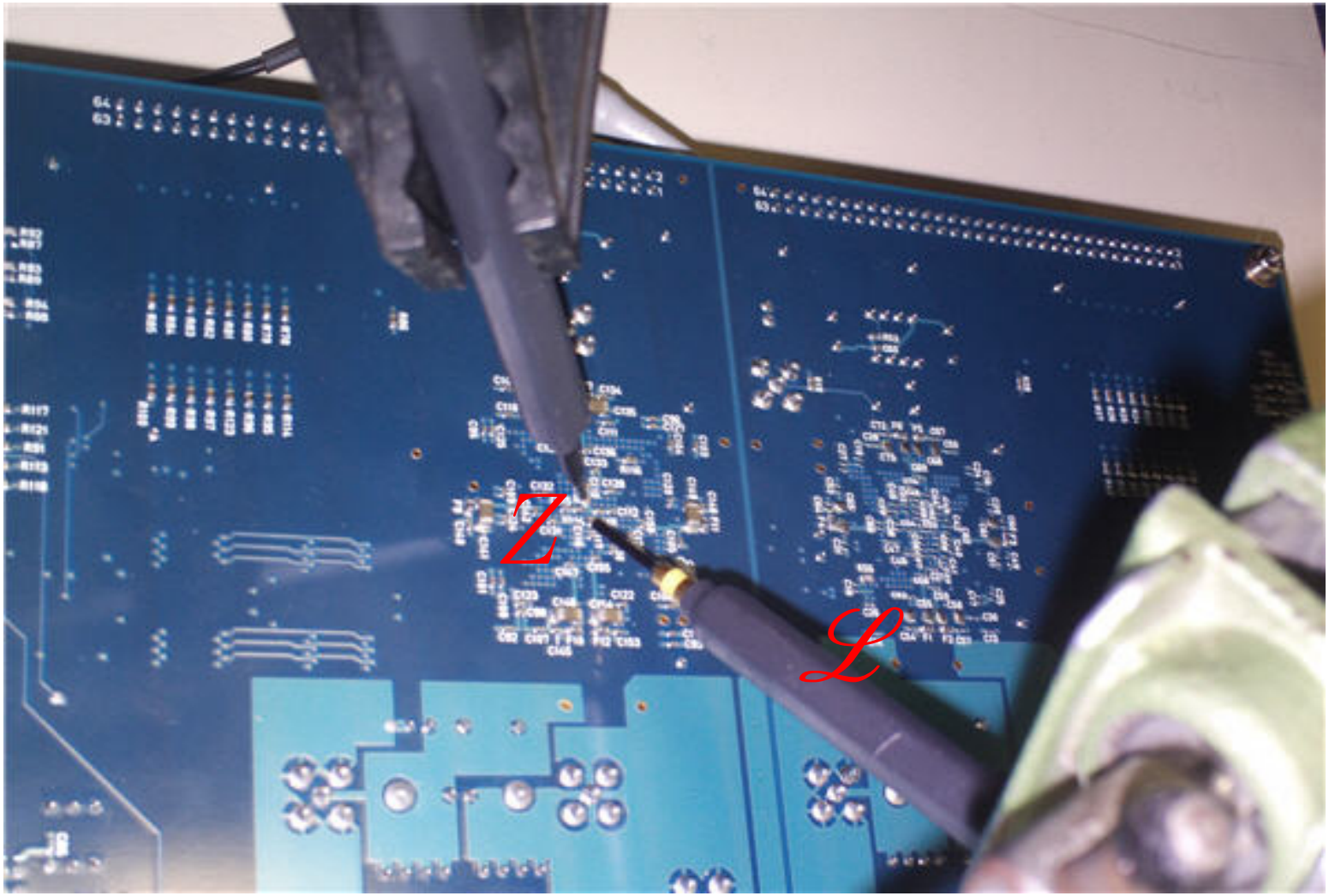
Fact:

manipulating a variable leaks.

