

Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks

Maxime Nassar, Sylvain Guilley and Jean-Luc Danger

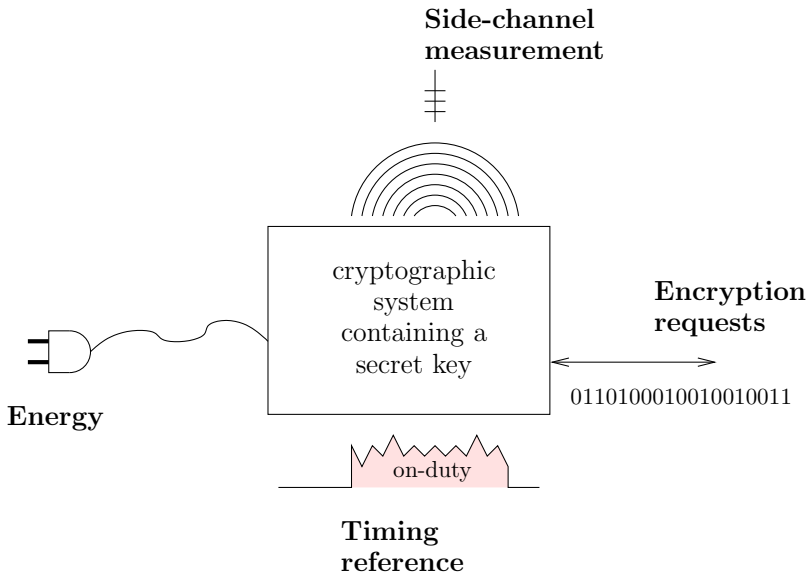
Bull TrustWay, Rue Jean Jaurès, B.P. 68,
78 340 Les Clayes-sous-Bois, France.

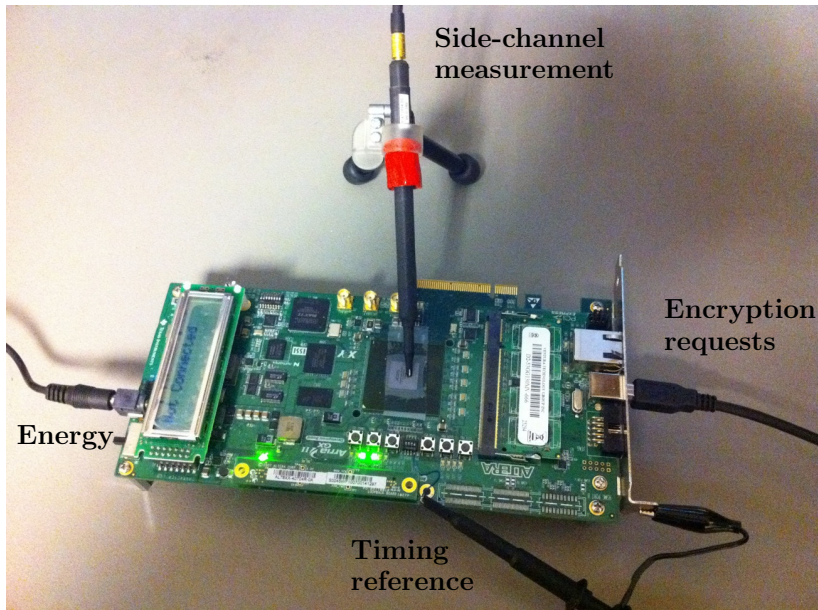
Institut TELECOM / TELECOM ParisTech,
46 rue Barrault, 75 634 Paris Cedex, France.

Secure-IC S.A.S.,
80 avenue des Buttes de Coësmes,
35700 Rennes, France.

