Countermeasures against Physical Attacks using Error-Correcting Codes

Sylvain GUILLEY[1,2]

[1]Institut MINES-TELECOM, TELECOM-ParisTech
[2]Secure-IC S.A.S.

MCrypt, August 13, 2014 – Les Deux Alpes

Presentation Outline

Presentation Outline

Definition

- Let k and n be two integers, such that $k \leq n$.
- The set of n-bit vectors, noted $\mathbb{F}_2^n$, is endowed with a structure of space vector.
- Let $\mathcal{C}$ be a subspace of $\mathbb{F}_2^n$ of dimension k.
- Then, $\mathcal{C}$ is a linear code of length n and dimension k.

Definition (supplement of a space vector)

$\mathcal{C}$ can be completed with some vectors in order to spawn $\mathbb{F}_2^n$. Those vectors define the supplement $\mathcal{D}$ of $\mathcal{C}$ in $\mathbb{F}_2^n$. We write $\mathbb{F}_2^n = \mathcal{C} \oplus \mathcal{D}$ to say that $\mathbb{F}_2^n$ is the direct sum of $\mathcal{C}$ and $\mathcal{D}$.

A linear code is spawned by a basis: the matrix whose rows consist in the basis vectors is called a *generating matrix*. We denote by G (resp. H) the generating matrix of $\mathcal{C}$ (resp. $\mathcal{D}$, the supplement of $\mathcal{C}$). Then, we have that every element $z \in \mathbb{F}_2^n$ can be written uniquely as:

$$\boxed{z = c \oplus d} \ , \tag{1}$$

where $c \in \mathcal{C}$ and $d \in \mathcal{D}$. Now, as all $c \in \mathcal{C}$ (resp. $d \in \mathcal{D}$) can also be written uniquely as xG (resp. yH), for a given $x \in \mathbb{F}_2^k$ (resp. $y \in \mathbb{F}_2^{n-k}$), we have the following equation:

$$\boxed{z = xG \oplus yH} \ . \tag{2}$$

Definition (minimal distance)

The minimal distance $d_{\mathcal{C}}$ of a linear code $\mathcal{C}$ of length n and dimension k is the minimal Hamming distance of any two different elements of $\mathcal{C}$. We say that $\mathcal{C}$ has parameters $[n, k, d_{\mathcal{C}}]$.

Definition (dual distance)

The dual distance $d_{\mathcal{C}}^{\perp}$ of a code $\mathcal{C}$ is the minimal Hamming weight $\mathrm{HW}(z)$ of a nonzero vector $z \in \mathbb{F}_2^n$ such as $\sum_{c \in \mathcal{C}} (-1)^{z \cdot c} \neq 0$, where $z \cdot c$ is the scalar product between z and c:

- $z \cdot c = \sum_{i=1}^{n} z_i c_i$, or equivalently
- $z \cdot c = z c^{\mathsf{T}} \in \mathbb{F}_2$ using matrix notations.

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance $= 4$:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 1:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 1:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 1:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 2:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 2:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 2:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 2:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 3:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 3:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 3:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance > 3:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

Definition (orthogonal)

The orthogonal of a set $\mathcal{C} \subseteq \mathbb{F}_2^n$ is the space vector $\mathcal{C}^\perp$ defined as $\{d \in \mathbb{F}_2^n | \forall c \in \mathcal{C}, d \cdot c = 0\}$. When $\mathcal{C}$ is a linear code, $\mathcal{C}^\perp$ is called the dual code of $\mathcal{C}$. The generating matrix of $\mathcal{C}^\perp$ is called the parity matrix of $\mathcal{C}$.

Proposition

For a linear code $\mathcal{C}$, $d_{\mathcal{C}}^\perp = d_{\mathcal{C}^\perp}$.

Non-linear codes

- Systematic codes can be better than linear codes
- Ex. The Nordstrom-Robinson code $(16, 2^8, 6)$, though the BKLC is $[16, 8, 5]$.
- But the NR is ... $\mathbb{Z}_4$-linear ($[8, 4, 6]_{\mathbb{Z}_4}$, with $\{0, 1, 2, 3\} \rightarrow \{00, 01, 11, 10\}$).
- Distance polynomial:
  - $D_{\mathcal{C}}(X, Y) = \frac{1}{\text{Card}[C]} \sum_{x,y \in \mathcal{C}} X^{n-\text{HD}(x,y)} Y^{\text{HD}(x,y)}$.
  - $D_C(X, Y) = \sum_{d=0}^{n} B_d X^{n-d} Y^d$, where B_d is the normalized distance distribution, equal to: $\frac{1}{\text{Card}[C]} \text{Card}[\{(x, y) \in C \times C \text{ s.t. } \text{HD}(x, y) = d\}]$.
- The dual distance distribution $B_d^{\perp} \in \mathbb{Q}^+$ is the MacWilliams transform of the distance distribution, in the sense that $D_C^{\perp}(X, Y) = \frac{1}{\text{Card}[C]} D_C(X + Y, X - Y) = \sum_{d=0}^{n} B_d^{\perp} X^{n-d} Y^d$. The dual distance $d_C^{\perp}$ of C is the smallest $d > 0$ s.t. $B_d^{\perp} \neq 0$.

Constructions

- Cyclic codes, as an ideal of $\mathbb{F}[X]/(X^n - 1)$.
- Secondary constructions:
  - Puncturing, shortening, $(u, u + v)$, etc.
  - Example: [CG14a]. Let $\mathcal{C}$ be the QR (cyclic) $[17, 9, 5]$-code whose zeroes are β^i, $i = 1, 2, 4, 8, 9, 13, 15, 16$ where β is a primitive n-th root of unity. The generator polynomial of $\mathcal{C}$ is $X^8 + X^7 + X^6 + X^4 + X^2 + X + 1$. The shortened $\mathcal{C}_{\{17\}}$ has parameters $[16, 8, 5]$.
- BCH bound: longest string + 1; QR codes: $d_{\mathcal{C}} \geq \sqrt{n}$.

```
C:=QRCode(FiniteField(2),89);
MinimumDistance(C)
# ==> 17
```

but $BCH = 3, \lceil \sqrt{89} \rceil = 10$.

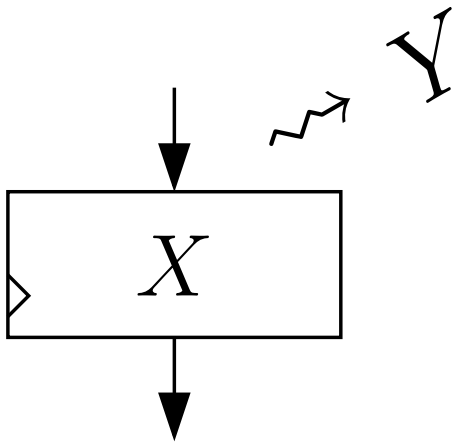
Presentation Outline

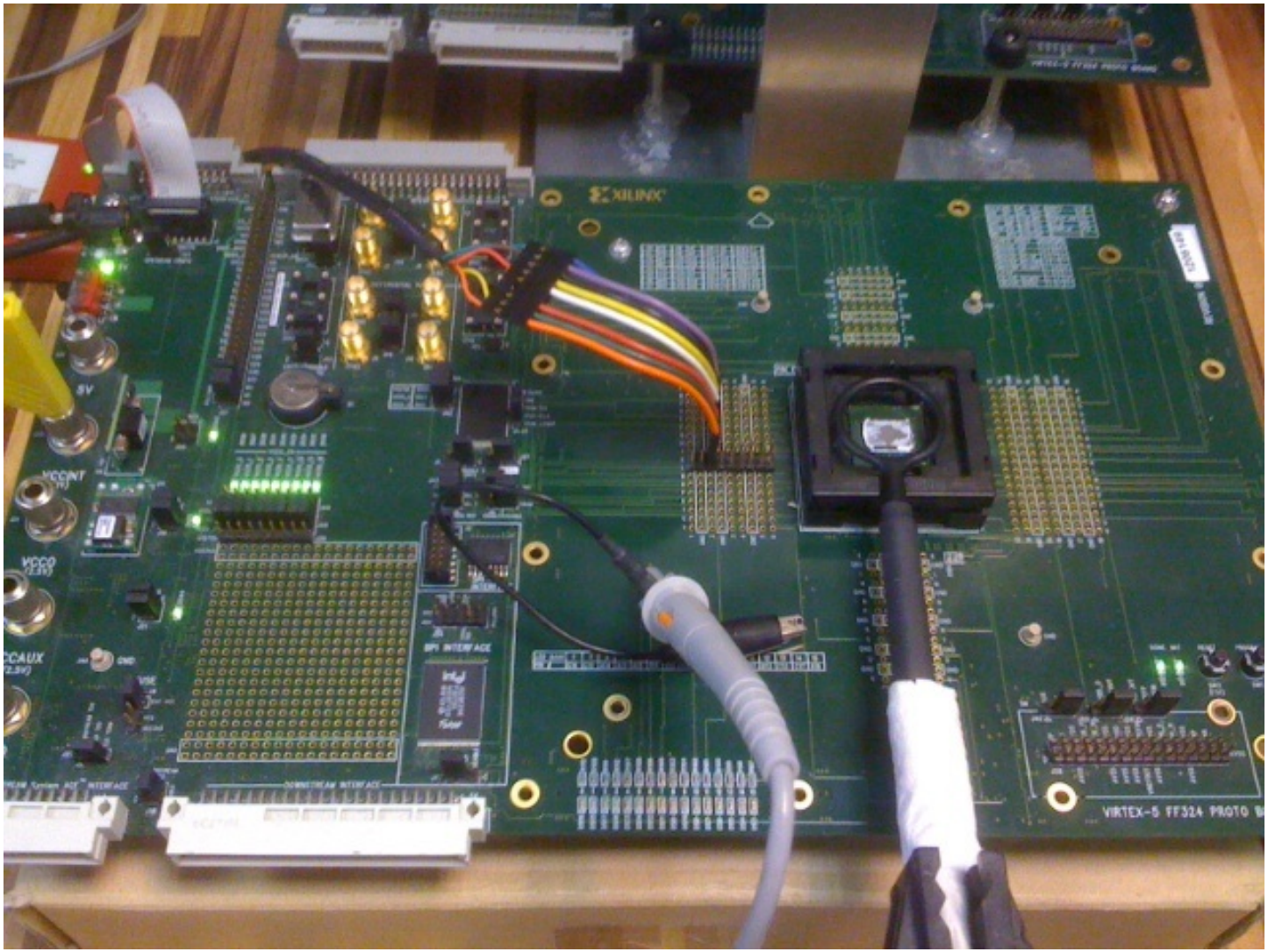
Masking (1/3)

