Masking with Codewords in Hardware
— Presentation at CryptArchi 2013 —

Shivam Bhasin, **Claude Carlet**, **Jean-Luc Danger**,
Sylvain Guilley and **Zakaria Najm**

Paris 8 & 13 U., TELECOM-ParisTech and Secure-IC S.A.S.

June 25th, 2013; 14.30–16.00

Side-Channel Leakage

- Current or electromagnetic leakage
  $\Longrightarrow$ "side-channel analyses"
- Sensitive variables (*e.g.* $Z = X \oplus K$) are conveyed **noisy** through a **non-injective function**
- We note: $\boxed{\mathscr{L}^\star = \mathcal{L}^\star(X \oplus k^\star) + N^\star}$, where $N^\star \sim \mathcal{N}(0, \sigma^2)$
- Attacker observes $\mathscr{L}^\star$, can have an idea about $\mathcal{L}^\star$, and enumerates all k

Side-Channel Attacks

- Use a distinguisher $\mathcal{D}(\mathscr{L}^\star; (X, k))$
- Attack possible if $\forall k \neq k^\star$, $\mathcal{D}(\mathscr{L}^\star; (X, k)) \leqslant \mathcal{D}(\mathscr{L}^\star; (X, k^\star))$

Metrics *vs* Distinguishers

Metric

- **Metric**: $\mathcal{D}(A, B) = \text{Var}\left[\mathbb{E}\left[A^d | B\right]\right]$;
- **Attack order**: $\min\{d > 0, \text{Var}\left[\mathbb{E}\left[\mathscr{L}^{\star d} | X, k^\star\right]\right] \neq 0\}$
- This **inter-class variance** is not a distinguisher, since $\forall k$, $\text{Var}\left[\mathbb{E}\left[\mathscr{L}^{\star d} | X, k\right]\right] = \text{Var}\left[\mathbb{E}\left[\mathscr{L}^{\star d} | X\right]\right]$.

Distinguisher

- **Attack**, $\mathcal{D} = \rho$, *i.e. high-order* correlation: $\rho\left[\mathscr{L}^{\star d}; P(X, k)\right] \leqslant \rho\left[\mathscr{L}^{\star d}; P(X, k^\star)\right]$
- Greatest correlation in $k = k^\star \implies$ $P_{\text{opt}}(x, k^\star) = \mathbb{E}\left[\mathscr{L}^{\star d} | X = x\right]$
- $\rho\left[\mathscr{L}^{\star d}; P_{opt}(X, k^\star)\right] = \sqrt{\frac{\text{Var}\left[\mathbb{E}\left[\mathscr{L}^{\star d} | X\right]\right]}{\text{Var}\left[\mathscr{L}^{\star d}\right]}}$ (see [PRB09])

Contributions

- Masking scheme, termed **homomorphic**, $X \longrightarrow X \oplus M$

- Keys are not recovered **uniquely**
- If $C^\star$ (support of M) is *secret*, then **unconditional security**
- If $C^\star = C$ is *public*, then **equiprobable** keys (*ex æquo*)

- Application to AES:
  - $|C| = w = 16$ masked sboxes $\tilde{S}$ (no overhead)
  - Zero-offset correlation attacks: resistance at order $d = 1, 2, 3$.
  - If C is public, number of *ex æquo* is $w = 16$.

State-of-the-Art

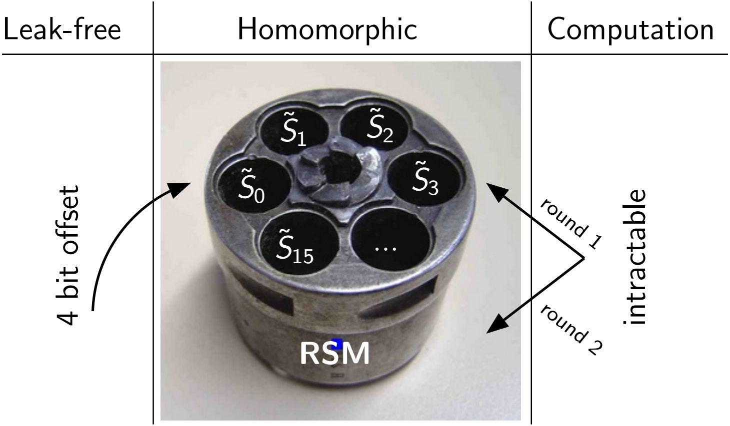
In protection against side-channel attacks