- 1 Introduction
 - Side-Channel Analysis (SCA)
 - Countermeasures
 - Goal of the Presentation
- 2 RSM: Rotating Sboxes Masking
 - Rationale of the Countermeasure
 - RSM Modelization
- 3 Information Theoretic Evaluation of RSM
- 4 Security Evaluation of RSM against CPA and 2O-CPA
 - Optimal HO-CPA
 - Expression of $\rho_{\text{opt}}^{(1,2)}$
- 5 Conclusions and Perspectives

- 1 Introduction
 - Side-Channel Analysis (SCA)
 - Countermeasures
 - Goal of the Presentation
- 2 RSM: Rotating Sboxes Masking
 - Rationale of the Countermeasure
 - RSM Modelization
- 3 Information Theoretic Evaluation of RSM
- 4 Security Evaluation of RSM against CPA and 2O-CPA
 - Optimal HO-CPA
 - Expression of $\rho_{\text{opt}}^{(1,2)}$
- 5 Conclusions and Perspectives



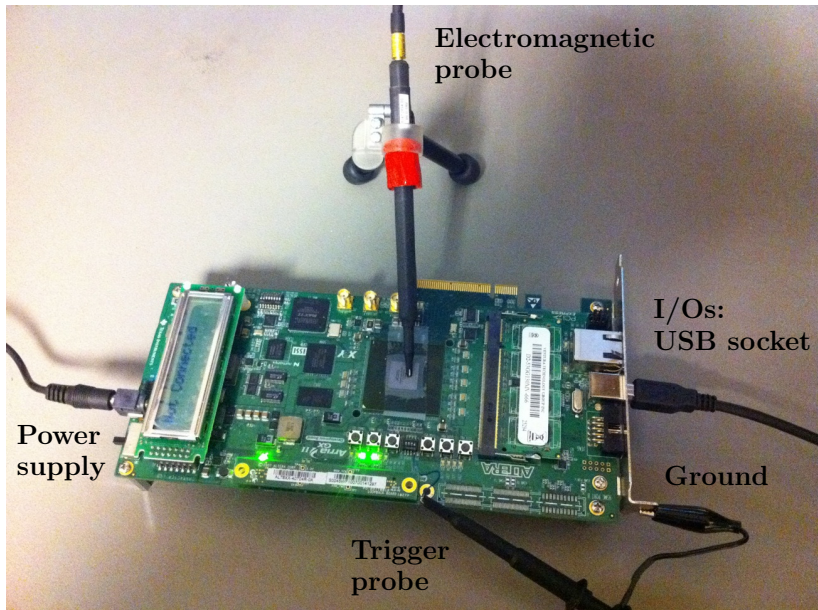


Side-channel
measurement

Encryption
requests

Energy

Timing
reference



Electromagnetic probe

I/Os:
USB socket

Power supply

Ground

Trigger probe

Protection against side-channel attacks

Extrinsic countermeasures

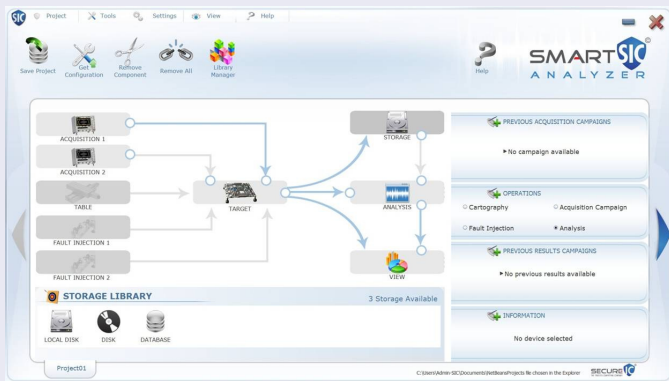
- Noise addition .. makes the attack difficult but not impossible
- Internal powering can be tampered with

Internal countermeasures

- Make the power constant .. require design skills [DGBN09] ✘
- Masking the power susceptible to HO-SCA ✔

