Information Leakages in Code-based Masking: A Unified Quantification Approach

Wei Cheng, Sylvain Guilley, Claude Carlet,

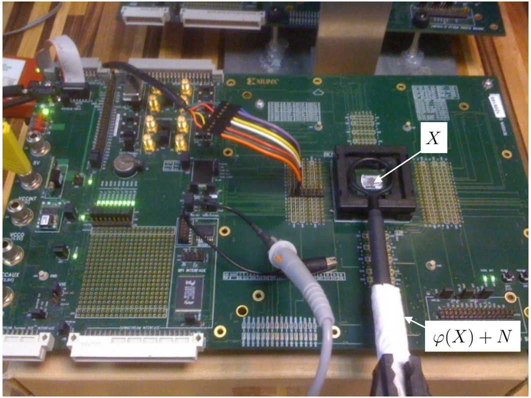
Sihem Mesnager and Jean-Luc Danger

wei.cheng@telecom-paris.fr

Sep 13, 2021 @ TCHES 2021

Outline

Side-channel analysis on observable leakages



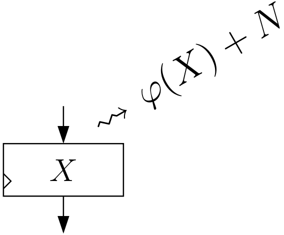


Figure 1: Observable leakages from the manipulation of X [CG18].

Masking as a countermeasure against SCA

Masking

- **Security**: provably secure against SCA [ISW03, PR13]
- **Costs**: quadratically or cubically in higher-order glitch-free case [GSF13]
- **Others**: device independent

Boolean masking [CJRR99]

Let $\mathbb{K} = \mathbb{F}_{2^\ell}$ be a finite field, e.g., $\mathbb{K} = \mathbb{F}_{2^8} \cong \mathbb{F}_2[\alpha]/\langle \alpha^8 + \alpha^4 + \alpha^3 + \alpha + 1 \rangle$, then

- $X \in \mathbb{K}$: the sensitive variable
- $Y \in \mathbb{K}^{n-1}$: the random masks
- $Z \in \mathbb{K}^n$: the masked variable

For Boolean masking with n shares:

$$Z = (Z_1, \ldots, Z_n) = \left(X + \sum_{i=1}^{n-1} Y_i, Y_1, Y_2, \ldots, Y_{n-1} \right).$$

Code-based masking

GCM: a uniform representation

In a generalized code-based masking [WMCS20, CGC+21a], the encoding is:

$$Z = X\mathbf{G} + Y\mathbf{H}$$

where

- $X \in \mathbb{K}^k$: the sensitive variables
- $Y \in \mathbb{K}^t$: the random masks
- $Z \in \mathbb{K}^n$: the masked variable
- $\mathbf{G} \in \mathbb{K}^{k \times n}$ and $\mathbf{H} \in \mathbb{K}^{t \times n}$: generator matrices of $\mathcal{C}$ and $\mathcal{D}$, resp.

Constraints & conditions

- Condition for decoding: $\mathcal{C} \cap \mathcal{D} = \{0\}$
- Without redundancy: $n = k + t$; with redundancy: $n > k + t$.

Code-based masking

Two examples

Boolean masking

$$Z = (Z_1, \ldots, Z_n) = \left(X + \sum_{i=1}^{n-1} Y_i,\ Y_1, Y_2, \ldots, Y_{n-1} \right) = X\mathbf{G} + Y\mathbf{H}, \quad (1)$$

where $\mathbf{G}$ and $\mathbf{H}$ are:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \end{pmatrix} \in \mathbb{K}^{1\times n}$$

$$\mathbf{H} = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathbb{K}^{t\times n}.$$

Inner Product masking [BFG15]

$$Z = (Z_1, \ldots, Z_n) = \left(X + \sum_{i=1}^{n-1} \alpha_i Y_i,\ Y_1, Y_2, \ldots, Y_{n-1} \right) = X\mathbf{G} + Y\mathbf{H}, \quad (2)$$

where $\mathbf{G}$ and $\mathbf{H}$ are:

$$\mathbf{G} = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \end{pmatrix} \in \mathbb{K}^{1\times n}$$

$$\mathbf{H} = \begin{pmatrix} \alpha_1 & 1 & 0 & \cdots & 0 \\ \alpha_2 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_t & 0 & 0 & \cdots & 1 \end{pmatrix} \in \mathbb{K}^{t\times n}.$$