- **Resilience**, in theory (PRF)
- **Resilience**, in practice (key update, rekeying, tweaks, *etc.*)
- **Palliative** protections, *e.g.* [GM11]
- **Curative** protections, *e.g.* dual-rail, masking

In masking

- **Provable masking**: 800 bytes of randomness for AES protected at order $d = 1$
- **Threshold implementations**, withstand glitches (that can be suppressed by other means [MM12])
- **Homomorphic masking**:
  - Configure the algorithm
  - Compute homomorphically

Homomorphic Masking Scheme: Description



$\tilde{S}_i(Z) \doteq S(Z \oplus M_i) \oplus M_{i+1 \mod 16}$: precomputed sboxes.

Security metric

Theorem (RSM security [BCG13])

Let $\mathscr{L} = \mathcal{L}(X \oplus M \oplus k^\star)$, where $\mathcal{L} : \mathbb{F}_2^n \to \mathbb{R}$ is a form, $X \sim \mathcal{U}(\mathbb{F}_2^n)$ and $M \sim \mathcal{U}(C)$ are two random variables, and $k^\star \in \mathbb{F}_2^n$ is a secret key. Then,

$$d = \min\left\{i > 0,\ \mathrm{Var}\left[\mathbb{E}\left[\mathscr{L}^i | X\right]\right] \neq 0\right\} \iff$$

$$C \text{ is a code of dual distance } d_C^\perp = d \ .$$

- Attacks of order $d < d_C^\perp$ fail
- Attacks of order $d \geqslant d_C^\perp$ succeed

Attack Metric

For a Hamming weight leakage:

$$\forall d < d_C^{\perp}, \quad \mathrm{Var}\left[\mathbb{E}\left[\mathscr{L}^{d} | Z\right]\right] = 0 \tag{1}$$

and

$$\mathrm{Var}\left[\mathbb{E}\left[\mathscr{L}^{d_C^{\perp}} | Z\right]\right] = B^{\perp}_{d_C^{\perp}} \left(\frac{d_C^{\perp}!}{2^{d_C^{\perp}}}\right)^2 \quad . \tag{2}$$

Table: Coefficients of the distance enumerator polynomial for the studied codes ($B^{\perp}_{d^{\perp}_C}$ in **bold**).

Code #	Nickname	$B^{\perp}_0$	$B^{\perp}_1$	$B^{\perp}_2$	$B^{\perp}_3$	$B^{\perp}_4$	$B^{\perp}_5$	$B^{\perp}_6$	$B^{\perp}_7$	$B^{\perp}_8$
1	*M0_1*	1	**8**	28	56	70	56	28	8	1
2	*M1_2*	1	0	**28**	0	70	0	28	0	1
3	*M2_16*	1	0	0	**4.5**	5	3	2	0.5	0
4	*M2_16_bis*	1	0	0	**3.5**	7	3.5	0	0	1
5	*M2_16_bis2*	1	0	0	**3.5**	7	3.5	0	0	1
6	*M2_16_ter*	1	0	0	**4**	5	4	2	0	0
7	*M3_16*	1	0	0	0	**14**	0	0	0	1

- **Code length**: $n = 8$
- **Code size**: $M0\_1 : 1$, $M1\_2 : 2$, $others : 16$

Leakage Metric

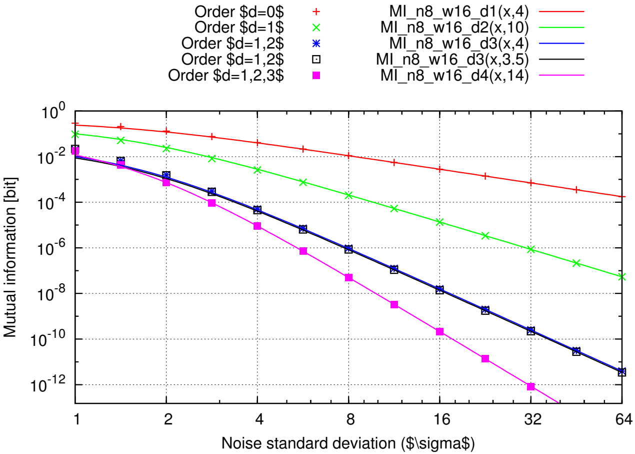


Figure: Approximation of $\mathrm{I}\left[\mathscr{L}+N; Z\right]$ by $\left(d_C^{\perp}! B_{d_C^{\perp}}^{\perp}\right) \Big/ \left(2\ln 2 \cdot 2^{2d_C^{\perp}} \sigma^{2d_C^{\perp}}\right)$.