Security Evaluation of Countermeasures

Off-the-shelf platforms, e.g. the Smart-SIC Analyzer



Context

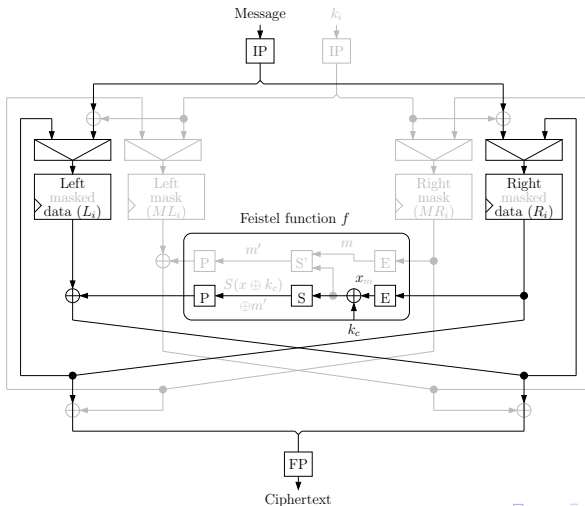
- + Security 😊 \implies + Costs 😞
- Trade-offs?
 - Maximal security within a given budget
 - Minimal spendings for a target security level (CC EALx?)
- Formal analysis: sound and realistic metrics for both security and cost.

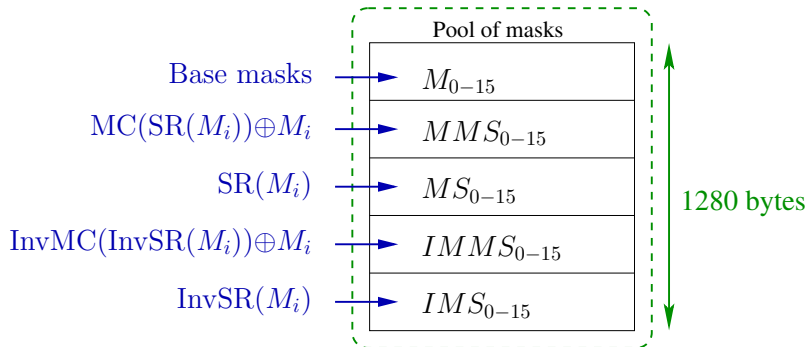
Context

- — Costs ☹ \implies — Security ☺
- Trade-offs?
 - Maximal security within a given budget
 - Minimal spendings for a target security level (CC EALx?)
- Formal analysis: sound and realistic metrics for both security and cost.

- 1 Introduction
 - Side-Channel Analysis (SCA)
 - Countermeasures
 - Goal of the Presentation
- 2 RSM: Rotating Sboxes Masking
 - Rationale of the Countermeasure
 - RSM Modelization
- 3 Information Theoretic Evaluation of RSM
- 4 Security Evaluation of RSM against CPA and 2O-CPA
 - Optimal HO-CPA
 - Expression of $\rho_{\text{opt}}^{(1,2)}$
- 5 Conclusions and Perspectives

Masking with two (or more) paths



Masking with one path: $Z \rightarrow Z \oplus M$ (ex. AES)

- Homomorphic computation.
- This masking is the less costly in the litterature [NGDS12].
- Requires leak-free ROMs (well suited for ASIC & FPGA).

Performances

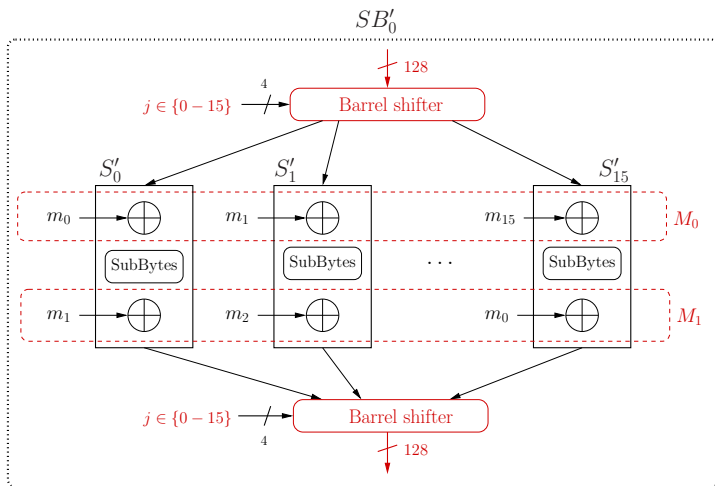
Table: Implementation results for reference and protected AES