Code-based masking: a brief history

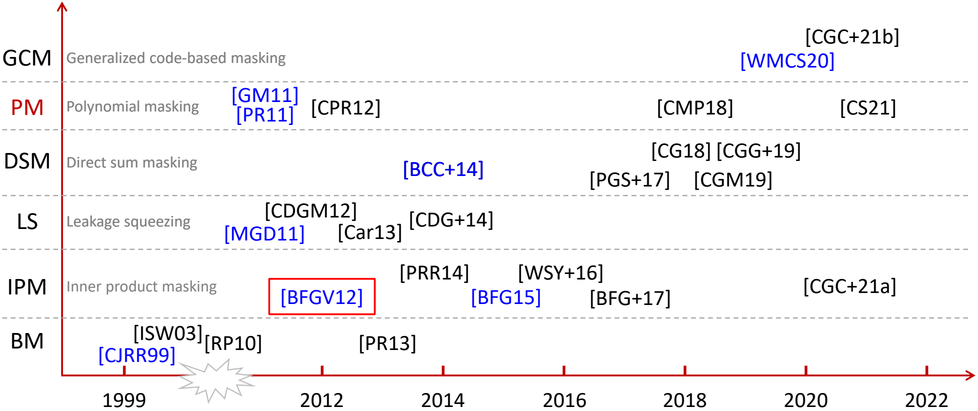


Figure 2: A brief history of masking schemes.

- Marked in BLUE are the first proposals of the corresponding schemes
- For IPM, we consider the improved IPM [BFG15] rather than the original one [BFGV12].

Code-based masking: overview

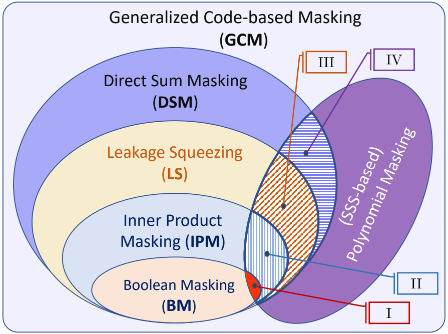


Figure 3: Overview of code-based masking schemes.

- The core Russian dolls: BM ⊆ IPM ⊆ LS ⊆ DSM support masking only, since $n = t + 1$
- Whilst SSS-based masking and GCM also allow for error detection/correction when $n > t + 1$

Two problems

- **How to measure information leakage in different schemes?**
- **For each scheme, how to choose optimal codes?**

Dual codes and transformations

Definition (Dual Code).

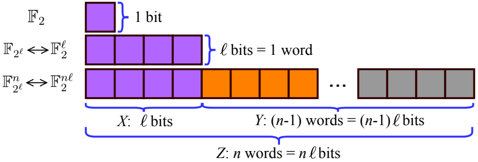
The dual code of $\mathcal{D}$, denoted as $\mathcal{D}^{\perp}$, is: $\mathcal{D}^{\perp} = \{v \mid \forall u \in \mathcal{D},\ \langle v, u \rangle = 0\}$.

Sub-field representation [MS77]

Let $x \in \mathbb{F}_{2^\ell}$, the sub-field representation of x is $[x]_2 \in \mathbb{F}_2^\ell$.

Code Expansion [MS77]

Consider a generator matrix of a linear code of size $k \times n$ in $\mathbb{F}_{2^\ell}$, the generator matrix of the expanded code has a size of $k\ell \times n\ell$ in $\mathbb{F}_2$.



The kissing number of a code

Definition (Weight Enumerator [MS77]).

For a linear code $\mathcal{D}$ of parameters $[n, k, d]$, its weight enumerator is defined as:

$$W_{\mathcal{D}}(\mathsf{X}, \mathsf{Y}) = \sum_{i=0}^{n} B_i \mathsf{X}^{n-i} \mathsf{Y}^i,$$

where $B_i = |\{u \in \mathcal{D} | w_H(u) = i\}|$ and w_H is the Hamming weight function.

In particular, B_d is called the kissing number of $\mathcal{D}$.

Example.

For the linear code [8,4,4], we have $W_{\mathcal{D}}(\mathsf{X}, \mathsf{Y}) = \mathsf{X}^8 + 14\mathsf{X}^4\mathsf{Y}^4 + \mathsf{Y}^8$, thus: $B_0 = 1,\ B_4 = 14,\ B_8 = 1$.

Definition (Adjusted kissing number [CGC+21a]).

Let $\mathcal{C}$ and $\mathcal{D}$ denote two linear codes, the adjusted kissing number B'_d is defined as:

$$B'_d = \left|\{(x, y) \in (\mathcal{D} \backslash \mathcal{C})^2 \,|\, x + y \in \mathcal{C},\ w_H(x) = w_H(y) = d\}\right|. \quad (3)$$

Outline

Security models

Two probing models

The two kinds of probing model (see also [DGH+18, PGS+17]) are:

- **Bit-probing model**: each probe only gets one bit at a time where each bit leaks independently or jointly. The security order under the bit-probing model is denoted by t_b.
- **Word-probing model**: each probe gets an ℓ-bit word at a time, where an ℓ-bit variable leaks as a whole. Similarly, the security order is then denoted by t_w.