$Z \rightsquigarrow$



Side-Channel Analysis: Spying Internals



Protection... extracting secrets is harder

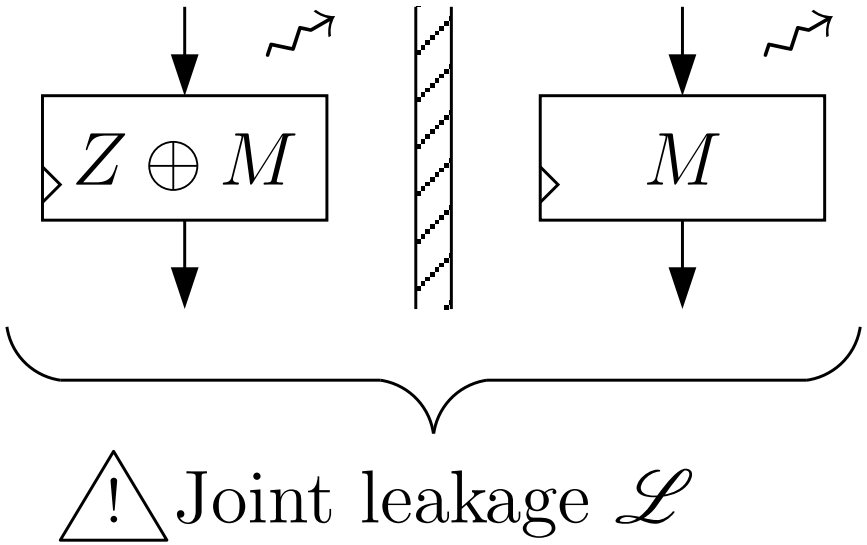
Masking:

splitting Z (in 2, ... or more, e.g. $d+1$)

$Z \oplus M \rightsquigarrow \quad \| \quad M \rightsquigarrow$

Attacks: joint $(Z \oplus M, M)$ leaks on Z.

Modulo: leakage function, noise.



Definition of dth-Order Masking

Sensitive Variables

A sensitive variable Z is hidden in $d+1$ shares S_i, such as:

- Z is a deterministic function of all the S_i, but
- $Z \perp\!\!\!\perp (S_i)_{i \in I}$ if $|I| \leqslant d$.

Examples

Additive Boolean Masking:

- The sharing is done in the group $(\mathbb{F}_2^n, \oplus)$
- $Z = \bigoplus_{i=0}^{d} S_i$.

Additive Arithmetic Masking:

- The sharing is done in the group $(\mathbb{Z}_{2^n}, \boxplus)$
- $Z = \boxplus_{i=0}^{d} S_i = \sum_{i=0}^{d} S_i \mod 2^n$.

Leakage Function

General Setup to Capture the Leakage Function

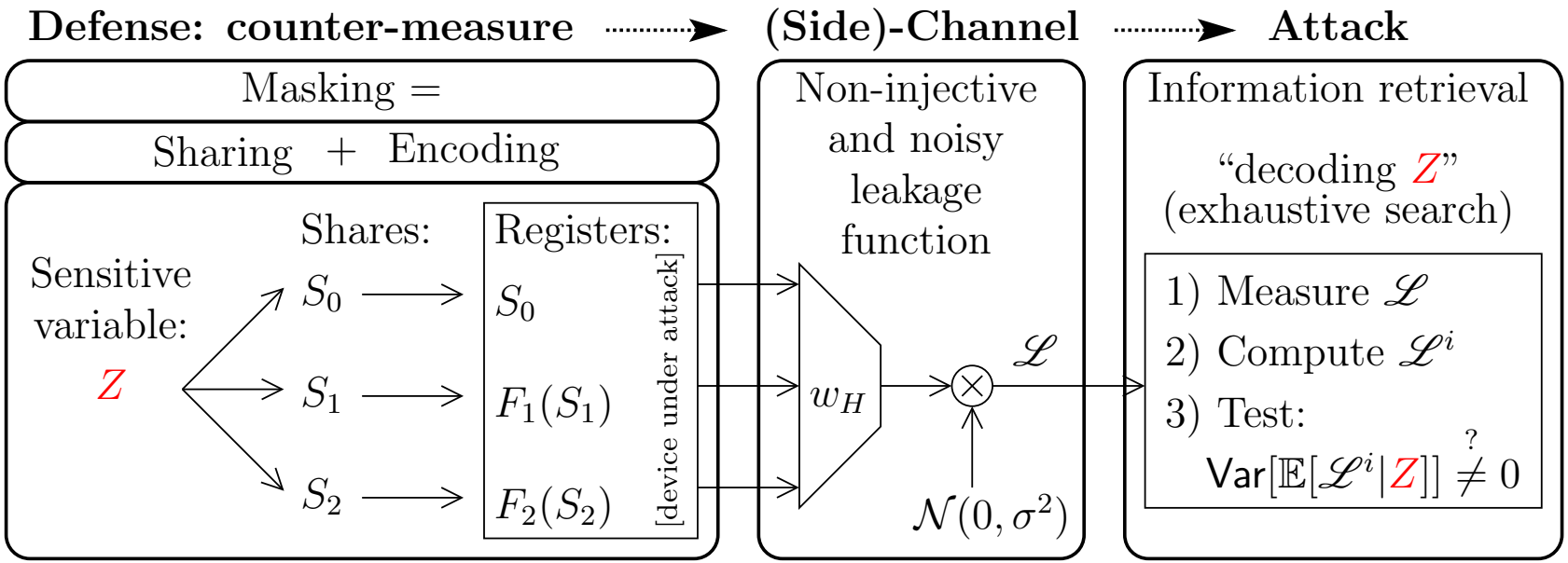
- In the optimal case for the attacker, each share leaks S_i independently through L_i
- $L_i(S_i) =$ [attacker's function] $\circ$ [device's function] $\circ$ [defender's function] (S_i)