Fact:

manipulating a variable leaks.

$X \rightsquigarrow Y$



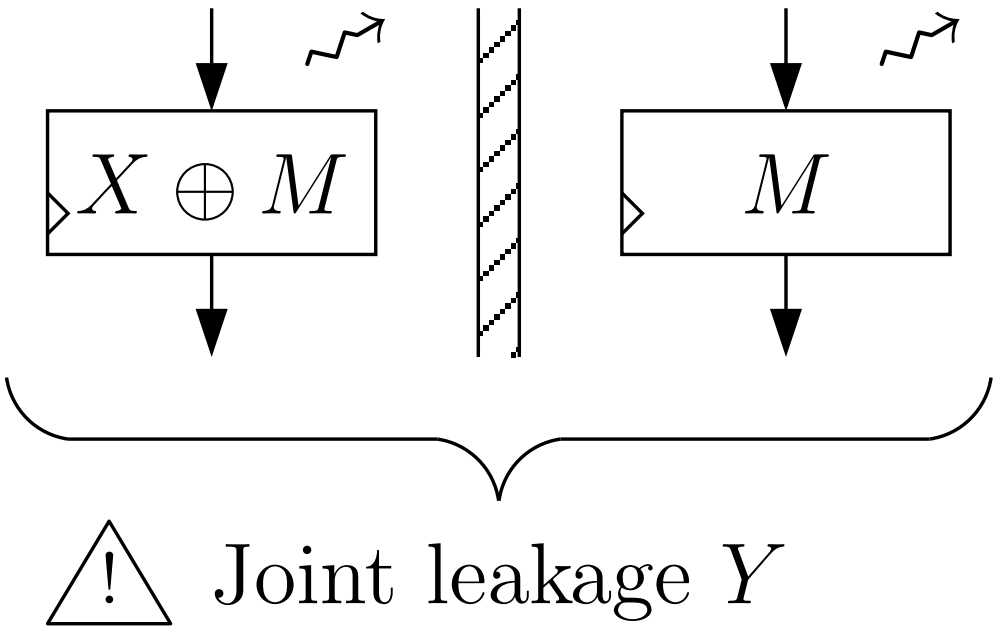

XILINX
VIRTEX-5 FF324 PROTO

Masking (2/3)

Fact:

manipulating a variable leaks.

$X \rightsquigarrow Y$



Masking (3/3)

Two drawbacks in this approach (namely: $Y = \mathrm{HW}(X \oplus M) + N$):

1. Existance of second-order attacks
2. Cost of masking non-linear functions ($n \times n \quad \rightarrow \quad 2n \times 2n$)

Unless...

1. Secure S-box computation ..... [RP10]
2. H-tables ..... [Cor13]

... long to execute (but a nice software protection)

Objective: minimize the attack **degree** (not the order!)

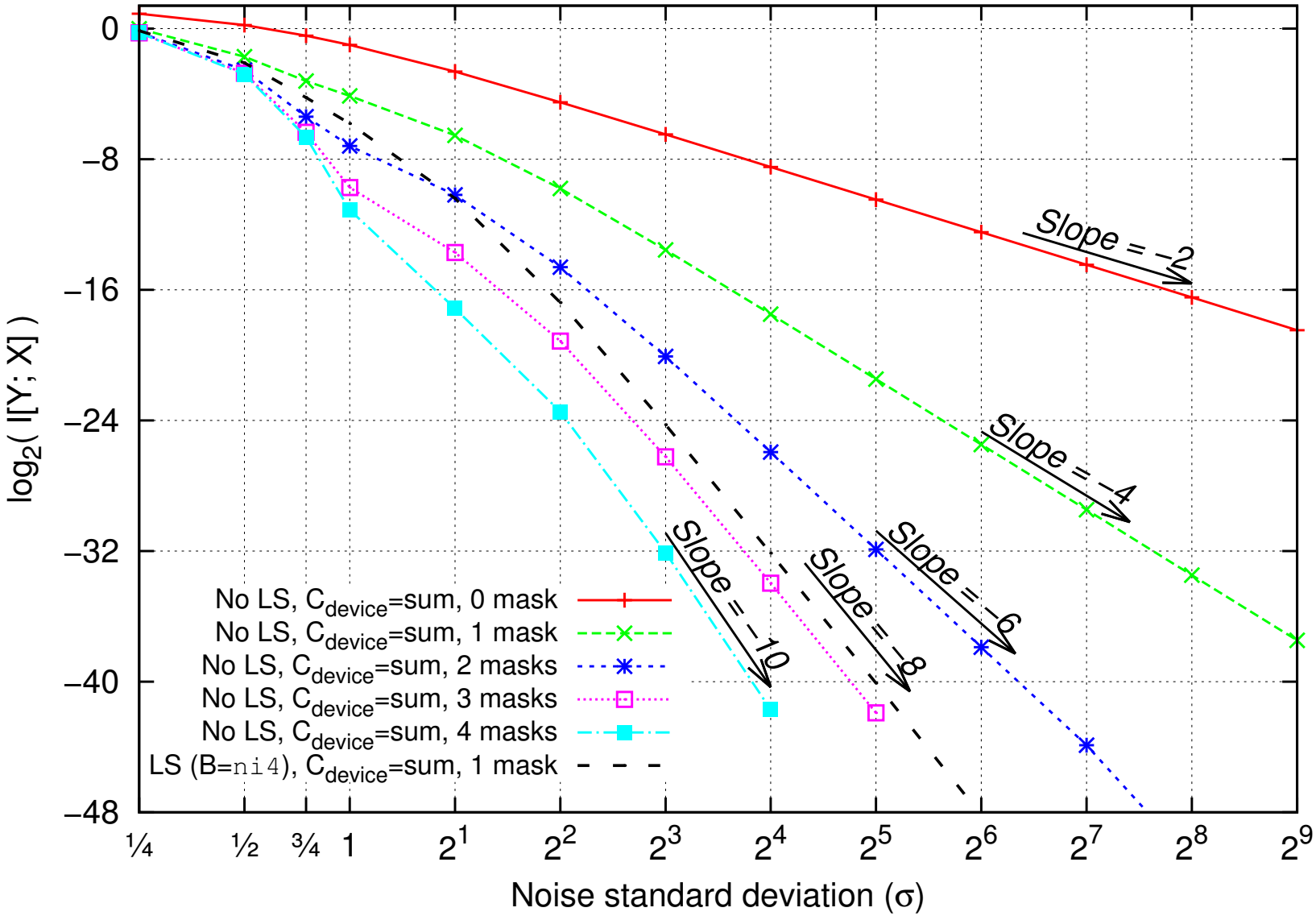
- Maximize d such as $\mathrm{Var}[\mathbb{E}[Y^d \mid X]] = 0$.
- We define Higher-order Correlation Immunity (HCI, [CDG+14]) as:

$$\mathrm{HCI} = \min\{d \in \mathbb{N}^\star; \mathrm{Var}[\mathbb{E}[Y^d \mid X]] > 0\} \ .$$