	Unprotected	RSM	Overhead
Number of ALUTs (%)	2136 (8%)	2734 (10%)	28%
Number of M4K ROM Blocs (%)	20 (14%)	24 (17%)	20%
Frequency (MHz)	133	88	34%

Setting:

- $n = 8$ bit,
- 16 masks only, and (Price metric)
- provable security up to 2nd-order attacks (Security metric)

RSM mode of operation



RSM leakage

- Masked sboxes $Z \mapsto M_{\text{out}} \oplus S(Z \oplus M_{\text{in}})$.



$$\mathcal{L}(Z, M) = \mathcal{L}(Z \oplus M) .$$

In this expression, Z and M are n -bit vectors, *i.e.* live in \mathbb{F}_2^n .
The leakage function $\mathcal{L} : \mathbb{F}_2^n \rightarrow \mathbb{R}$ depends on the hardware.

- In a conservative perspective, \mathcal{L} is assumed to be bijective.
- In a realistic perspective, \mathcal{L} is assumed to non-injective.

Metrics

- ① **Cost:** $\text{Card}[\mathcal{M}] \in \{1, \dots, 2^n\}$.
- ② **Security:**
 - Leakage: mutual information.
 - Attack: resistance against HO-CPA.

Modelization that bridges both notions:

$$P[M = m] = \begin{cases} 1/\text{Card}[\mathcal{M}] & \text{if } m \in \mathcal{M}, \text{ and} \\ 0 & \text{otherwise.} \end{cases}$$

- 1 Introduction
 - Side-Channel Analysis (SCA)
 - Countermeasures
 - Goal of the Presentation
- 2 RSM: Rotating Sboxes Masking
 - Rationale of the Countermeasure
 - RSM Modelization
- 3 Information Theoretic Evaluation of RSM
- 4 Security Evaluation of RSM against CPA and 2O-CPA
 - Optimal HO-CPA
 - Expression of $\rho_{\text{opt}}^{(1,2)}$
- 5 Conclusions and Perspectives

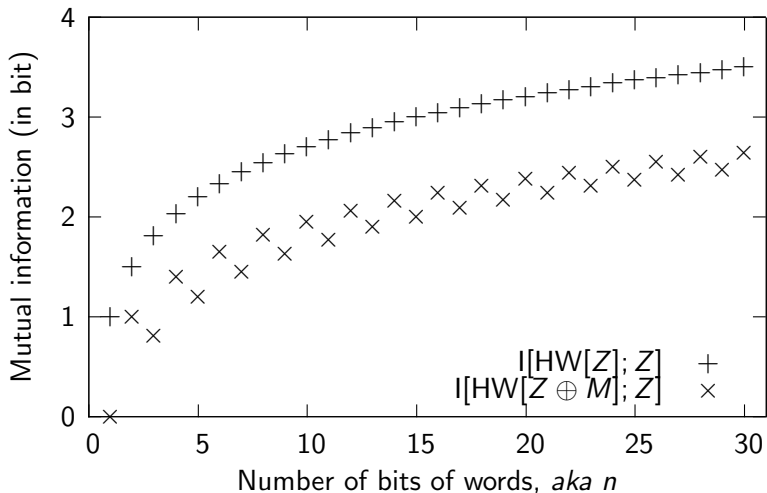
General Considerations

- $\forall \mathcal{L}, I[\mathcal{L}(Z \oplus M); Z] = 0$ if $H[M] = n$ bit (or equivalently, if $M \sim \mathcal{U}(\mathbb{F}_2^n)$). So with all the masks, the countermeasure is perfect.
- If \mathcal{L} is bijective (e.g. $\mathcal{L} = \text{Id}$), then $I[\mathcal{L}(Z \oplus M); Z] = n - H[M]$, irrespective of \mathcal{M} .
- If \mathcal{L} is non-injective (e.g. $\mathcal{L} = \text{HW}$), then $I[\mathcal{L}(Z \oplus M); Z] < n - H[M]$, but depends on \mathcal{M} .