Playing with two parameters

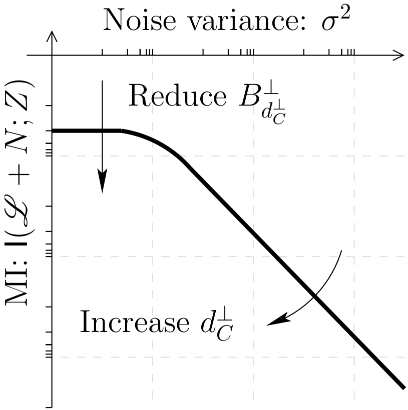


Figure: Two concomitant objectives to reduce the mutual information.

In concrete cases, it is better to increase $d_C^\perp$

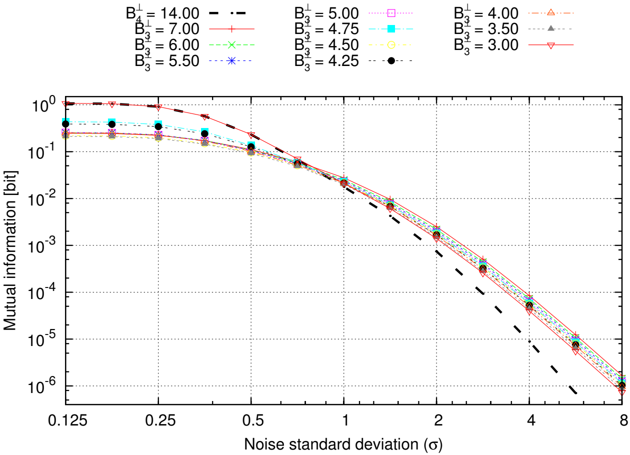


Figure: Computation of MI *versus* the noise standard deviation for optimal and non-optimal dual distances, when $n = 8$ and $w = 16$.

Ties in High-Order Correlation Attacks [CG13]

Ingredients

- Leakage function: $\mathscr{L} = \mathcal{L}(X \oplus M \oplus K)$
- $M \in C \subseteq \mathbb{F}_2^n$, and f the indicator of C
- d: attack order

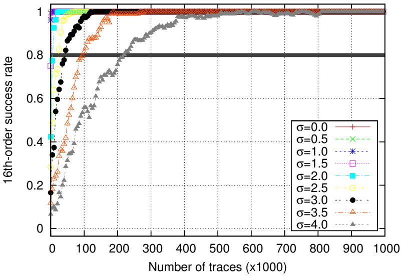
Ex æquo keys

The attacker recovers

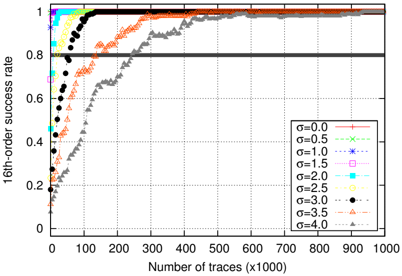
- $k^\star \oplus \{\text{null linear structures of } \mathcal{L}^d \otimes f\}$,
- *i.e.* $k^\star \oplus \{\text{null linear structures of } f\}$ .... (for non-special $\mathcal{L}$),
- *i.e.* $k^\star \oplus \mathrm{dir}(C)$ .... (when the code is affine),
- *i.e.* $k^\star \oplus C$ .... (when the code is linear).

So, we end up on an *intuitive* result (modulo some conditions).