Leakage functions and numerical degree

Leakage functions

Leakage functions, turning a bitvector into a real value, are pseudo-Boolean functions $P : \mathbb{K}^{n\ell} \mapsto \mathbb{R}$, where $\mathbb{K} = \mathbb{F}_2$.

$$P(Z) = \sum_{I \in \{0,1\}^{n\ell}} \beta_I Z^I, \tag{4}$$

where $Z^I = \prod_{i \in I} Z_i$, and $\beta_I \in \mathbb{R}$.

Definition (Numerical Degree [CG99]).

The numerical degree of a pseudo-Boolean function P denoted by $\deg(P)$ equals: $\deg(P) := d = \max\{|I| \,|\beta_I \neq 0\}$.

Example.

- $Z^{(100\cdots0)_2}$ *for MSB, and* $Z^{(000\cdots1)_2}$ *for LSB, with* $\deg(P) = 1$
- $w_H(Z) = Z^{(100\cdots0)_2} + Z^{(010\cdots0)_2} + \cdots + Z^{(000\cdots1)_2}$ *for the Hamming weight, with* $\deg(P) = 1$
- $Z^{(110\cdots0)_2} = Z_1 Z_2$ *with* $\deg(P) = 2$.

Concrete security level of CBM

SNR as a leakage metric

Let

$$\mathcal{L} = P(Z) + N$$

denote the leakages where $N \sim \mathcal{N}(0, \sigma^2)$ denotes the independent Gaussian noise.

How to exploit the leakage in SCA?

The distinguishing rule in SCA:

$$\mathbb{E}\left[\mathcal{L}|X\right] \stackrel{?}{=} \mathbb{E}\left[\mathcal{L}\right] \qquad \longrightarrow \qquad \text{Var}\left[\mathbb{E}\left[\mathcal{L}|X\right]\right] \stackrel{?}{=} 0$$

Concrete security level of CBM

SNR as a leakage metric

Let

$$\mathcal{L} = P(Z) + N$$

denote the leakages where $N \sim \mathcal{N}(0, \sigma^2)$ denotes the independent Gaussian noise.

How to exploit the leakage in SCA?

The distinguishing rule in SCA:

$$\mathbb{E}[\mathcal{L}|X] \stackrel{?}{=} \mathbb{E}[\mathcal{L}] \qquad \longrightarrow \qquad \text{Var}[\mathbb{E}[\mathcal{L}|X]] \stackrel{?}{=} 0$$

We have

$$\text{Var}[\mathbb{E}[P(Z) + N|X]] = \text{Var}[\mathbb{E}[P(Z)|X]],$$

where $Z = X\mathbf{G} + Y\mathbf{H} \in \mathbb{K}^n \in \mathbb{F}_{2^\ell}^n$. The SNR of leakages is defined as:

$$\text{SNR} = \frac{\text{Var}[\mathbb{E}[\mathcal{L}|X]]}{\text{Var}[N]} = \frac{\text{Var}[\mathbb{E}[P(Z)|X]]}{\sigma_{total}^2}, \qquad (5)$$

where $\text{Var}[N] = \sigma_{total}^2 \propto \sigma^{2d}$ [CGC+21b].

Quantifying leakage of CBM by SNR

Taking $P(z) = w_H(z)^d$ as higher-order moments of leakages, then

$$P(z) = \sum_{J_1+\cdots+J_{n\ell}=d} \binom{d}{J_1,\ldots,J_{n\ell}} \prod_{i=1}^{n\ell} z_i^{J_i} = \sum_{\substack{J\in\mathbb{N}^{n\ell},\text{ s.t. } w_H(J)<d;\\ \sum_{i=1}^{n\ell} J_i=d}} \binom{d}{J} z^J + d! \sum_{\substack{I\in\{0,1\}^{n\ell};\\ w_H(I)=d}} z^I \qquad (6)$$

where $\mathbb{N} = \{0, 1, 2, \ldots\}$. The multinomial coefficient $\binom{d}{J_1,\ldots,J_{n\ell}}$ is defined as $\frac{d!}{J_1!\cdots J_{n\ell}!}$.

Theorem (SNR for Hamming Weight Leakage [CGC+21a]).

Let a device be protected by the GCM scheme as $Z = X\mathbf{G} + Y\mathbf{H}$. Assume the device is leaking in Hamming weight model in the form: $\mathcal{L} = P(Z) + N$. Then the SNR of the exploitable leakages is:

$$\mathit{SNR} = \frac{\mathrm{Var}\left[\mathbb{E}\left[P(Z)|X\right]\right]}{\sigma^2_{total}} = \frac{B'_{d^\perp_{\mathcal{D}}}}{\sigma^2_{total}} \left(\frac{d^\perp_{\mathcal{D}}!}{2^{d^\perp_{\mathcal{D}}}}\right)^2, \qquad (7)$$

where σ^2_{total} is the total noise such that $\sigma^2_{total} \propto \sigma^{2d}$.