Examples

- Defender's function: bijection F for the leakage squeezing, Id otherwise
- Device's function: Hamming Weight (HW) if no additional effort is done on the hardware
- Attacker's function: assuming the "power" $x \mapsto x^{p_i}$

Side-Channel Attacks Prevention

"A setup similar to coding in digital communications, where the goal is to make it hard for the receiver to decode the signal".



Exploitation

Measured Combination (*first result*)

- The attacker computes the **optimal combination**, *i.e.* the product $\prod_{i=0}^{d} L_i(S_i)$
- However, the attacker does not know the shares ...
- so, she simply checks whether there is a dependence, in average, with $Z = z$:

$$\mathbb{E}\left[\prod_{i=0}^{d} L_i(S_i) \mid Z = z\right] = 2^{-nd} \bigotimes_{i=0}^{d} L_i(z)$$

General Theorem for Additive Masking

- Boolean: the attack fails $\iff$ $\bigotimes_{i=0}^{d} L_i(z)$ is constant;
- Arithmetic: the attack fails $\iff$ $\boxtimes_{i=0}^{d} L_i(z)$ is constant.

Optimal combination?

- The reason is that L_i are actually measured noisy;
- $$\mathbb{E}\left[\overbrace{\sum_{(\alpha_i)\in\mathbb{N}^{d+1}} \beta_{\alpha_i} \prod_{i=0}^{d} L_i(S_i)^{\alpha_i}}^{\text{General polynomial in } \mathbb{R}[L_0(S_0),\cdots,L_d(S_d)]} \mid Z = z\right] =$$

  $$\sum_{(\alpha_i)\in\mathbb{N}^{d+1}} \beta_{\alpha_i} \mathbb{E}\left[\prod_{i=0}^{d} L_i(S_i)^{\alpha_i} \mid Z = z\right] =$$

  $$\sum_{(\alpha_i)\in(\mathbb{N}^\star)^{d+1}} \beta_{\alpha_i} \mathbb{E}\left[\prod_{i=0}^{d} L_i(S_i)^{\alpha_i} \mid Z = z\right] \quad (i.e.\ \forall i, \alpha_i > 0).$$

- The smallest noise happens when $\forall i, \alpha_i = 1$. □

Order of the **Optimal** Attack (*i.e.* estimation with fewest noise)

- $\sum_i p_i \geqslant d + 1$.

Attack Feasibility Condition

Distinguishing Property

$$\mathbb{E}\left[\prod_{i=0}^{d} L_i(S_i) \mid Z = z\right] = 2^{-nd} \bigotimes_{i=0}^{d} L_i(z) \quad \dots$$

- Actually, the attacker guesses mainly Z, depending on a exhaustive search on keys
- For the correct key, there is a dependance, but not otherwise, since we assume $Z(k^\star) \perp\!\!\!\perp Z(k \neq k^\star)$ (approximately)

Success Criteria

Characterization in Terms of Boolean Functions Fourier Transform

$$\text{The attack fails}$$

$$\iff \bigotimes_{i=0}^{d} L_i(z) \text{ does not depend on } z \quad (1)$$

$$\iff \prod_{i=0}^{d} \widehat{L}_i(a) = 0, \forall a \neq 0 \quad (2)$$

- Recall that L_i typically writes $L_i = G_i \circ \mathrm{HW} \circ F_i$;
- W.l.o.g., when F_i are linear, we can take $F_0 = \mathrm{Id}$ in Eqn. (1), simply by using $F'_i = F_i \circ F_0^{-1}$ instead
- **Goal: find F_i such as $\sum_i \mathbf{d}^\circ(G_i) = \sum_i p_i$ is maximal**