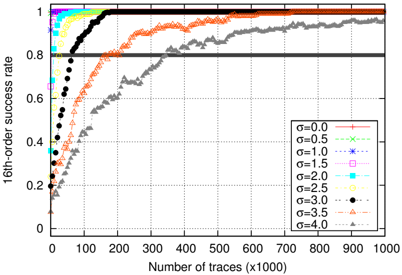
$M2\_16$ at order $d = 3$



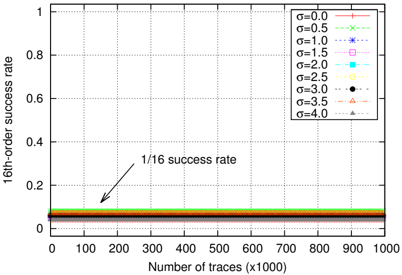
$M2\_16\_bis$ at order $d = 3$



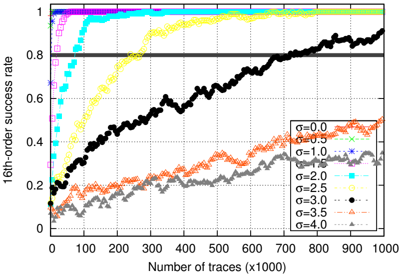
$M2\_16\_ter$ at order $d = 3$



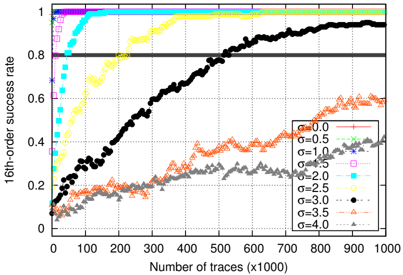
$M3\_16$ at order $d = 3$



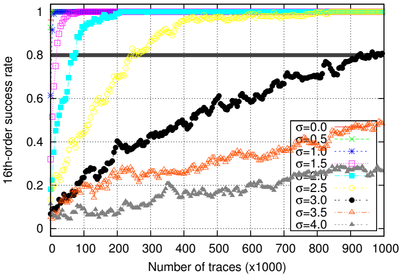
$M2\_16$ at order $d = 4$



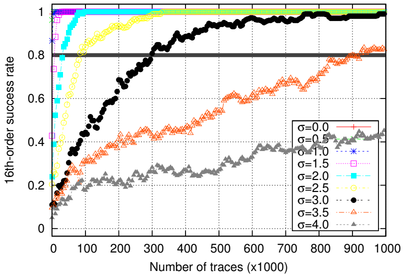
$M2\_16\_bis$ at order $d = 4$



$M2\_16\_ter$ at order $d = 4$



$M3\_16$ at order $d = 4$



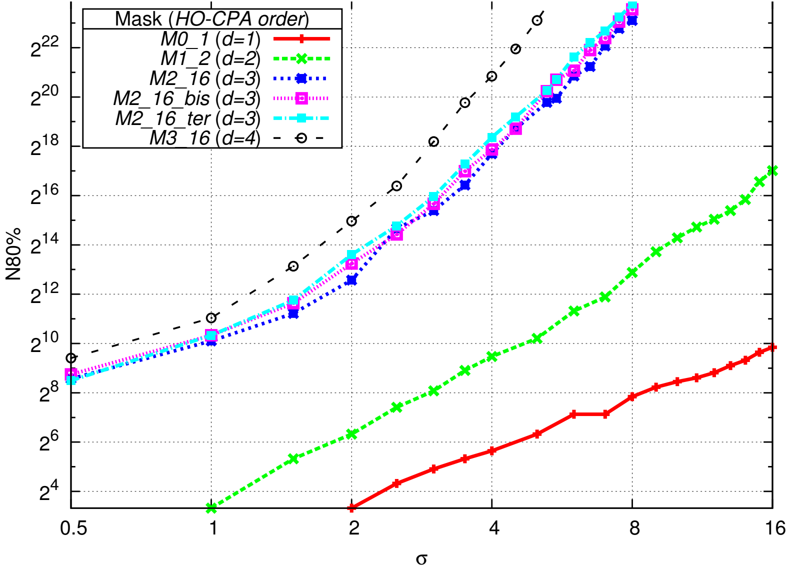


Figure: Number of traces to achieve a success rate $\geqslant 80\%$ for various noise standard deviations σ.