Concrete security level of CBM

In an information-theoretic sense

MI between $\mathcal{L}$ and X is defined as $\mathsf{I}(\mathcal{L}; X) = \mathsf{H}(\mathcal{L}) - \mathsf{H}(\mathcal{L}|X)$ where:

- the total entropy is: $\mathsf{H}(\mathcal{L}) = -\int_l \mathbb{P}[l] \log_2 \mathbb{P}[l] \, \mathrm{d}l$,
- the conditional entropy $\mathsf{H}(\mathcal{L}|X)$ is: $\mathsf{H}(\mathcal{L}|X) = -\sum_{x \in \mathbb{F}_2^\ell} \mathbb{P}[x] \int_l \mathbb{P}[l|x] \log_2 \mathbb{P}[l|x] \, \mathrm{d}l$.

Theorem (MI for Hamming Weight Leakage [CGC+21a]).

Let a device be protected by the GCM scheme as $Z = X\mathbf{G} + Y\mathbf{H}$. Assume the leakages of the device can be represented in the form: $\mathcal{L} = P(Z) + N$. Then the MI between $\mathcal{L}$ and X is:

$$\mathsf{I}(\mathcal{L}; X) = \begin{cases} 0\,, & \text{if } \deg(P) < d_{\mathcal{D}}^{\perp} \\ \frac{d_{\mathcal{D}}^{\perp}! B'_{d_{\mathcal{D}}^{\perp}}}{2 \ln 2 \cdot 2^{2d_{\mathcal{D}}^{\perp}}} \times \frac{1}{\sigma^{2d_{\mathcal{D}}^{\perp}}} + \mathcal{O}\left(\frac{1}{\sigma^{2(d_{\mathcal{D}}^{\perp}+1)}}\right), & \text{if } \deg(P) = d_{\mathcal{D}}^{\perp}, \text{ when } \sigma \to +\infty \end{cases} \tag{8}$$

where σ is the standard deviation of noise in the leakage of each share.

Proof. See [CGC+21a].

Mutual information of IPM and DSM

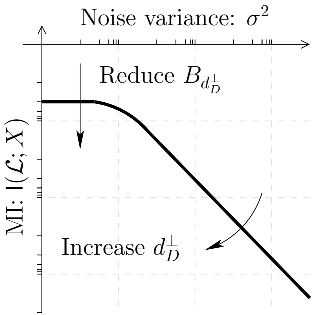


Figure 4: Two concomitant objectives to reduce the mutual information.

Two observations:

- the slope in the log-log representation of the MI versus the noise standard deviation is all the steeper as $d_D^\perp$ is high, and
- the vertical offset is adjusted by $B_{d_D^\perp}$: the smaller it is the smaller the MI.

Mutual information of different codes in IPM

Numerical validation

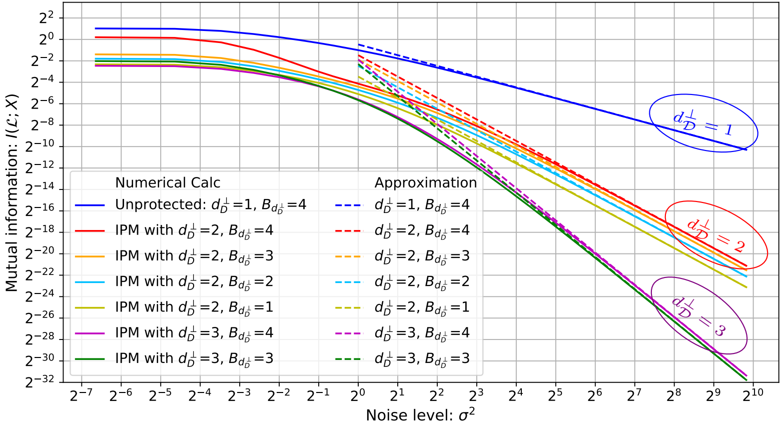


Figure 5: Numerical calculation and approximation of $\mathrm{I}(\mathcal{L}; X)$ between leakages and X in IPM.

Evaluation framework and optimal codes for GCM

A unified evaluation framework for GCM

For GCM with $Z = X\mathbf{G} + Y\mathbf{H}$, its side-channel resistance can be characterized by two defining parameters $d_{\mathcal{D}}^{\perp}$ and $B'_{d_{\mathcal{D}}^{\perp}}$, where codes $\mathcal{C}$ and $\mathcal{D}$ are generated by $\mathbf{G}$ and $\mathbf{H}$.