Classical Result

No Leakage Squeezing $(X \oplus X' = Z)$

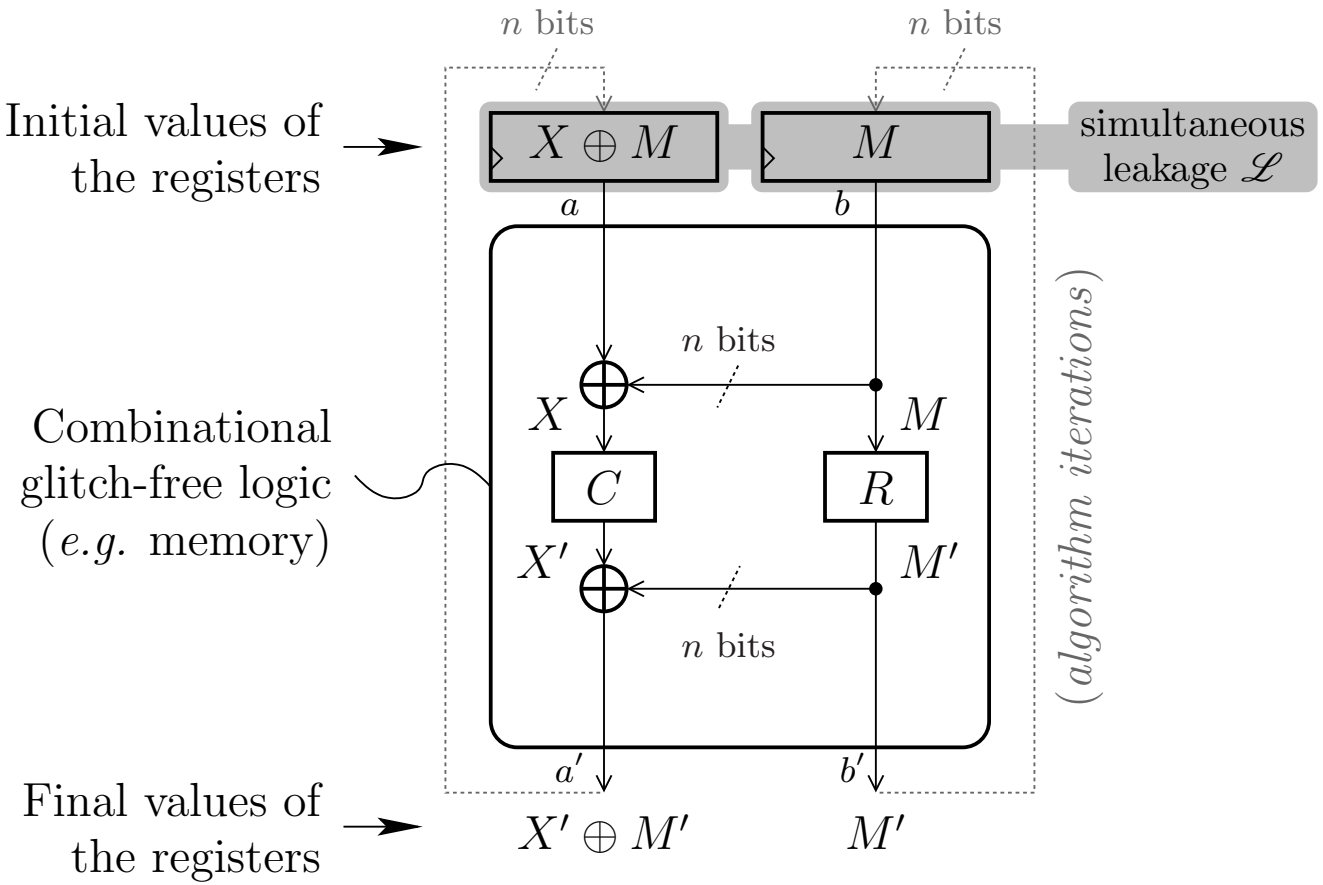
- $L_i = \mathrm{HW}^{p_i}$
- Theorem: $\widehat{\mathrm{HW}^p}(a) = 0 \iff \mathrm{HW}(a) > p$