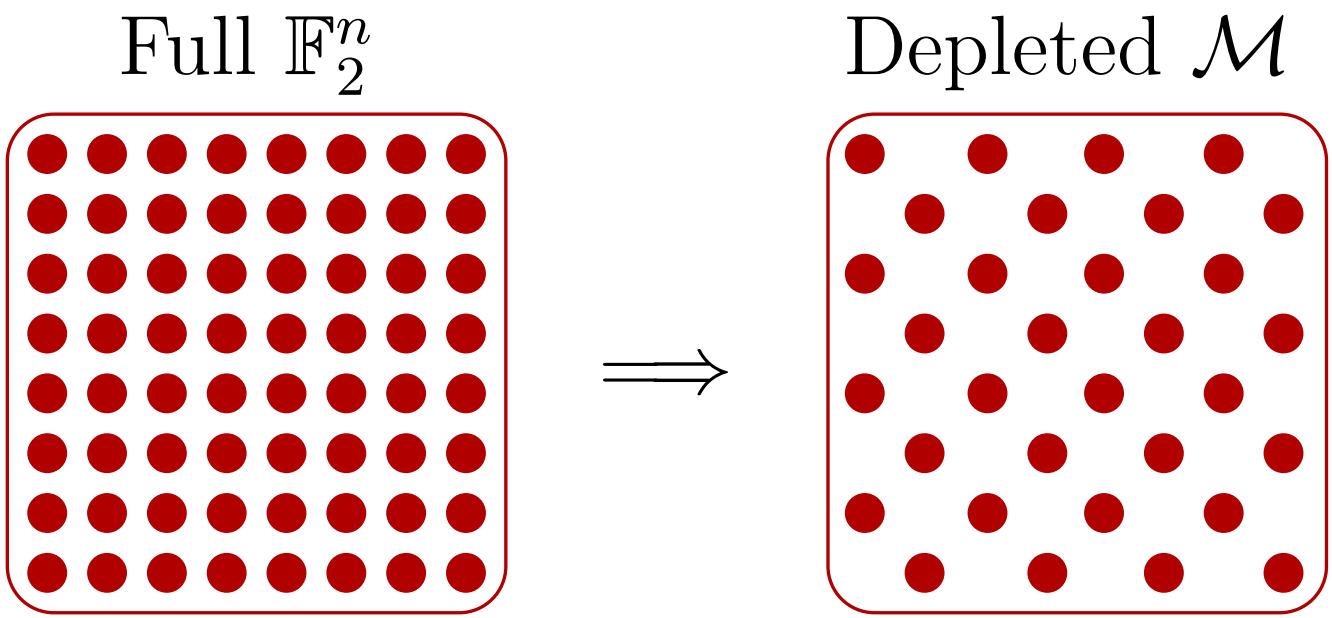
- Theorem 1 in [CDG+14]:

Theorem

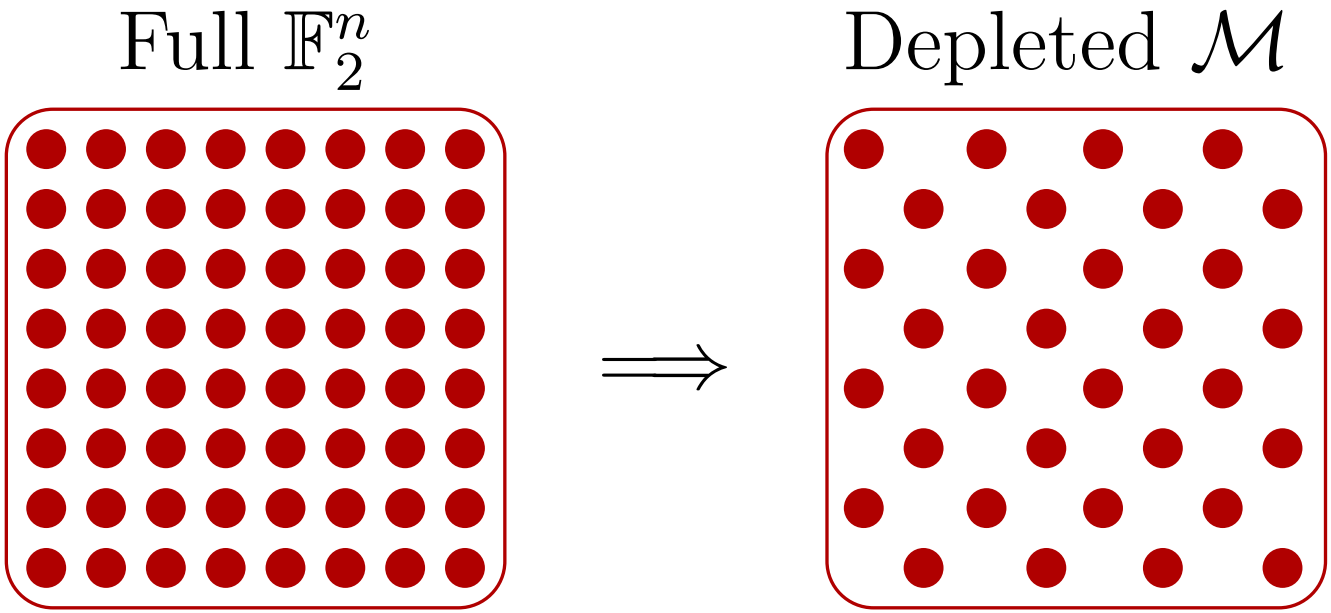
Let σ denote the standard deviation of the noise N, the mutual information $\mathrm{I}[X; Y]$ tends towards $\mathcal{O}\left(\sigma^{-2\times \mathrm{HCI}}\right)$ when σ tends towards infinity.


0
−8
−16
−24
−32
−40
−48
log2(I[Y; X])
¼
½
¾
1
2^1
2^2
2^3
2^4
2^5
2^6
2^7
2^8
2^9
Noise standard deviation (σ)
Slope = −2
Slope = −4
Slope = −6
Slope = −8
Slope = −10
No LS, Cdevice=sum, 0 mask
No LS, Cdevice=sum, 1 mask
No LS, Cdevice=sum, 2 masks
No LS, Cdevice=sum, 3 masks
No LS, Cdevice=sum, 4 masks
LS (B=ni4), Cdevice=sum, 1 mask

LEMS . . . . . Principle



LEMS . . . . . Principle



E.g., $\mathcal{M} = \{\texttt{0x00}, \texttt{0xff}\} \implies \mathsf{HCI} = 2$

Proof of the two-masks protection [BDGN13]

$$
\begin{aligned}
& \mathrm{Var}[\mathbb{E}[Y^1 \mid X]] = 0 \\
\iff & \forall x \in \mathbb{F}_2^n,\ \mathbb{E}[Y \mid X = x] = \mathbb{E}[Y] \\
\iff & \forall x \in \mathbb{F}_2^n,\ \mathbb{E}[\mathrm{HW}(X \oplus M) \mid X = x] = \mathbb{E}[Y] \\
\iff & \forall x \in \mathbb{F}_2^n,\ \mathbb{E}[\mathrm{HW}(x \oplus M)] = \mathbb{E}[Y] \\
\iff & \forall x \in \mathbb{F}_2^n,\ \sum_{m \in \{\mathtt{0x00}, \mathtt{0xff}\}} \frac{1}{2}\mathrm{HW}(x \oplus m) = \mathbb{E}[Y] \\
\iff & \forall x \in \mathbb{F}_2^n,\ \mathrm{HW}(x \oplus \mathtt{0x00}) + \mathrm{HW}(x \oplus \mathtt{0xff}) = 2\mathbb{E}[Y] \\
\iff & \forall x \in \mathbb{F}_2^n,\ \mathrm{HW}(x) + \mathrm{HW}(\neg x) = 2\mathbb{E}[Y] \\
\iff & \forall x \in \mathbb{F}_2^n,\ n = 2\mathbb{E}[Y]
\end{aligned}
$$

It is easy to prove that it applies also to $Y = \sum_{i=1}^{n} \alpha_i x_i$, $\alpha_i \in \mathbb{R}$.

RSM: Rotating Sboxes Masking . . . . . Implementation

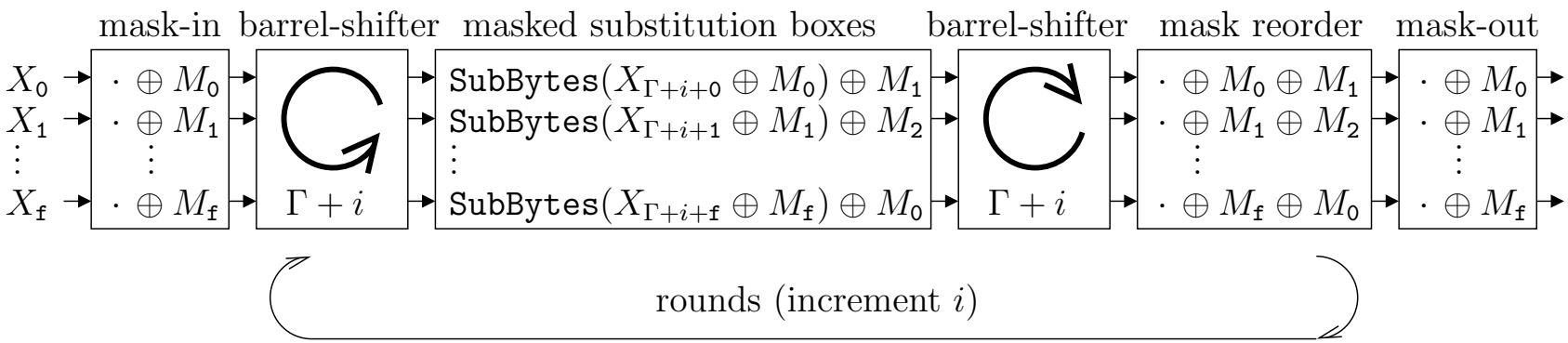
Leakage Model

$Y = \mathrm{HW}(M \oplus X)$, where $M \sim \mathcal{U}(\mathcal{M})$, with $\mathcal{M} \subseteq \mathbb{F}_2^n$.