Optimal codes for GCM

The optimal codes for GCM are determined by $d_{\mathcal{D}}^{\perp}$ and $B'_{d_{\mathcal{D}}^{\perp}}$, which can be chosen by maximizing $d_{\mathcal{D}}^{\perp}$ and /or minimizing $B'_{d_{\mathcal{D}}^{\perp}}$.

Outline

SSS-based masking and RS code

Definition (Reed-Solomon Code [CMP18]).

The Reed-Solomon code RS$(\mathcal{S}, t+1) \subset \mathbb{K}^n$ *of dimension* $t+1$ *over a finite field* $\mathbb{K}$ *and with evaluation subset* $\mathcal{S} = \{\alpha_0, \alpha_1, \ldots, \alpha_n\}$ *of* $\mathbb{K}$ *is the subspace:*

$$RS(\mathcal{S}, t+1) = \{(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_n)); f(\mathsf{X}) \in \mathbb{K}[\mathsf{X}] \textit{ and } \deg(f) \leq t\} .$$

SSS-based masking and RS code

In fact, the sharing of X with SSS scheme is an encoding with a RS code: RS$(\{\alpha_1, \ldots, \alpha_n\}, t+1)$:

$$Z = (Z_1, Z_2, \ldots, Z_n) = (X, Y) \begin{pmatrix} \mathbf{G} \\ \mathbf{H} \end{pmatrix} = X\mathbf{G} + Y\mathbf{H}, \tag{9}$$

where $\begin{pmatrix} \mathbf{G} \\ \mathbf{H} \end{pmatrix}$ is the generator matrix $(\alpha_i^j)_{i \in [1;\, n],\, j \in [0;\, t]}$ shown as below.

$$\mathbf{G} = \begin{pmatrix} 1 & 1 & \cdots & 1 \end{pmatrix} \in \mathbb{K}^{1 \times n}$$

$$\mathbf{H} = \begin{pmatrix} \alpha_1^1 & \alpha_2^1 & \cdots & \alpha_n^1 \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^t & \alpha_2^t & \cdots & \alpha_n^t \end{pmatrix} \in \mathbb{K}^{t \times n}$$

By denoting $\mathbf{G}_i$ and $\mathbf{H}_i$ the i-th column of $\mathbf{G}$ and $\mathbf{H}$ resp., we have:

$$Z_i = f_X(\alpha_i) = X + \sum_{j=1}^{t} Y_j \alpha_i^j = X\mathbf{G}_i + (Y_1, \ldots, Y_t)\, \mathbf{H}_i.$$

SSS-based masking: one instance

$(3,1)$-SSS based masking

Considering $n = 3$ and $t = 1$, giving α_1, α_2 and α_3 are three public points, we have

$$\begin{aligned} \mathbf{G} & & &= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, \\ \mathbf{H} &= \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} &&= \begin{pmatrix} 1 & \alpha^j & \alpha^k \end{pmatrix}. \end{aligned}$$

Therefore, taking a random mask u_1, X is encoded into:

$$\begin{aligned} Z &= (Z_1, Z_2, Z_3) \\ &= X\mathbf{G} + u_1\mathbf{H} \\ &= (X + u_1\alpha_1, X + u_1\alpha_2, X + u_1\alpha_3). \end{aligned} \tag{10}$$

Mutual information of SSS-based masking

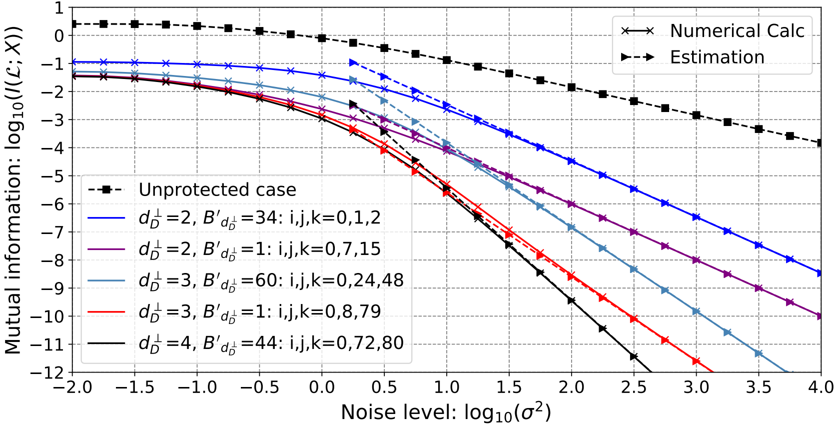


Figure 6: Numerical calculation and approximation of $I(\mathcal{L}; X)$ between leakage $\mathcal{L}$ and X in $(3,1)$-SSS based masking. The three public points are $\alpha_1 = \alpha^i$, $\alpha_2 = \alpha^j$, $\alpha_3 = \alpha^k$.