Results

- If $\exists i$ such as $p_i = 0$, the attack fails (we need all the shares)
- If $\forall i, p_i > 0$, the attack works.
- Minimal degree of a successful attack:

$$\sum_{i=0}^{d} p_i = \sum_{i=0}^{d} 1 = d + 1$$

No Leakage Squeezing



Enhanced Results with Leakage Squeezing

Goal

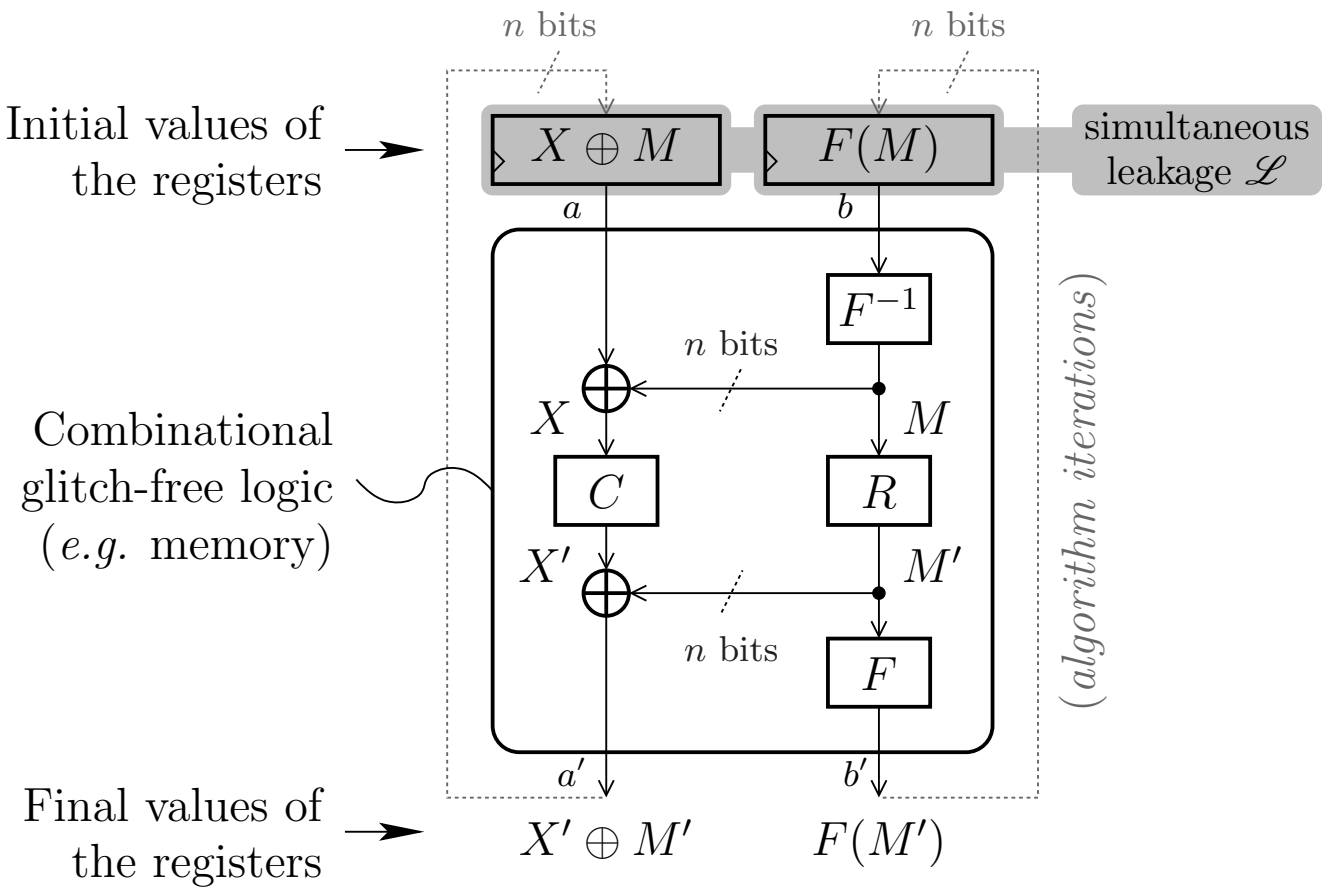
- We want a family of $L_i : \mathbb{F}_2^n \to \mathbb{Z}$ such that $\forall a \neq 0, \prod_{i=0}^{d} \widehat{L_i}(a) = 0$
- If all the L_i are identical (equal to L), this is equivalent to $\widehat{L}\Big|_{\mathbb{F}_2^{n\star}} = 0$.