Motivating examples: for $\mathcal{L} = \text{HW}$ on $n = 8$ bits,

- $I[\mathcal{L}(Z \oplus M); Z] = 1.42701$ bit if $\mathcal{M} = \{0x00, 0x0f, 0xf0, 0xff\}$, but
- $I[\mathcal{L}(Z \oplus M); Z] = 0.73733$ bit if $\mathcal{M} = \{0x00, 0x01, 0xfe, 0xff\}$.

Example for $\mathcal{M} = \{m, \neg m\}$



- 1 Introduction
 - Side-Channel Analysis (SCA)
 - Countermeasures
 - Goal of the Presentation
- 2 RSM: Rotating Sboxes Masking
 - Rationale of the Countermeasure
 - RSM Modelization
- 3 Information Theoretic Evaluation of RSM
- 4 Security Evaluation of RSM against CPA and 2O-CPA
 - Optimal HO-CPA
 - Expression of $\rho_{\text{opt}}^{(1,2)}$
- 5 Conclusions and Perspectives

Optimal CPA

In [PRB09], it is explained that best possible d O-CPA has $\rho_{\text{opt}}^{(d)}$:

$$\frac{\text{Var} \left(f_{\text{opt}}^{(d)}(Z) \right)}{\text{Var} \left((\mathcal{L}(Z, M) - \mathbb{E}\mathcal{L}(Z, M))^d \right)} = \frac{\text{Var} \left(\mathbb{E} \left((\text{HW}[Z \oplus M] - \frac{n}{2})^d \mid Z \right) \right)}{\text{Var} \left((\text{HW}[Z \oplus M] - \frac{n}{2})^d \right)}$$

where

$$\begin{aligned} f_{\text{opt}}^{(d)}(z) &\doteq \mathbb{E} \left((\mathcal{L}(Z, M) - \mathbb{E}\mathcal{L}(Z, M))^d \mid Z = z \right) \\ &= \frac{1}{\text{Card}[\mathcal{M}]} \sum_{m \in \mathcal{M}} \left(\frac{-1}{2} \sum_{i=1}^n (-1)^{(z \oplus m)_i} \right)^d, \end{aligned}$$

noting that

$$\mathbb{E} \text{HW}[Z \oplus M] = \frac{1}{\text{Card}[\mathcal{M}]} \sum_{m \in \mathcal{M}} \frac{1}{2^n} \sum_{z \in \mathbb{F}_2^n} \text{HW}[z \oplus m] = \frac{n}{2}.$$

Example for the intuition

 $(n = 4)$

	$\text{Card}[\mathcal{M}] = 2^4$	$\text{Card}[\mathcal{M}] = 2^3$	$\text{Card}[\mathcal{M}] = 2^2$	$\text{Card}[\mathcal{M}] = 2^1$
\mathcal{M}	0000	0000	0000	0000
	0001			
	0010			
	0011	0011	0011	
	0100	0100		
	0101			
	0110			
	0111	0111		
	-----	-----	-----	-----
	1000	1000		
	1001			
	1010			
	1011	1011		
	1100	1100	1100	
	1101			
	1110			
1111	1111	1111	1111	

Example evaluation

Card[\mathcal{M}]	H[M]	$\rho_{\text{opt}}^{(1)}$	$\rho_{\text{opt}}^{(2)}$	I[HW[Z \oplus M]; Z]	I[Z \oplus M; Z]
2^4	4	0	0	0	0
2^3	3	0	0.166667	0.15564	1
2^2	2	0	0.333333	1.15564	2
2^1	1	0	1	1.40564	3
2^0	0	1	1	2.03064	4

- It seems that the most entropy, the least leakage in $\mathcal{L} = \text{HW}$ and in $\mathcal{L} = \text{Id}$.
- But this will be challenged by exhaustive searches...