Solution

The scheme is dth-degree secure if $1_{\mathcal{M}} : \mathbb{F}_2^n \to \mathbb{F}_2$ is dth-order correlation immune.

For AES: 16 identical S-boxes = SubBytes.



Equivalent properties of a code C and its indicator function f [MS77].

Code $C \subseteq \mathbb{F}_2^n$	**Indicator** $f : \mathbb{F}_2^n \to \mathbb{F}$ **of** C
C has size $w = \mathrm{Card}[C]$	f has weight $w = \widehat{f}(0)$
C has dual distance $d_C^\perp$	f is $(d_C^\perp - 1)$-CI and not $d_C^\perp$-CI
$B_d^\perp = \sum_{\substack{z \in \mathbb{F}_2^n, \text{ s.t.} \\ \mathrm{HW}(z)=d}} \left(\frac{1}{\mathrm{Card}[C]} \sum_{x \in C} (-1)^{x \cdot z} \right)^2$	$B_d^\perp = \sum_{\substack{z \in \mathbb{F}_2^n, \text{ s.t.} \\ \mathrm{HW}(z)=d}} \left(\widehat{f}(z) / \widehat{f}(0) \right)^2$

"*Implementation attacks*" side		"*Countermeasures*" side
Resistance at degree d to high-order correlation attacks		The indicator of the masks $\mathcal{M} = \text{supp}(M)$ is a dth-order correlation-immune Boolean function
$\forall i \in [\![1, d]\!]$, $\text{Var}[\mathbb{E}[w_H(X \oplus M)^i \mid X]] = 0$	$\Longleftrightarrow$	$\forall x \in \mathbb{F}_2^n, 1 \leq w_H(x) \leq d$, $\sum_{m \in \mathcal{M}} (-1)^{x \oplus m} = 0$

$n = 8$, $|\mathcal{C}| = 2^4$: Boolean linear code $[8, 4, 4]$

Dual distance $= 4$:

0x00	0	0	0	0	0	0	0	0
0x0f	0	0	0	0	1	1	1	1
0x36	0	0	1	1	0	1	1	0
0x39	0	0	1	1	1	0	0	1
0x53	0	1	0	1	0	0	1	1
0x5c	0	1	0	1	1	1	0	0
0x65	0	1	1	0	0	1	0	1
0x6a	0	1	1	0	1	0	1	0
0x95	1	0	0	1	0	1	0	1
0x9a	1	0	0	1	1	0	1	0
0xa3	1	0	1	0	0	0	1	1
0xac	1	0	1	0	1	1	0	0
0xc6	1	1	0	0	0	1	1	0
0xc9	1	1	0	0	1	0	0	1
0xf0	1	1	1	1	0	0	0	0
0xff	1	1	1	1	1	1	1	1

Properties of the code [CG14b]

$$G = \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{array}\right) .$$

generates a *self-dual* code and *BKLC*.

Proposition

There are only three different distributions of $\mathsf{HW}(y \oplus M)$*, when* $M \sim \mathcal{U}(C)$ *when* $y \in \mathbb{F}_2^8$*. Namely, the set of probabilities* $(p(\mathsf{HW}(y \oplus M) = \ell))_{\ell \in [\![0,8]\!]}$ *are equal to:*

1. $\left(\frac{1}{16}, 0, 0, 0, \frac{14}{16}, 0, 0, 0, \frac{1}{16}\right)$ *if* $y \in C$*;*
2. $\left(0, \frac{1}{16}, 0, \frac{7}{16}, 0, \frac{7}{16}, 0, \frac{1}{16}, 0\right)$ *if there exists a codeword of Hamming weight* 1 *in* $y \oplus C$*;*
3. $\left(0, 0, \frac{4}{16}, 0, \frac{8}{16}, 0, \frac{4}{16}, 0, 0\right)$ *if there exists a codeword of Hamming weight* 2 *in* $y \oplus C$*.*

$$\mathrm{Var}[\mathbb{E}[\mathscr{L}^{d+1}|Z]] = \frac{1}{2^{2n}} \sum_{\substack{z\in\mathbb{F}_2^n, \text{ s.t.} \\ \mathrm{HW}(z)=d+1}} \left(\frac{\widehat{f}(z)}{\widehat{f}(0)} \cdot \widehat{\mathcal{L}^{d+1}}(z) \right)^2 . \qquad (3)$$

For a Hamming weight leakage:

$$\forall d < d_C^\perp, \mathrm{Var}[\mathbb{E}[\mathscr{L}^d|Z]] = 0 \quad \text{and} \quad \mathrm{Var}[\mathbb{E}[\mathscr{L}^{d_C^\perp}|Z]] = B_{d_C^\perp}^\perp \left(\frac{d_C^\perp !}{2^{d_C^\perp}} \right)^2 .$$

$$\mathsf{I}[\mathscr{L}+N;Z] = \frac{1}{\ln 2}\sum_{d=0}^{+\infty}\frac{1}{2\,d!}\sum_{z\in\mathbb{F}_2^n} p(Z=z)\frac{\left(k_d(\mathscr{L}\mid Z=z)-k_d(\mathscr{L})\right)^2}{\left(\mathrm{Var}[\mathscr{L}]+\sigma^2\right)^d}$$

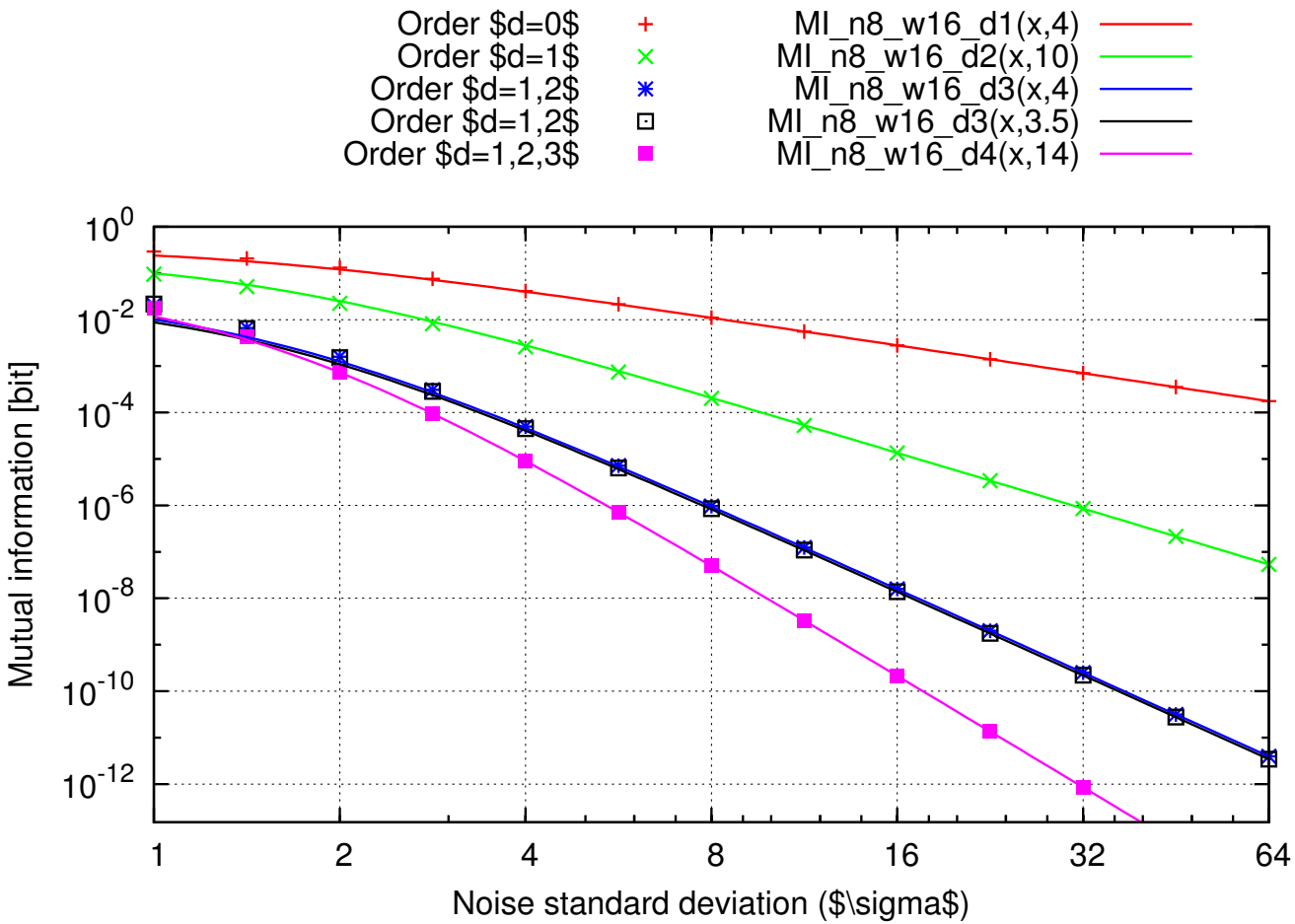
$$= \frac{1}{\ln 2}\sum_{d=0}^{+\infty}\frac{1}{2\,d!}\frac{\mathrm{Var}[\mathbb{E}[k_d(\mathscr{L}\mid Z)]]}{\left(\mathrm{Var}[\mathscr{L}]+\sigma^2\right)^d}\quad , \tag{4}$$

$$= \frac{d_C^{\perp}!B_{d_C^{\perp}}^{\perp}}{2\ln 2\cdot 2^{2d_C^{\perp}}}\times\frac{1}{\sigma^{2d_C^{\perp}}}+\mathcal{O}\left(\frac{1}{\sigma^{2(d_C^{\perp}+1)}}\right)\quad \text{when } \sigma\to\infty\ . \tag{5}$$