Strategy (*second result*)

- Dispatch the constraint on the many L_i.
- We use this property, for $a \neq 0$:

$$\forall q' \leqslant q, \quad \widehat{\mathrm{HW}^{q'} \circ F}(a) = 0$$
$$\iff \quad \forall b, \mathrm{HW}(b) \leqslant q, \quad \widehat{b \cdot F}(a) = 0$$

First-Order Leakage Squeezing



Example with $d = 1$ and F Linear

Condition on share 0 ($F_0 = \mathrm{Id}$)

- $\forall a \neq 0,\ \widehat{L_0}(a) = 0 \iff \mathrm{HW}(a) > 1$

Condition on share 1 ($F_1 = F$, $F(a) = \neg\mathrm{Id} \times a$)

- $\forall a \neq 0,\ \widehat{L_1}(a) = 0 \iff \forall b, \mathrm{HW}(b) \leqslant 1, \widehat{b \cdot F}(a) = 0$
- Now, $\widehat{b \cdot F}(a) \neq 0 \iff b = M \times a$,
  where M is the inverse of the transpose of $\neg\mathrm{Id}$, *i.e.* $\neg\mathrm{Id}$

Altogther

- Because of the condition on $\widehat{L_0}$, we only need $\widehat{L_1}(a) = 0$ for a such that $\mathrm{HW}(a) = 1$
- But thus we must check that $\forall b, \mathrm{HW}(b) \leqslant 1,\ b \neq M \times a$
- This is correct, as $M \times a$ has Hamming weight $n - 1 \neq 1$

Theorem of AfricaCrypt'2012 [MCGD12]