Resistance against 1O-CPA and 2O-CPA

$$\rho_{\text{opt}}^{(1)} = \frac{1}{n} \sum_{i=1}^n \left(\frac{1}{\text{Card}[\mathcal{M}]} \sum_{m \in \mathcal{M}} (-1)^{m_i} \right)^2,$$

$$\rho_{\text{opt}}^{(2)} = \frac{1}{n(n-1)} \left(\frac{1}{\text{Card}[\mathcal{M}]^2} \sum_{(m, m') \in \mathcal{M}^2} \left(\sum_{i=1}^n (-1)^{(m \oplus m')_i} \right)^2 - n \right).$$

Expression in Boolean theory — With Indicator f of \mathcal{M}

- Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, defined as:

$$\forall m \in \mathbb{F}_2^n, f(m) = 1 \iff m \in \mathcal{M}.$$
- The Fourier transform $\hat{f} : \mathbb{F}_2^n \rightarrow \mathbb{Z}$ of the Boolean function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is defined as

$$\forall a \in \mathbb{F}_2^n, \hat{f}(a) \doteq \sum_{m \in \mathbb{F}_2^n} f(m) (-1)^{a \cdot m}.$$
- It allows for instance to write

$$\text{Card}[\mathcal{M}] = \sum_{m \in \mathcal{M}} 1 = \sum_{m \in \mathbb{F}_2^n} f(m) = \hat{f}(0).$$
 Recall

$$\text{Card}[\mathcal{M}] \in \llbracket 1, 2^n \rrbracket, \text{ hence } \hat{f}(0) > 0.$$

Expression of $\rho_{\text{opt}}^{(1,2)}$ in Boolean theory

$$\rho_{\text{opt}}^{(1)} = \frac{1}{n} \sum_{i=1}^n \left(\frac{\hat{f}(e_i)}{\hat{f}(0)} \right)^2, \quad (1)$$

$$\rho_{\text{opt}}^{(2)} = \frac{1}{n(n-1)} \sum_{\substack{(i,i') \in \llbracket 1, n \rrbracket^2 \\ i \neq i'}} \left(\frac{\hat{f}(e_i \oplus e_{i'})}{\hat{f}(0)} \right)^2. \quad (2)$$

The e_i are the canonical basis vectors $(0, \dots, 0, 1, 0, \dots, 0)$.

Thus, RSM resists:

- 1 first-order attacks iff $\forall a, \text{HW}[a] = 1 \implies \hat{f}(a) = 0$;
- 2 first- and second-order attacks iff $\forall a, 1 \leq \text{HW}[a] \leq 2 \implies \hat{f}(a) = 0$.

Example: $n = 4$

All the functions $f : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2$ that cancel $\rho_{\text{opt}}^{(1,2)}$.

f	HW[f]	H[M]	$\rho_{\text{opt}}^{(1,2)}$	I[HW[$Z \oplus M$]; Z]	I[$Z \oplus M$; Z]	$d_{\text{alg}}^{\circ}(f)$
0x3cc3	8	3	0,0	0.219361	1	1
0x5aa5	8	3	0,0	0.219361	1	1
0x6699	8	3	0,0	0.219361	1	1
0x6969	8	3	0,0	0.219361	1	1
0x6996	8	3	0,0	1	1	1
0x9669	8	3	0,0	1	1	1
0x9696	8	3	0,0	0.219361	1	1
0x9966	8	3	0,0	0.219361	1	1
0xa55a	8	3	0,0	0.219361	1	1
0xc33c	8	3	0,0	0.219361	1	1
0xffff	16	4	0,0	0	0	0

Functions f are classified by equivalence relationships

- Let us call σ a permutation of $\llbracket 1, n \rrbracket$. Thus

$$\rho_{\text{opt}}^{(1,2)}(f \circ \sigma) = \rho_{\text{opt}}^{(1,2)}(f).$$

- The complementation

$$\rho_{\text{opt}}^{(1,2)}(\neg f) = \rho_{\text{opt}}^{(1,2)}(f).$$

Solutions are derived from: $f(x_1, x_2, x_3, x_4) = x_1 \oplus x_2 \oplus x_3, \bigoplus_i x_i, 1$.