All codes for $(3, 1)$-SSS based masking

Table 1: Exhibiting different codes in $(3, 1)$-SSS scheme generated by Eqn. 10. Note that we take $\alpha_1 = \alpha^i = 1$, $\alpha_2 = \alpha^j$ and $\alpha_3 = \alpha^k$.

	$j = 1$, $k = 2$	$j = 7$, $k = 15$	$j = 24$, $k = 48$	$j = 8$, $k = 79$	$j = 59$, $k = 172$	$\boldsymbol{j = 72}$, $\boldsymbol{k = 80}$
Minimum distance $d_{\mathcal{D}}$	3	3	3	3	3	3
Dual distance (word) $d_{\mathcal{D}}^{\perp}$	2	2	2	2	2	2
Dual distance (bit) $d_{\mathcal{D}_2}^{\perp}$	2	2	3	3	**4**	**4**
Kissing number (bit) $B_{d_{\mathcal{D}_2}^{\perp}}$	20	**1**	22	**1**	76	**36**
Adjusted kissing number (bit) $B'_{d_{\mathcal{D}_2}^{\perp}}$	34	**1**	60	**1**	140	**44**

We extend the state-of-the-art [CS21] in two directions:

- we show the BEST cases of the linear codes, that are recommended to use,
- we give the WORST cases of the linear codes that are NOT recommend for practical applications.

[0] All codes are available at: https://github.com/Qomo-CHENG/GeneralizedCM

More redundancy leaks more

Recall that in $(3, 1)$-SSS based masking:

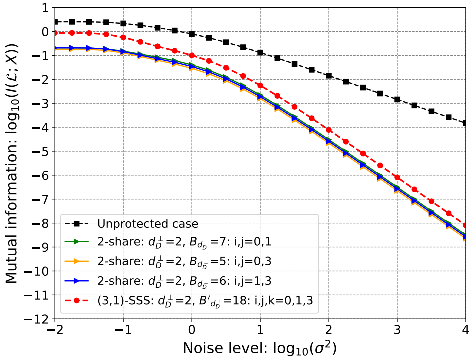
$$\begin{aligned}\mathbf{G} &= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}, \\ \mathbf{H} = \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 \end{pmatrix} &= \begin{pmatrix} 1 & \alpha^j & \alpha^k \end{pmatrix}.\end{aligned}$$

Taking a random mask u_1, then X is encoded into:

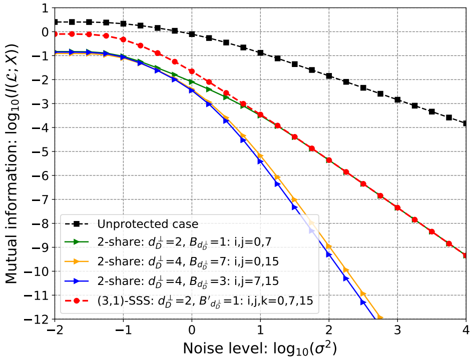
$$\begin{aligned} Z &= (Z_1, Z_2, Z_3) \\ &= X\mathbf{G} + u_1\mathbf{H} \\ &= (X + u_1\alpha_1, X + u_1\alpha_2, X + u_1\alpha_3). \end{aligned}$$

More redundancy leaks more

In $(3,1)$-SSS based masking



(a) $\alpha^i, \alpha^j, \alpha^k = 1, \alpha, \alpha^2$.

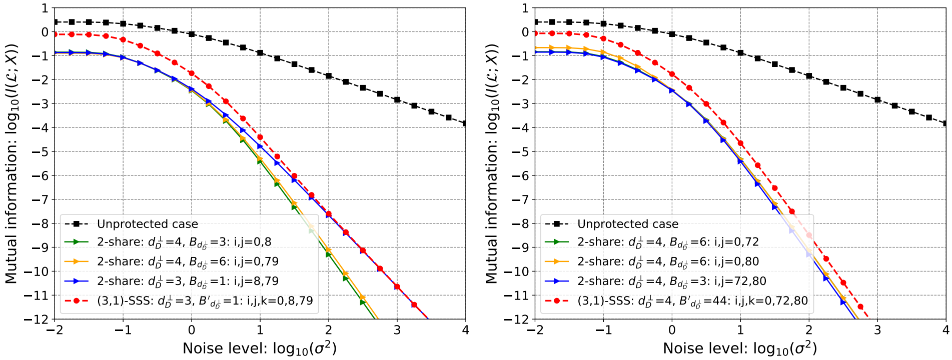


(b) $\alpha^i, \alpha^j, \alpha^k = 1, \alpha^7, \alpha^{15}$.

Figure 7: More shares leak more information, two cases on $(3,1)$-SSS based masking.