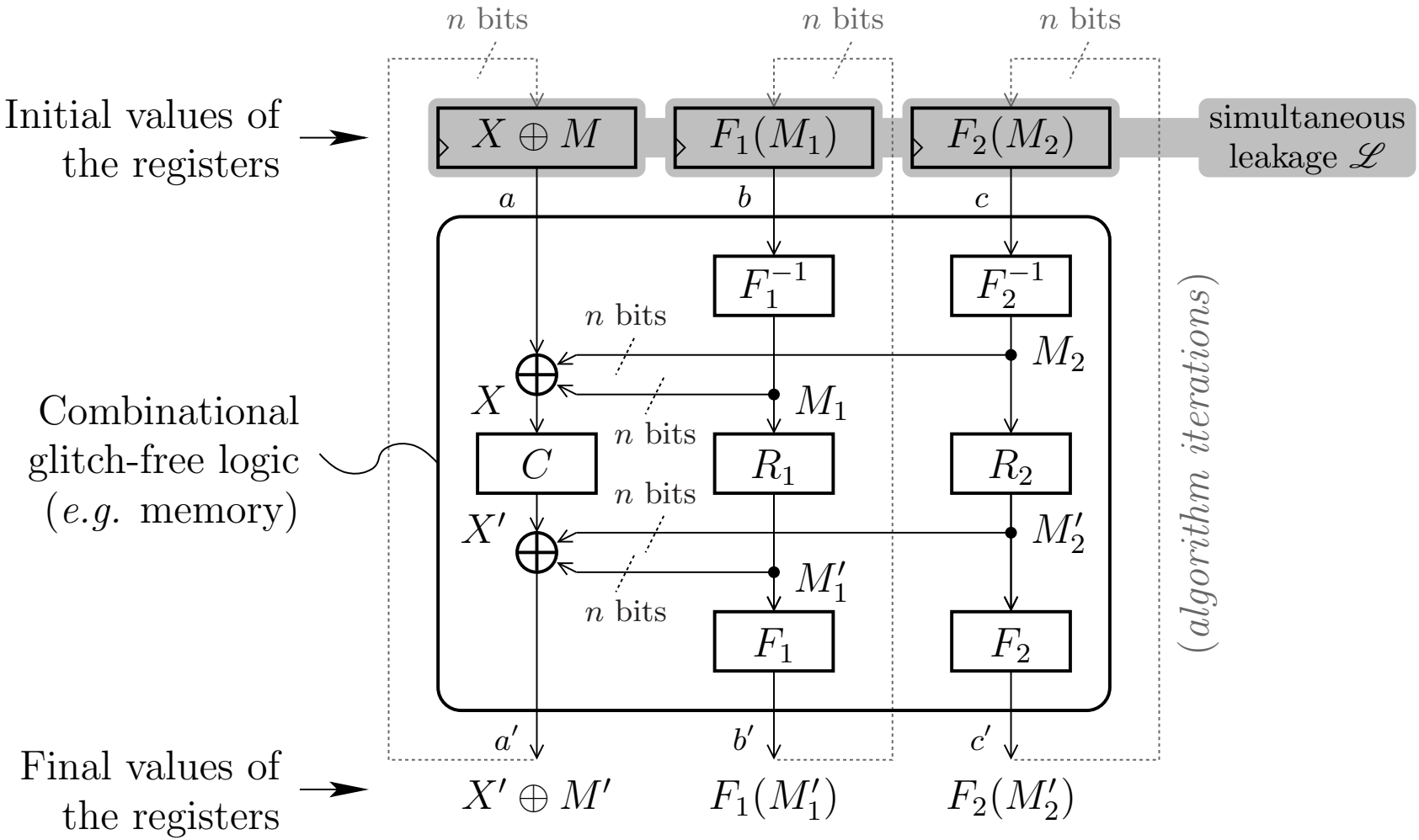
Theorem

- With one mask, the minimal order of the best attack is not 2, but
- it is equal to the dual distance of the graph of F, or
- to the correlation-immunity of the indicator of F plus the number one.

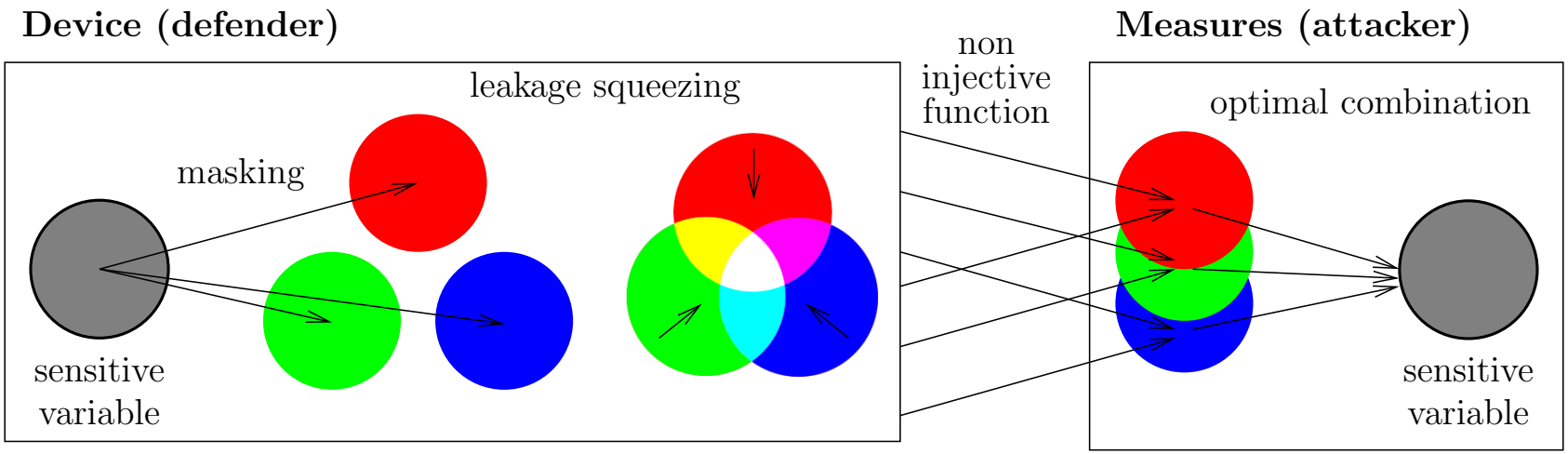
For F linear

- It is equal to the maximal minimal distance of the graph of F.
- E.g.: $\boxed{4 \text{ for } n = 4}$ or $\boxed{5 \text{ for } n = 8}$.

Second-Order Leakage Squeezing



Second-Order Leakage Squeezing



Hence the leakage: $\mathscr{L} =$

$$\begin{aligned} & \mathrm{HW}(Z \oplus M_1'' \oplus M_2'', F_1(M_1) \oplus F_1(M_1 \oplus M_1''), F_2(M_2) \oplus F_2(M_2 \oplus M_2'')) \\ = \; & \mathrm{HW}(Z \oplus M_1'' \oplus M_2'', D_{M_1''}F_1(M_1), D_{M_2''}F_2(M_2)) \quad . \end{aligned}$$