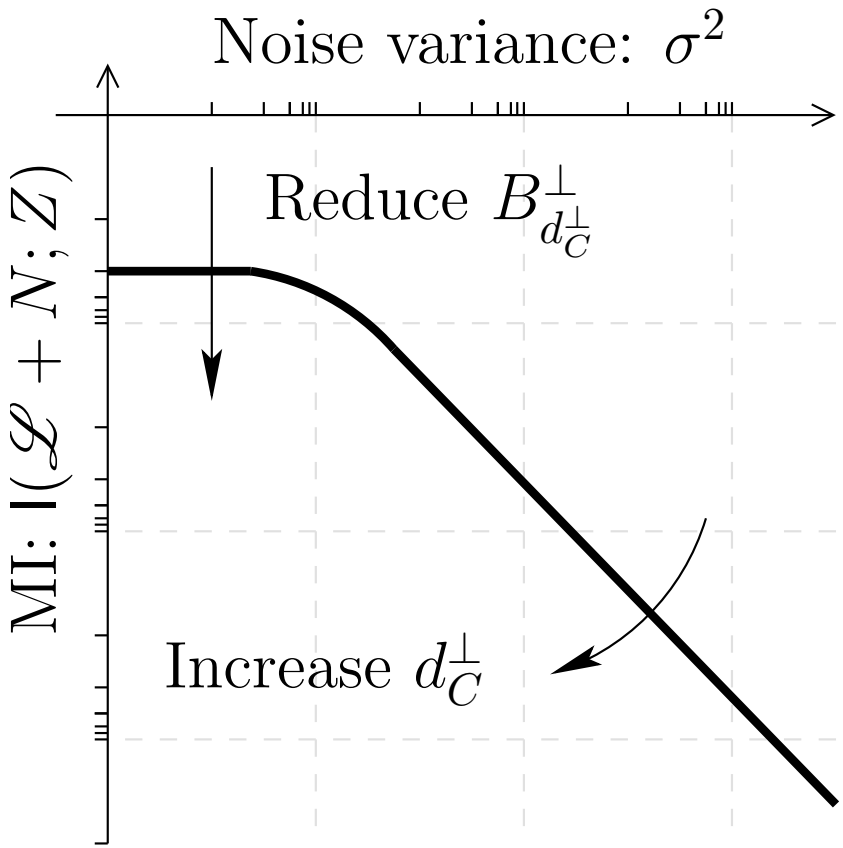
where k_d are order d cumulants [LB10].

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

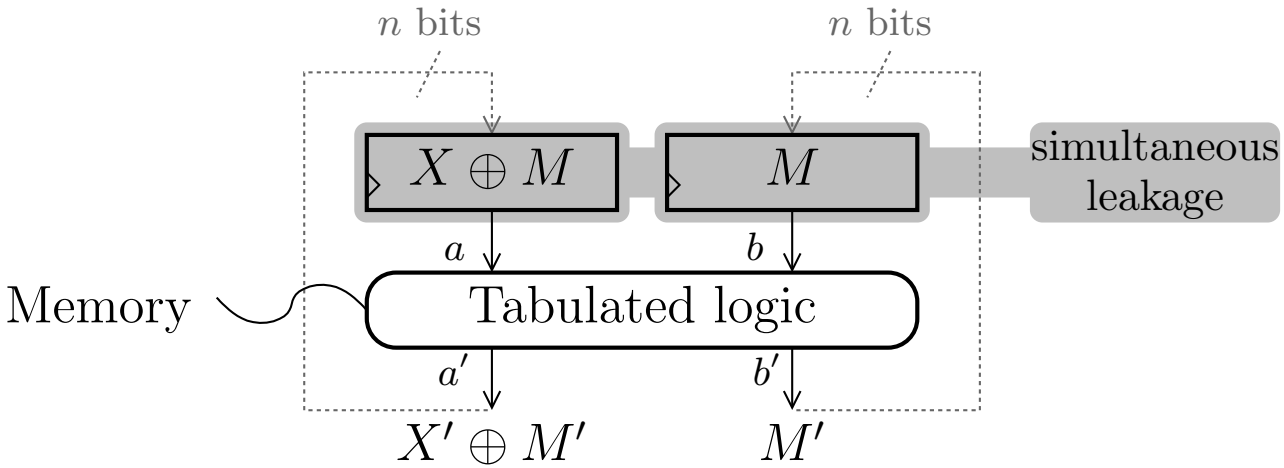
Code #	$B^{\perp}_0$	$B^{\perp}_1$	$B^{\perp}_2$	$B^{\perp}_3$	$B^{\perp}_4$	$B^{\perp}_5$	$B^{\perp}_6$	$B^{\perp}_7$	$B^{\perp}_8$
1	1	**8**	28	56	70	56	28	8	1
2	1	0	**28**	0	70	0	28	0	1
3	1	0	0	**3.5**	7	3.5	0	0	1
4	1	0	0	**4**	5	4	2	0	0
5	1	0	0	0	**14**	0	0	0	1



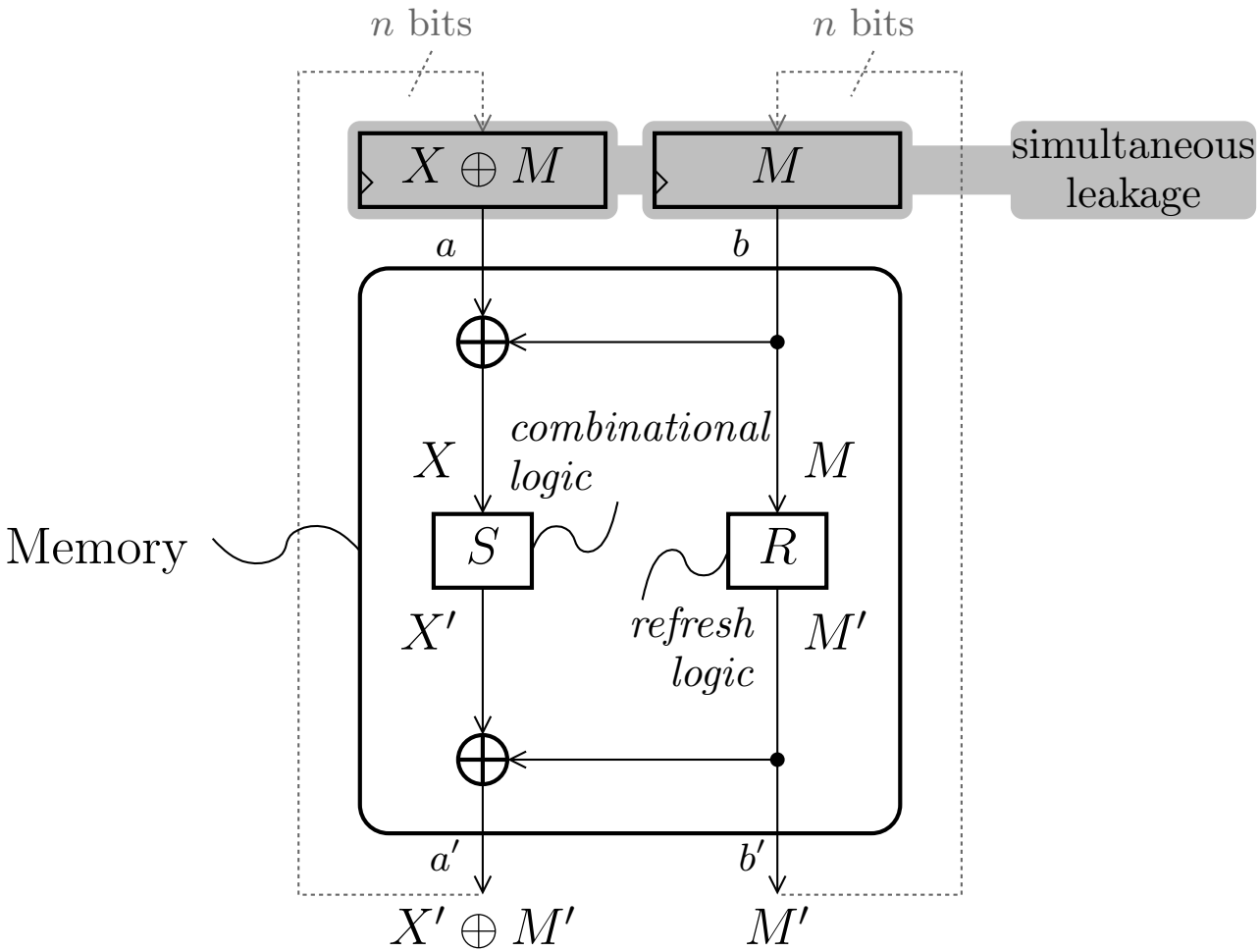
Approximation of $\mathrm{I}[\mathscr{L} + N; Z]$ by $\left(d_C^{\perp} ! B_{d_C^{\perp}}^{\perp}\right) \Big/ \left(2 \ln 2 \cdot 2^{2d_C^{\perp}} \sigma^{2d_C^{\perp}}\right)$.