Summary

Collect leakage → Preprocess → Distinguish

$\mathscr{L}^\star$ → $\mathscr{L}^{\star d_C^\perp}$ → $\rho_{k^\star,k} = \rho\left[\mathscr{L}^{\star d_C^\perp}; P_{\mathrm{opt}}(X,k)\right]$

$C \neq C^\star$:

$$\operatorname*{argmax}_{k \in \mathbb{F}_2^n} \rho_{k^\star,k} = \mathbb{F}_2^n$$

↓

Unconditional security

✖ Attack failed

$C = C^\star$:

$$\operatorname*{argmax}_{k \in \mathbb{F}_2^n} \rho_{k^\star,k} = k^\star \oplus \mathrm{dir}(C)$$

↓

Brute force (2^{64})

✔ Attack successful

Conclusions

- **Application to AES**:
  - Lucky code C of characteristic $[8, 4, 4]$, self-dual ($d_C^\perp = n - d_{C^\perp} = 8 - d_C = 4$, hence $d_C^\perp = d_C$)
  - $|C| = w = 16$ sboxes (no overhead)
  - Zero-offset correlation attacks: resistance at order $d = 1, 2, 3$, since $d^\perp = 4$
  - If C is public, number of *ex æquo* is $w = 16$.
    - $16^{16} = 2^{64}$ hypotheses for the whole key

Bibliography I

[BCG13] Shivam Bhasin, Claude Carlet, and Sylvain Guilley.
Theory of masking with codewords in hardware: low-weight dth-order correlation-immune Boolean functions.
Cryptology ePrint Archive, Report 2013/303, 2013.
http://eprint.iacr.org/2013/303/.

[CG13] Claude Carlet and Sylvain Guilley.
Side-Channel Indistinguishability.
In *HASP*, pages 9:1–9:8, Tel-Aviv, Israel, June 23-24 2013. ACM.
Extended version:
http://hal.archives-ouvertes.fr/hal-00826618/en.

[GM11] Tim Güneysu and Amir Moradi.
Generic side-channel countermeasures for reconfigurable devices.
In Bart Preneel and Tsuyoshi Takagi, editors, *CHES*, volume 6917 of *LNCS*, pages 33–48. Springer, 2011.

Bibliography II

[MM12] Amir Moradi and Oliver Mischke.
Glitch-free Implementation of Masking in Modern FPGAs.
In *HOST*, IEEE Computer Society, pages 89–95, June 2-3 2012.
Moscone Center, San Francisco, CA, USA. DOI:
10.1109/HST.2012.6224326.

[PRB09] Emmanuel Prouff, Matthieu Rivain, and Régis Bevan.
Statistical Analysis of Second Order Differential Power Analysis.
IEEE Trans. Computers, 58(6):799–811, 2009.

Masking with Codewords in Hardware
— Presentation at CryptArchi 2013 —

Shivam Bhasin, **Claude Carlet**, **Jean-Luc Danger**,
Sylvain Guilley and **Zakaria Najm**

Paris 8 & 13 U., TELECOM-ParisTech and Secure-IC S.A.S.

June 25th, 2013; 14.30–16.00

www.proofs-workshop.org

proofs

- Home
- Venue
- Call for papers
- Call for sponsors
- Submissions
- Program
- Registration
- Committees
- About PROOFS...

PROOFS: Security Proofs for Embedded Systems

UCSB, Santa Barbara, CA, USA — Saturday, August 24th, 2013

Announcement for PROOFS 2013

PROOFS 2013 will be held at UCSB (Santa Barbara, CA) on August 24, after CRYPTO and CHES.
All accepted papers will be published in the Journal of Cryptographic Engineering.

Important dates

• Diffusion of the CfP:	**Friday February 8th, 2013**
• Submission deadline:	**Saturday July 20th, 2013 (Deadline extension!!!)**
• Authors notification:	**Sunday July 28th, 2013**
• Final version due:	**Sunday August 11th, 2013**
• PROOFS workshop venue:	**Saturday August 24th, 2013**

Sponsors

Other conferences of interest

FPS, La Rochelle

- *Foundations and Practice of Security*
- October 21-22, 2013
- Springer LNCS
- http://conferences.telecom-bretagne.eu/fps/2013/

SPACE, IIT Kharagpur

- *Security, Privacy, and Applied Cryptography Engineering*
- October 19-23, 2013
- Springer LNCS
- http://cse.iitkgp.ac.in/conf/SPACE2013/

DPA contest V4

http://www.dpacontest.org/

- Masked AES 8-bit software implementation
- Source code & masks are made available
- Mask=0 breaks in <50 traces
- 100,000 traces available
- ~400,000 time samples per trace (1st round only)
- Any attack: 1st/hi-order, uni-/multi-variate attacks are acceptable