Note: \mathcal{M} does not decompose as $\tilde{\mathcal{M}} \cup \neg\tilde{\mathcal{M}}$,

Case $n = 5$

Nb. classes	HW[f]	H[M]	$\rho_{\text{opt}}^{(1)}$	$\rho_{\text{opt}}^{(2)}$	I[HW[Z \oplus M]; Z]	I[Z \oplus M; Z]	$d_{\text{alg}}^{\text{O}}(f)$
3	8	3	0	0	0.32319	2	2
4	12	3.58496	0	0	0.18595	1.41504	3
2	16	4	0	0	0.08973	1	1
2	16	4	0	0	0.08973	1	2
4	16	4	0	0	0.12864	1	2
2	16	4	0	0	0.16755	1	1
4	16	4	0	0	0.26855	1	2
6	16	4	0	0	0.32495	1	2
1	16	4	0	0	1	1	1
4	20	4.32193	0	0	0.07349	0.67807	3
3	24	4.58496	0	0	0.04300	0.41504	2
1	32	5	0	0	0	0	0

Here, we start to see the compromise, with good choices in **bold**.

SAT solvers

- f is a 2^n Boolean variable set, noted $\{f_x = f(x), x \in \mathbb{F}_2^n\}$.
- For every value Price (defined as $\text{Card}[\mathcal{M}]$), we have:

$$\forall a, 1 \leq \text{HW}[a] \leq 2, \quad \sum_x f(x)(-1)^{a \cdot x} = 0 \quad \Leftrightarrow$$

$$\forall a, 1 \leq \text{HW}[a] \leq 2, \quad \sum_x f_x \wedge (a \cdot x) = \frac{\sum_x f_x}{2} = \frac{\text{Card}[\mathcal{M}]}{2}.$$

- More precisely, any condition " $\leq k(f_1, \dots, f_n)$ ", for $0 \leq k \leq n$, can be expressed in terms of CNF clauses [Sin05]. We note that:

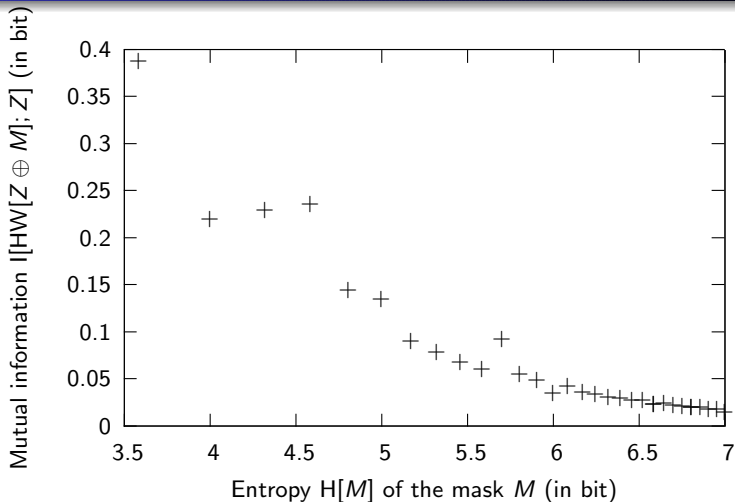
$$\text{HW}[f] \leq k \quad \Leftrightarrow \quad n - \text{HW}[\neg f] \leq k \quad \Leftrightarrow \quad \text{HW}[\neg f] \geq n - k.$$

- Example: 256 literals, but 1,105,664 auxiliary variables and 2,219,646 clauses, irrespective of $\text{Card}[\mathcal{M}] \in \mathbb{N}^*$.