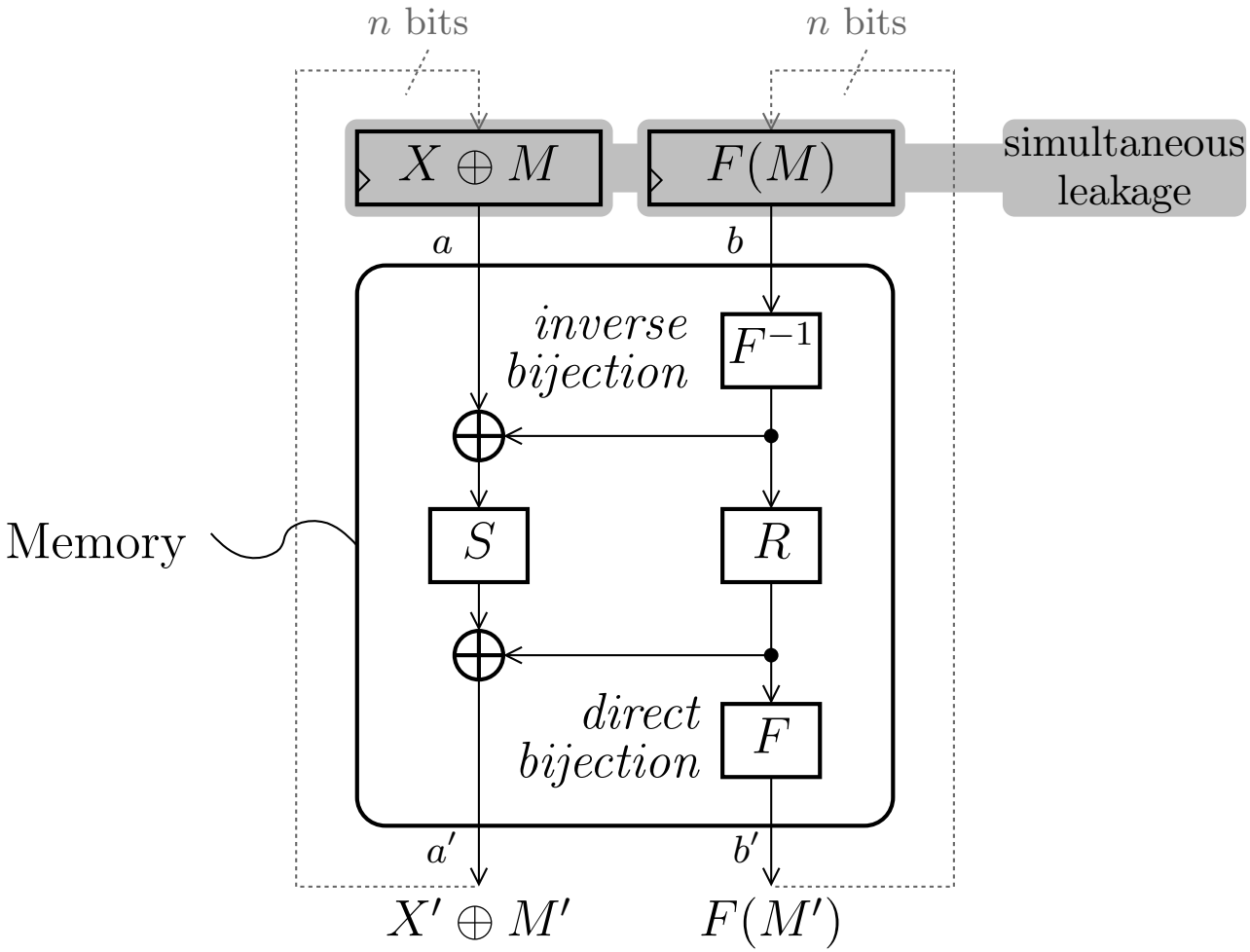
Two concomitant objectives to reduce the mutual information.



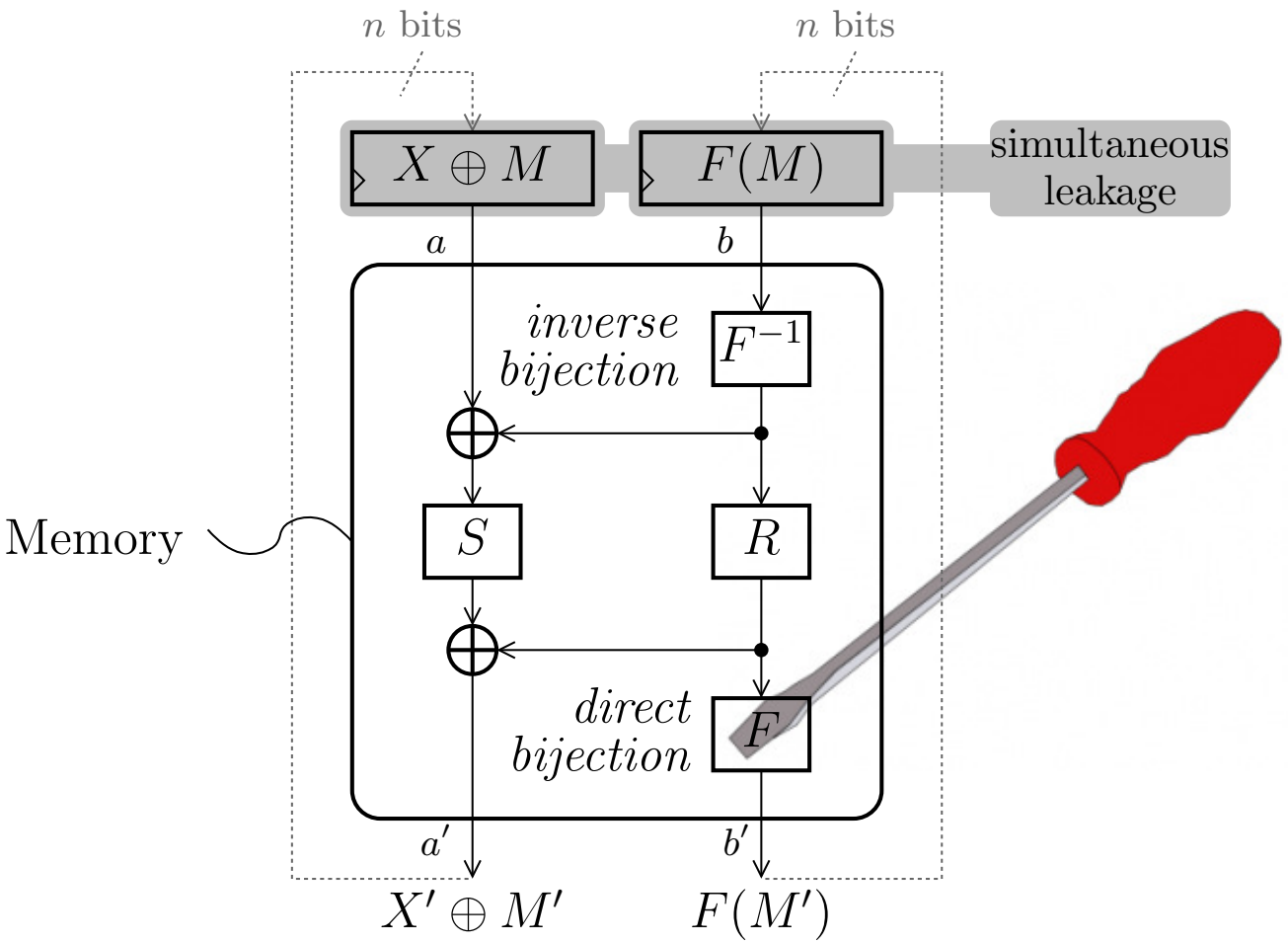
Principle of masking without throughput loss.



Detail of the computation.



Principle of leakage squeezing, within throughput loss.


n bits
n bits
$X \oplus M$
$F(M)$
simultaneous leakage
a
b
inverse bijection
F^{-1}
Memory
S
R
direct bijection
F
a'
b'
$X' \oplus M'$
$F(M')$

Objective

Maximize d such as $\mathrm{Var}[\mathbb{E}[(\mathrm{HW}(X \oplus M, F(M)))^d \mid X]] = 0$.

Solution

Resistance order d: $1 \leq d \leq n-1$, where $d+1$ is the maximal dual distance of codes $(2n, 2^n, \delta)$ with complementary information sets.

The code is the support of the indicator of the graph of F.

Examples

- Optimal code: NR $(16, 2^8, 6)$ for $n = 8$. See [CGKS12] $(\forall n)$
- High-order CIS codes [CDGM12, CFG$^+$].

Presentation Outline

Theorem (rank-nullity)

$\dim(\mathcal{C}) + \dim(\mathcal{C}^\perp) = \dim(\mathbb{F}_2^n) = n$, *where* $\dim(\cdot)$ *is the dimension of the vector space.*

As a direct consequence of Theorem 6, we have $\dim(\mathcal{C}^\perp) = n - k$.