More redundancy leaks more

In $(3,1)$-SSS based masking



(a) $\alpha^i, \alpha^j, \alpha^k = 1, \alpha^8, \alpha^{79}$.

(b) $\alpha^i, \alpha^j, \alpha^k = 1, \alpha^{72}, \alpha^{80}$.

Figure 8: More shares leak more information, two cases on $(3,1)$-SSS based masking.

Outline

Conclusions

We propose a coding-theoretic approach to quantify the side-channel resistance of general code-based masking:

- using SNR and MI to characterize the SCA resistance quantitatively
- proposing a unified framework to evaluate all codes for GCM systematically
- presenting a simple method to choose optimal codes for GCM and provide some instances

Open sources on `Github`

- Optimal linear codes for IPM: `https://github.com/Qomo-CHENG/OC-IPM`
- Optimal linear codes for GCM: `https://github.com/Qomo-CHENG/GeneralizedCM`
  The paper is available at: `https://tches.iacr.org/index.php/TCHES/article/view/8983`

Welcome to our talk in *PROOFS 2021* on Sep 17, 2021, we will show our justification of MI and how to choose optimal linear codes for GCM based on the complete weight distribution.

PROOFS 2021: `http://www.proofs-workshop.org/2021/`

Questions?

Acknowledgments

This work has been partly financed by:

- the BRAINE ("Big data pRocessing and Artificial Intelligence at the Network Edge") H2020 ECSEL European Project, N°876967
- the French FUI (AAP-22) program CSAFE+, related to secure implementation of cryptographic algorithm ready to be protected against perturbation attacks
- the National Natural Science Foundation of China, N°61632020.

References I

[BCC+14] Julien Bringer, Claude Carlet, Hervé Chabanne, Sylvain Guilley, and Houssem Maghrebi.
Orthogonal Direct Sum Masking - A Smartcard Friendly Computation Paradigm in a Code, with Builtin Protection against Side-Channel and Fault Attacks.
In David Naccache and Damien Sauveron, editors, *Information Security Theory and Practice. Securing the Internet of Things - 8th IFIP WG 11.2 International Workshop, WISTP 2014, Heraklion, Crete, Greece, June 30 - July 2, 2014. Proceedings*, volume 8501 of *Lecture Notes in Computer Science*, pages 40–56. Springer, 2014.

[BFG15] Josep Balasch, Sebastian Faust, and Benedikt Gierlichs.
Inner Product Masking Revisited.
In Elisabeth Oswald and Marc Fischlin, editors, *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 I*, volume 9056 of *Lecture Notes in Computer Science*, pages 486–510. Springer, 2015.

[BFGV12] Josep Balasch, Sebastian Faust, Benedikt Gierlichs, and Ingrid Verbauwhede.
Theory and Practice of a Leakage Resilient Masking Scheme.
In Xiaoyun Wang and Kazue Sako, editors, *Advances in Cryptology - ASIACRYPT 2012 - 18th International Conference on the Theory and Application of Cryptology and Information Security, Beijing, China, December 2-6, 2012. Proceedings*, volume 7658 of *Lecture Notes in Computer Science*, pages 758–775. Springer, 2012.

[Car13] Claude Carlet.
Correlation-Immune Boolean Functions for Leakage Squeezing and Rotating S-Box Masking against Side Channel Attacks.
In Benedikt Gierlichs, Sylvain Guilley, and Debdeep Mukhopadhyay, editors, *SPACE*, volume 8204 of *Lecture Notes in Computer Science*, pages 70–74. Springer, 2013.

[CDG+14] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, Houssem Maghrebi, and Emmanuel Prouff.
Achieving side-channel high-order correlation immunity with leakage squeezing.
J. Cryptographic Engineering, 4(2):107–121, 2014.

References II

[CDGM12] Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Maghrebi.
Leakage Squeezing of Order Two.
In Steven D. Galbraith and Mridul Nandi, editors, *Progress in Cryptology - INDOCRYPT 2012, 13th International Conference on Cryptology in India, Kolkata, India, December 9-12, 2012. Proceedings*, volume 7668 of *Lecture Notes in Computer Science*, pages 120–139. Springer, 2012.

[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.

[CG18] Claude Carlet and Sylvain Guilley.
Statistical properties of side-channel and fault injection attacks using coding theory.
Cryptography and Communications, 10(5):909–933, 2018.

[CGC+21a] Wei Cheng, Sylvain Guilley, Claude Carlet, Jean-Luc Danger, and Sihem Mesnager.
Information leakages in code-based masking: A unified quantification approach.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2021(3):465–495, 2021.

[CGC+21b] Wei Cheng, Sylvain Guilley, Claude Carlet, Sihem Mesnager, and Jean-Luc Danger.
Optimizing Inner Product Masking Scheme by a Coding Theory Approach.
IEEE Trans. Inf. Forensics Secur., 16:220–235, 2021.