So attacks fail at order d if for all p, q and r such as $p + q + r \leqslant d$, the function

$$
\begin{aligned}
& z \mapsto f(z) \\
\doteq & \sum_{m_1'', m_2''} \sum_{m_1, m_2} \mathrm{HW}^p(z \oplus m_1'' \oplus m_2'') \cdot \mathrm{HW}^q(D_{m_1''} F_1(m_1)) \cdot \mathrm{HW}^r(D_{m_2''} F_2(m_2)) \\
= & \sum_{m_1'', m_2''} \mathrm{HW}^p\left(z \oplus m_1'' \oplus m_2''\right) \cdot \sum_{m_1} \mathrm{HW}^q\left(D_{m_1''} F_1(m_1)\right) \cdot \sum_{m_2} \mathrm{HW}^r\left(D_{m_2''} F_2(m_2)\right) \\
= & \sum_{m_1'', m_2''} \mathrm{HW}^p\left(z \oplus m_1'' \oplus m_2''\right) \cdot \mathbb{E}(\mathrm{HW}^q\left(D_{m_1''} F_1(M_1)\right)) \cdot \mathbb{E}(\mathrm{HW}^r\left(D_{m_2''} F_2(M_2)\right)) \\
= & \left\{\mathrm{HW}^p \otimes \mathbb{E}(\mathrm{HW}^q \circ D_{(\cdot)} F_1(M_1)) \otimes \mathbb{E}(\mathrm{HW}^r \circ D_{(\cdot)} F_2(M_2))\right\}(z) \qquad (3)
\end{aligned}
$$

is constant.

Thus $\hat{f}$ is null everywhere except in zero:

$$
\hat{f} = \widehat{\mathrm{HW}^p} \cdot \mathbb{E}(\mathrm{HW}^q \circ \widehat{D_{(\cdot)}} F_1(M_1)) \cdot \mathbb{E}(\mathrm{HW}^r \circ \widehat{D_{(\cdot)}} F_2(M_2)) \ .
$$

In summary, to resist at order d, we are attempting to find two bijections F_1 and F_2 such as:

$$\forall a \in \mathbb{F}_2^{n*}, \quad \widehat{\mathrm{HW}^p}(a) = 0 \quad \text{or} \quad \mathbb{E}(\mathrm{HW}^q \circ \widehat{D_{(\cdot)}F_1(M)})(a) = 0$$
$$\text{or} \quad \mathbb{E}(\mathrm{HW}^r \circ \widehat{D_{(\cdot)}F_2(M)})(a) = 0 \quad (4)$$

for every triple of integers p, q and r such as $p + q + r \leqslant d$, d being the targeted protection order.

Proposition

Let F_1 be a bijection such that the security is reached at order d with one mask. Then, by introducing a second mask processed through whatever bijection F_2, the security is reached at order at least $d + 1$.

F_1 and F_2 are assumed to be linear

Thus $d = \min\{\mathrm{HW}(a) + \mathrm{HW}(L_1(a)) + \mathrm{HW}(L_2(a)) - 1; a \neq 0\}$, which is exactly the minimal distance of the code $\{(x, L_1^t(x), L_2^t(x)); x \in \mathbb{F}_2^n\}$ (of rate 1/3 and with three disjoint information sets) minus the number 1.

New records in high-order attacks resistance

Old values:

- $n = 4$ bit: $[8, 4, \mathbf{4}]$ (linear)
- $n = 8$ bit: $[16, 8, \mathbf{5}]$ (linear) / $(16, 256, \mathbf{6})$ (non-linear)

New values:

- $n = 4$ bit: $[12, 4, \mathbf{6}]$ (linear)
- $n = 8$ bit: $[24, 8, \mathbf{8}]$ (linear)

A high-order leakage squeezing countermeasure allows:

... to increase the security

- $n = 4$ bit: from first successful HO-CPA of order 2 to order 6
- $n = 8$ bit: from first successful HO-CPA of order 2 to order 8

Acknowledgments

Acknowledgments

Special thanks to Secure-IC S.A.S. for financing this mission:

Visit http://www.secure-ic.com; the company is hiring.

Leakage Squeezing of Order Two

Claude CARLET[1], Jean-Luc DANGER[2,3],
Sylvain GUILLEY[2,3] and Houssem MAGHREBI[2].

[1] LAGA, UMR 7539, CNRS, Department of Mathematics,
University of Paris XIII and University of Paris VIII,
2 rue de la liberté, 93 526 Saint-Denis Cedex, France.

[2] TELECOM-ParisTech, Crypto Group,
37/39 rue Dareau, 75 634 Paris Cedex 13, France.

[3] Secure-IC S.A.S., 80 avenue des Buttes de Coësmes,
35 700 Rennes, France.

Houssem Maghrebi, Claude Carlet, Sylvain Guilley, and Jean-Luc Danger.

Optimal First-Order Masking with Linear and Non-linear Bijections.

In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT*, volume 7374 of *Lecture Notes in Computer Science*, pages 360–377. Springer, 2012.