Remark

However, $\mathcal{C}$ *and* $\mathcal{C}^\perp$ *are not necessarily supplementary, i.e., we do not have* $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$*. For instance, if* $\mathcal{C}$ *is autodual, then* $\mathcal{C} = \mathcal{C}^\perp$*.*

Indeed, unlike in Euclidean spaces, the scalar product does not define a norm.

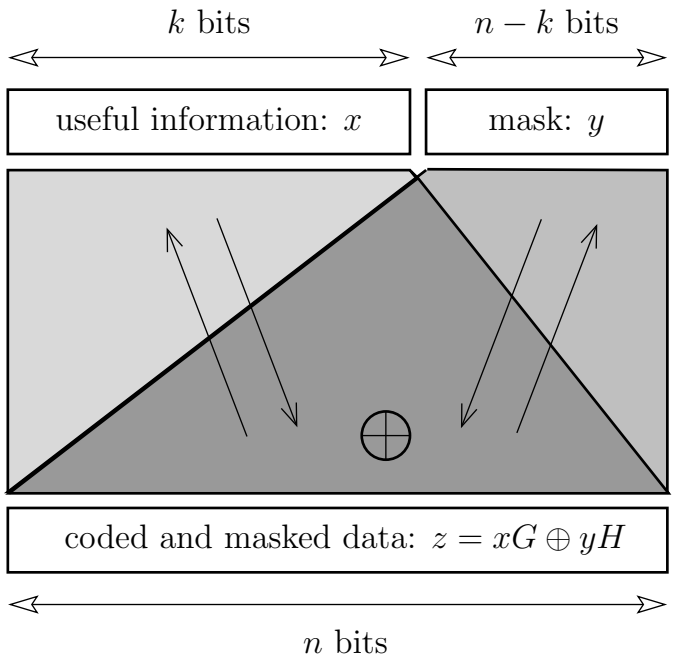
Proposition (Condition for $\mathbb{F}_2^n = \mathcal{C} \oplus \mathcal{C}^\perp$)

Without loss of generality (a permutation of coordinates might be necessary), we can assume that the generating matrix of $\mathcal{C}$ is systematic, and thus takes the form $[I_k \| M]$, where I_k is the $k \times k$ identity matrix. The supplementary $\mathcal{D}$ of $\mathcal{C}$ is equal to $\mathcal{C}^\perp$ if and only if (iff) the matrix $I_k \oplus MM^\mathsf{T}$ is invertible.

When $\mathcal{D} = \mathcal{C}^{\perp}$, there is an orthogonal projection. Indeed, we thus have $GH^{\mathsf{T}} = 0$ (the all-zero $k \times (n-k)$ matrix). In this case, H is the *parity matrix* of code $\mathcal{C}$. So, in Eq. (2), x and y can be recovered from z, as follows:

$$x = zG^{\mathsf{T}}(GG^{\mathsf{T}})^{-1} \ , \tag{6}$$

$$y = zH^{\mathsf{T}}(HH^{\mathsf{T}})^{-1} \ . \tag{7}$$



Computing in ODSM

$$L' = G^{\mathsf{T}} \left(G \cdot G^{\mathsf{T}} \right)^{-1} LG \oplus H^{\mathsf{T}} \left(H \cdot H^{\mathsf{T}} \right)^{-1} H \ . \tag{8}$$

$$\forall z \in \mathbb{F}_2^n, \quad S'(z) = S(zG^{\mathsf{T}}(GG^{\mathsf{T}})^{-1})G \oplus zH^{\mathsf{T}}(HH^{\mathsf{T}})^{-1}H \ , \tag{9}$$

SCA resistance

ODSM can be attacked by monovariate high-order SCA only at order $j \geq d_{\mathcal{C}}$.

DFA resistance

$$P_{\mathcal{D}}(z) \stackrel{?}{=} yH \ . \tag{10}$$

We consider a perturbation as the addition to the state z of a random error ε ($z \leftarrow z \oplus \varepsilon$). Like z (recall $z = xG \oplus yH$, see Eq. (2)), the fault can be uniquely written as:

$$\varepsilon = eG \oplus fH \ , \text{ where } e \in \mathbb{F}_2^k \text{ and } f \in \mathbb{F}_2^{n-k} \ . \tag{11}$$

The fault is undetected if
$P_{\mathcal{D}}(z \oplus \varepsilon) = (y \oplus f)H = yH \Leftrightarrow f = 0 \Leftrightarrow \varepsilon \in \mathcal{C}$ (**difficult!**)

Notations

- x is encoded: $\Psi(x) = xG \in \mathbb{F}_2^n$
- $\Psi(x)$ is manipulated masked by some $d \in \mathcal{D}$
- Indicator $1_{\mathcal{D}}$ of $\mathcal{D}$ is noted $f : \mathbb{F}_2^n \to \mathbb{F}_2$:

$$\forall d \in \mathbb{F}_2^n, \quad f(d) = 1 \iff d \in \mathcal{D} \ .$$

Said differently, $f(d) = 1 \iff \exists y \in \mathbb{F}_2^{n-k}$ s.t. $yH = d$.

Statistics

- Random variables: D
- Realizations: d
- Support: $\mathcal{D}$

Leakage model / attacker model

- We model the attacker as a pseudo-Boolean function $\Phi : \mathbb{F}_2^n \to \mathbb{R}$ of a given numerical degree j in the bits of Z.
- For example, Φ can be the power j of the Hamming weight (as in zero-offset attacks).
- The leakage model can be, in general, any affine function of the bits of Z. This simply means that there is no "glitch" nor "cross-couping". This case is usual for software platforms, and in hardware when using memories.

Proposition (jth-order security condition on the masks coding)

Let $\Phi : \mathbb{F}_2^n \to \mathbb{R}$ a leakage function of numerical degree j, an arbitrary $\Psi : \mathbb{F}_2^k \to \mathbb{F}_2^n$ and a mask D uniformly distributed in a code $\mathcal{D}$, with f the indicator of $\mathcal{D} \subset \mathbb{F}_2^n$. Then the leakage $\Phi(\Psi(X) \oplus D)$ resists a monovariate attack if $\mathcal{D}$ is a code of dual distance $j+1$.

In Proposition 4, the condition of jth-order security is: for all Φ of numerical degree smaller than or equal to j, $\mathbb{E}[\Phi(\Psi(X) \oplus D)|X = x]$ does not depend on $x \in \mathbb{F}_2^k$. This is rewritten as the condition:

$$\mathrm{Var}[\mathbb{E}[\Phi(\Psi(X) \oplus D)|X]] = 0 \ . \tag{12}$$

Indeed, in this case, any correlation attack fails: indeed, there is no linear dependency between the leakage $\Phi(\Psi(X) \oplus D)$ and the sensitive variable X.

Now, the expectation $\mathbb{E}[\Phi(\Psi(X) \oplus D)|X = x]$ is taken on the mask D random variable only, because $\Psi(X)$ depends only on X. So we have:

$$\begin{aligned}\mathbb{E}[\Phi(\Psi(X) \oplus D)|X = x] &= \sum_{d \in \mathcal{D}} \frac{1}{\mathrm{Card}[\mathcal{D}]} \Phi(\Psi(x) \oplus d) \\ &= 2^{-(n-k)} \sum_{d \in \mathbb{F}_2^n} f(d)\Phi(\Psi(x) \oplus d) \\ &= 2^{-(n-k)} \left(f \otimes \Phi\right)\left(\Psi(x)\right) \ .\end{aligned}$$

So, the countermeasure is jth-order secure if and only if $\left(f \otimes \Phi\right)\left(\Psi(x)\right)$ does not depend on x. Therefore, a sufficient condition for resistance against jth-order attacks is that $f \otimes \Phi(z)$ does not depend on $z \in \mathbb{F}_2^n$ (irrespective of function Ψ).

Let g a pseudo-Boolean function $\mathbb{F}_2^n \to \mathbb{R}$. We call $\hat{g}$ the Fourier transform of g, i.e., $\hat{g}(z) = \sum_a g(a)(-1)^{a \cdot z}$. We have:
(g is constant) $\iff \forall z \neq 0,\ \hat{g}(z) = 0 \iff \hat{g} \propto \delta$, the Kronecker symbol.
Let us apply this result to $g = f \otimes \Phi$. The Fourier transform turns a *convolution product* into a *product*, i.e., $\widehat{f \otimes \Phi}(z) = \hat{f}(z)\hat{\Phi}(z)$. To prove that:

$$\hat{f}\,\hat{\Phi} = 0 \ , \tag{13}$$

Lemma

Lemma

Let P be a pseudo-Boolean function $P : \mathbb{F}_2^n \to \mathbb{R}$ of numerical degree $d^\circ(P)$ [Car10, CG99]. Then, $\forall z \in \mathbb{F}_2^n$,
$\mathrm{HW}(z) > d^\circ(P) \Longrightarrow \widehat{P}(z) = 0.$

Proof.