[CGG+19] Claude Carlet, Sylvain Guilley, Cem Güneri, Sihem Mesnager, and Ferruh Özbudak.
Construction of efficient codes for high-order direct sum masking.
In José Luis Hernández Ramos and Antonio F. Skarmeta, editors, *Security and Privacy in the Internet of Things: Challenges and Solutions*, volume 27 of *Ambient Intelligence and Smart Environments*, pages 108–128. IOS Press, 2019.

References III

[CGM19] Claude Carlet, Sylvain Guilley, and Sihem Mesnager.
Direct Sum Masking as a Countermeasure to Side-Channel and Fault Injection Attacks.
In José Luis Hernández Ramos and Antonio F. Skarmeta, editors, *Security and Privacy in the Internet of Things: Challenges and Solutions*, volume 27 of *Ambient Intelligence and Smart Environments*, pages 148–166. IOS Press, 2019.

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi.
Towards Sound Approaches to Counteract Power-Analysis Attacks.
In *CRYPTO*, volume 1666 of *LNCS*. Springer, August 15-19 1999.
Santa Barbara, CA, USA. ISBN: 3-540-66347-9.

[CMP18] Hervé Chabanne, Houssem Maghrebi, and Emmanuel Prouff.
Linear repairing codes and side-channel attacks.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(1):118–141, 2018.

[CS21] Nicolas Costes and Martijn Stam.
Redundant code-based masking revisited.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2021(1):426–450, 2021.

[DGH+18] Jean-Luc Danger, Sylvain Guilley, Annelie Heuser, Axel Legay, and Ming Tang.
Physical Security Versus Masking Schemes.
In Çetin Kaya Koç, editor, *Cyber-Physical Systems Security.*, pages 269–284. Springer, 2018.

[GSF13] Vincent Grosso, François-Xavier Standaert, and Sebastian Faust.
Masking vs. Multiparty Computation: How Large Is the Gap for AES?
In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 400–416. Springer, 2013.

References IV

[ISW03] Yuval Ishai, Amit Sahai, and David Wagner.
Private Circuits: Securing Hardware against Probing Attacks.
In *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, August 17–21 2003.
Santa Barbara, California, USA.

[MGD11] Houssem Maghrebi, Sylvain Guilley, and Jean-Luc Danger.
Leakage squeezing countermeasure against high-order attacks.
In Claudio Agostino Ardagna and Jianying Zhou, editors, *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication - 5th IFIP WG 11.2 International Workshop, WISTP 2011, Heraklion, Crete, Greece, June 1-3, 2011. Proceedings*, volume 6633 of *Lecture Notes in Computer Science*, pages 208–223. Springer, 2011.

[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.

[PGS+17] Romain Poussier, Qian Guo, François-Xavier Standaert, Claude Carlet, and Sylvain Guilley.
Connecting and Improving Direct Sum Masking and Inner Product Masking.
In Thomas Eisenbarth and Yannick Teglia, editors, *Smart Card Research and Advanced Applications - 16th International Conference, CARDIS 2017, Lugano, Switzerland, November 13-15, 2017, Revised Selected Papers*, volume 10728 of *Lecture Notes in Computer Science*, pages 123–141. Springer, 2017.

[PR13] Emmanuel Prouff and Matthieu Rivain.
Masking against Side-Channel Attacks: A Formal Security Proof.
In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 142–159. Springer, 2013.

References V

[PRR14] Emmanuel Prouff, Matthieu Rivain, and Thomas Roche.
On the Practical Security of a Leakage Resilient Masking Scheme.
In Josh Benaloh, editor, *Topics in Cryptology - CT-RSA 2014 - The Cryptographer's Track at the RSA Conference 2014, San Francisco, CA, USA, February 25-28, 2014. Proceedings*, volume 8366 of *Lecture Notes in Computer Science*, pages 169–182. Springer, 2014.

[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.

[WMCS20] Weijia Wang, Pierrick Méaux, Gaëtan Cassiers, and François-Xavier Standaert.
Efficient and Private Computations with Code-Based Masking.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2020(2):128–171, 2020.

[WSY+16] Weijia Wang, François-Xavier Standaert, Yu Yu, Sihang Pu, Junrong Liu, Zheng Guo, and Dawu Gu.
Inner Product Masking for Bitslice Ciphers and Security Order Amplification for Linear Leakages.
In Kerstin Lemke-Rust and Michael Tunstall, editors, *Smart Card Research and Advanced Applications - 15th International Conference, CARDIS 2016, Cannes, France, November 7-9, 2016, Revised Selected Papers*, volume 10146 of *Lecture Notes in Computer Science*, pages 174–191. Springer, 2016.