Summary for $n = 8$

- $\text{Card}[\mathcal{M}] = 12$. One MIA found, 0.387582 bit
- $\text{Card}[\mathcal{M}] = 16$. Many MIA, in $[0.181675, 1.074950]$ bit.
- There are solutions only for $\text{Card}[\mathcal{M}] \in \{4 \times \kappa, \kappa \in \llbracket 3, 61 \rrbracket \cup \{64\}\}$.

Example of solutions



- 1 Introduction
 - Side-Channel Analysis (SCA)
 - Countermeasures
 - Goal of the Presentation
- 2 RSM: Rotating Sboxes Masking
 - Rationale of the Countermeasure
 - RSM Modelization
- 3 Information Theoretic Evaluation of RSM
- 4 Security Evaluation of RSM against CPA and 2O-CPA
 - Optimal HO-CPA
 - Expression of $\rho_{\text{opt}}^{(1,2)}$
- 5 Conclusions and Perspectives

Conclusions

- It is possible to achieve high-order security even with depleted entropy
- Case treated in the presentation: Resist 1O-CPA and 2O-CPA, with fewer masks as possible.
- We discovered that $\text{Card}[\mathcal{M}]$ was not the only variable
 \Rightarrow solutions actually depend on \mathcal{M} .
- An encoding in terms of indicator function f of \mathcal{M} shows that we are looking for 2nd order correlation-immune Boolean functions of lowest weight.
- Secure even if \mathcal{M} is public.

Perspectives

- Find other functions for $n > 8$.
- Algebraic constructions:
 - Maiorana-McFarland, or
 - codes of dual-distance $d...$
- Dynamic reconfiguration to update \mathcal{M} on a regular basis?

References

- [DGBN09] Jean-Luc Danger, Sylvain Guilley, Shivam Bhasin, and Maxime Nassar. Overview of Dual Rail with Precharge Logic Styles to Thwart Implementation-Level Attacks on Hardware Cryptoprocessors, — *New Attacks and Improved Counter-Measures* —. In *SCS*, IEEE, pages 1–8, November 6–8 2009. Jerba, Tunisia. DOI: 10.1109/ICSCS.2009.5412599.
- [NGDS12] Maxime Nassar, Sylvain Guilley, Jean-Luc Danger, and Youssef Souissi. RSM: a Small and Fast Countermeasure for AES, Secure against First- and Second-order Zero-Offset SCAs. In *DATE*, March 12-16 2012. Dresden, Germany. (TRACK A: “Application Design”, TOPIC A5: “Secure Systems”).
- [PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan. Statistical Analysis of Second Order Differential Power Analysis. *IEEE Trans. Computers*, 58(6):799–811, 2009.
- [Sin05] Carsten Sinz. Towards an Optimal CNF Encoding of Boolean Cardinality Constraints. In Peter van Beek, editor, *CP*, volume 3709 of *Lecture Notes in Computer Science*, pages 827–831. Springer, 2005.
- [SRQ06] François-Xavier Standaert, Gaël Rouvroy, and Jean-Jacques Quisquater. FPGA Implementations of the DES and Triple-DES Masked Against Power Analysis Attacks. In *FPL*. IEEE, August 2006. Madrid, Spain.

Formal Analysis of the Entropy / Security Trade-off in First-Order Masking Countermeasures against Side-Channel Attacks

Maxime Nassar, Sylvain Guilley and Jean-Luc Danger

Bull TrustWay, Rue Jean Jaurès, B.P. 68,
78 340 Les Clayes-sous-Bois, France.

Institut TELECOM / TELECOM ParisTech,
46 rue Barrault, 75 634 Paris Cedex, France.

Secure-IC S.A.S.,
80 avenue des Buttes de Coësmes,
35700 Rennes, France.