(Proof of Proposition 4) So, to prove that $\widehat{f}\,\widehat{\Phi} = 0$, we start by applying Lemma 7. As Φ is of numerical degree j, $\widehat{\Phi}(z) = 0$ for $\mathrm{HW}(z) > j$. So, the masking is jth-order secure if $\forall z \in \mathbb{F}_2^n$, $0 < \mathrm{HW}(z) \leq j$, $\widehat{f}(z) = 0$. By definition, this means that f is jth-order correlation-immune (j-CI in brief). This is equivalent to saying the $\mathcal{D}$ is of dual distance $d_{\mathcal{D}}^{\perp} = j + 1$.
Irrespective of the way the sensitive variable $X \in \mathbb{F}_2^k$ is mapped (by function Ψ) onto $\mathbb{F}_2^n$, a sufficient condition for security against zero-offset attacks [WW04] of orders $1, 2, \cdots, j$ is that the mask D be distributed uniformly in $\mathcal{D}$, a code of dual distance $j + 1$. Said differently, the lowest order j of a successful zero-offset attack is equal to the dual distance of $\mathcal{D}$.
As $\mathcal{D} = \mathcal{C}^{\perp}$, we have that $d_{\mathcal{D}}^{\perp} = d_{\mathcal{C}}$ (see Proposition 1). □

$$G = \left(\begin{array}{cccccccc|cccccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1
\end{array}\right),$$

$$H = \left(\begin{array}{cccccccc|cccccccc}
1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right).$$

$$G^{\mathsf{T}}(GG^{\mathsf{T}})^{-1} =$$

$$\begin{pmatrix}
0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 0
\end{pmatrix}$$

$$H^{\mathsf{T}}(HH^{\mathsf{T}})^{-1} =$$

$$\begin{pmatrix}
0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 1
\end{pmatrix}$$

xtime: multiplication by X in $\mathbb{F}_2^8$

Generated from this $k \times k$ (i.e., 8×8) matrix L:

$$L = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

$$L' = \left(\begin{array}{cccccccc|cccccccc}
1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
\hline
1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0
\end{array}\right).$$

Conclusions

- Codes can help increase the security level:
  - Against side-channel attacks, and
  - Against fault injection attacks
- Protection against multivariate attacks: is a perspective

Thank you!

- $x \in \mathbb{F}_2^k$ the clear data,
- $y = (y_1, y_2, \ldots, y_d) \in (\mathbb{F}_2^k)^d$ are the masks, and the protected data is:
- $z = (x + \sum_{i=1}^{d} y_i, y_2, \ldots, y_d)$.

So we have $n = tk$ $(t = d + 1)$, and $z = xG + yH$, where

$$G = \begin{pmatrix} I & 0 & 0 & \cdots & 0 \end{pmatrix},$$

$$H = \begin{pmatrix} I & I & 0 & \cdots & 0 \\ I & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I & 0 & 0 & \cdots & I \end{pmatrix}.$$

Notice that $GH^{\mathsf{T}} \neq 0$, thus the codes generated by G and H are not supplementary dual.

Security equivalence

We have proved with OSDM that the representation $z = xG + yH$ protects against attacks of order d if $d_D^\perp$ is of dual distance at least t, where D is the linear code of generator matrix H. Notice that $d_D^\perp \neq d_C$ since $D \neq C^\perp$ (unlike ODSM).

Remark

The dual distance of the linear code of generator matrix H is t. Indeed, the dual code of the code generated by H is generated by:

$$H^\perp = \begin{pmatrix} I & I & I & \cdots & I \end{pmatrix}, \tag{14}$$

which has minimal distance t (it is the t-wise repetition code).

Remark

This code is not optimal, unless $k = 1$.

Inverse coding

- We have $z = \begin{pmatrix} x & y \end{pmatrix} M$, where the matrix M is equal to $M = \begin{pmatrix} G \\ H \end{pmatrix}$.
- Therefore, $\begin{pmatrix} x & y \end{pmatrix} = zM^{-1}$, where $M^{-1} = M$ (the coding is *involutive*).

$$M^{-1} = \left(\begin{array}{c|cccc} I & 0 & 0 & \cdots & 0 \\ I & I & 0 & \cdots & 0 \\ I & 0 & I & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ I & 0 & 0 & \cdots & I \end{array}\right) = \begin{pmatrix} J & K \end{pmatrix}$$

$$\Longrightarrow \; x = Jz, y = Kz$$

Unification for the refresh

In all the schemes, the mask refresh is: $y' \in_{\mathcal{R}} \mathbb{F}_2^{n-k}$, $z \leftarrow z + y'H$.

C14

Remark (Steps of C14 for $d = 1$)

1. $\forall u \in \mathbb{F}_2^k,\ T(u) = S(u)G,$
2. $\forall u \in \mathbb{F}_2^k,\ T(u) = S(u + x_1)G + y_1 H,$
3. $\forall u \in \mathbb{F}_2^k,\ T(u) = S(u + x_1 + x_2)G + (y_1 + y_2)H,$
4. *return* $T(0)$

Somehow, if we collapse the iterations, C14 consists in computing: $S(zJ)G + (y_1 + y_2)KH$.

Countermeasures against Physical Attacks using Error-Correcting Codes

Sylvain GUILLEY[1,2]

[1]Institut MINES-TELECOM, TELECOM-ParisTech
[2]Secure-IC S.A.S.

MCrypt, August 13, 2014 – Les Deux Alpes

[BDGN13] Shivam Bhasin, Jean-Luc Danger, Sylvain Guilley, and Zakaria Najm.

A Low-Entropy First-Degree Secure Provable Masking Scheme for Resource-Constrained Devices.

In *Proceedings of the Workshop on Embedded Systems Security*, WESS '13, pages 7:1–7:10, New York, NY, USA, September 29 2013. ACM.

Montreal, Quebec, Canada. DOI: 10.1145/2527317.2527324.

[Car10] Claude Carlet.

Boolean Functions for Cryptography and Error Correcting Codes: Chapter of the monography Boolean Models and Methods in Mathematics, Computer Science, and Engineering.

pages 257–397. Cambridge University Press, Y. Crama and P. Hammer eds, 2010.

Preliminary version available at http://www.math.univ-paris13.fr/~carlet/chap-fcts-Bool-corr.pdf.

[CDG+14] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, Houssem Maghrebi, and Emmanuel Prouff.

Achieving side-channel high-order correlation immunity with Leakage Squeezing.

Journal of Cryptographic Engineering, pages 1–15, 2014.

DOI: 10.1007/s13389-013-0067-1.

[CDGM12] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Maghrebi.

Leakage Squeezing of Order Two.

In *INDOCRYPT*, volume 7668 of *LNCS*, pages 120–139. Springer, December 9-12 2012.

Kolkata, India.

[CFG+] Claude Carlet, Finley Freibert, Sylvain Guilley, Michael Kiermaier, Jon-Lark Kim, and Patrick Solé.

Higher-order CIS codes.

To appear in IEEE TIT.

[CG99] Claude Carlet and Philippe Guillot.
A New Representation of Boolean Functions.
In Marc P. C. Fossorier, Hideki Imai, Shu Lin, and Alain Poli, editors, *AAECC*, volume 1719 of *Lecture Notes in Computer Science*, pages 94–103. Springer, 1999.

[CG13] Claude Carlet and Sylvain Guilley.
Side-Channel Indistinguishability.
In *HASP*, pages 9:1–9:8, New York, NY, USA, June 23-24 2013. ACM.

[CG14a] Claude Carlet and Sylvain Guilley.
Construction of Supplementary Dual Codes.
In *ICMCTA, 4th International Castle Meeting on Coding Theory and Applications*, September 15-18 2014.
Palmela, Portugal.

[CG14b] Claude Carlet and Sylvain Guilley.
Side-Channel Indistinguishability, July 19 2014.
On HAL: http://hal.archives-ouvertes.fr/hal-00826618.
Extended version of [CG13] with more results in appendix.

[CGKS12] Claude Carlet, Philippe Gaborit, Jon-Lark Kim, and Patrick Solé.
A New Class of Codes for Boolean Masking of Cryptographic Computations.
IEEE Transactions on Information Theory, 58(9):6000–6011, 2012.

[Cor13] Jean-Sébastien Coron.
Higher Order Masking of Look-up Tables.
Cryptology ePrint Archive, Report 2013/700, 2013.
http://eprint.iacr.org/.

[LB10] Thanh-Ha Le and Maël Berthier.

Mutual Information Analysis under the View of Higher-Order Statistics.

In Isao Echizen, Noboru Kunihiro, and Ryôichi Sasaki, editors, *IWSEC*, volume 6434 of *Lecture Notes in Computer Science*, pages 285–300. Springer, 2010.

[MCGD12] 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.

[MGD11] Houssem Maghrebi, Sylvain Guilley, and Jean-Luc Danger.

Leakage Squeezing Countermeasure Against High-Order Attacks.

In *WISTP*, volume 6633 of *LNCS*, pages 208–223. Springer, June 1-3 2011.

Heraklion, Greece. DOI: 10.1007/978-3-642-21040-214.

[MS77] F. Jessie MacWilliams and Neil J. A. Sloane.
The Theory of Error-Correcting Codes.
Elsevier, Amsterdam, North Holland, 1977.
ISBN: 978-0-444-85193-2.

[RP10] Matthieu Rivain and Emmanuel Prouff.
Provably Secure Higher-Order Masking of AES.
In Stefan Mangard and François-Xavier Standaert, editors, *CHES*, volume 6225 of *LNCS*, pages 413–427. Springer, 2010.

[WW04] Jason Waddle and David Wagner.
Towards Efficient Second-Order Power Analysis.
In *CHES*, volume 3156 of *LNCS*, pages 1–15. Springer, 2004.
Cambridge, MA, USA.