Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings

COSADE, München, April 3, 2023

Julien Béguinot, Wei Cheng, Loïc Masure, Sylvain Guilley, Yi Liu, Olivier Rioul & François-Xavier Standaert

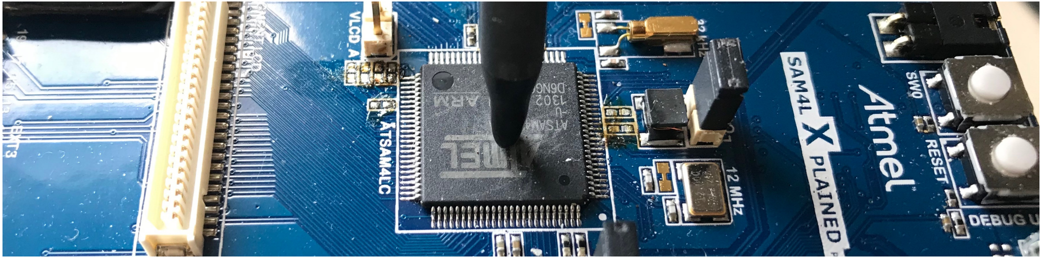
LTCI, Télécom Paris, Institut Polytechnique de Paris
Secure-IC S.A.S.
ICTEAM Institute, Université catholique de Louvain

April 3, 2023

https://eprint.iacr.org/2022/1738.pdf

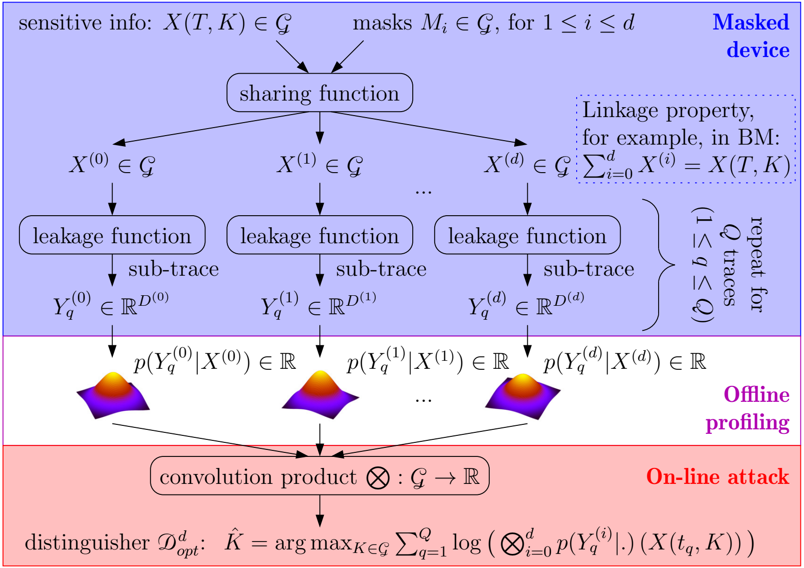
European Research Council
Established by the European Commission

Side Channel

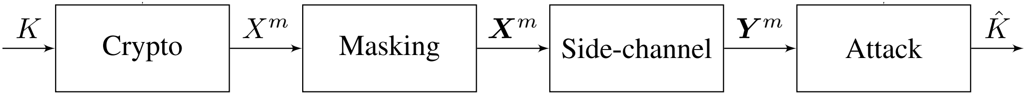


Masking as a Countermeasure

Example of Boolean Masking (BM) in $\mathcal{G} = \mathbb{Z}_{2^n}$

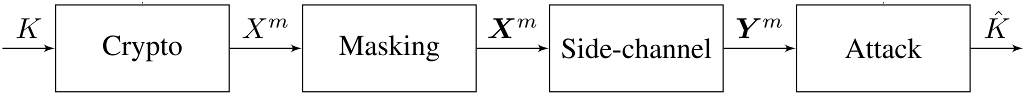


Theoretical Problem



- compute sensitive values $X \sim \mathcal{U}(M)$ in an Abelian group $(\mathcal{G}, \oplus)$ of order $M = |\mathcal{G}|$, which depends on some secret K;
- secret sharing computation: X is split into $d+1$ random shares $X_i \sim \mathcal{U}(M)$: $X = X_0 \oplus X_1 \oplus \cdots \oplus X_d$ in $\mathcal{G}$;
- this is a dth-order masking countermeasure against noisy leakages $Y_0, \ldots, Y_d$;
- defender's (worst case) problem: Evaluate the *minimum number of measurements* m that can achieve the *best possible performance* (SR), i.e., probability of success $\mathbb{P}_s = \mathbb{P}_s(K|\mathbf{Y}^m)$ given by the MAP rule.

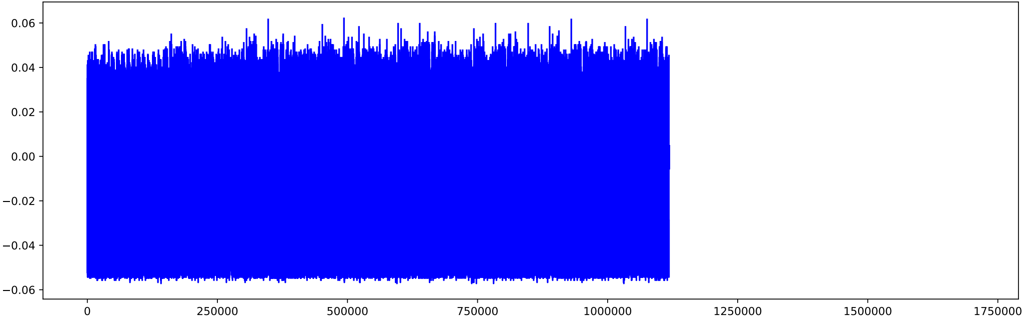
Theoretical Problem



- compute sensitive values $X \sim \mathcal{U}(M)$ in an Abelian group $(\mathcal{G}, \oplus)$ of order $M = |\mathcal{G}|$, which depends on some secret K;
- secret sharing computation: X is split into $d+1$ random shares $X_i \sim \mathcal{U}(M)$: $X = X_0 \oplus X_1 \oplus \cdots \oplus X_d$ in $\mathcal{G}$;
- the adversary performs m measurements to achieve a given success rate (SR);
- defender's (worst case) problem: Evaluate the *minimum number of measurements* m that can achieve the *best possible performance* (SR), i.e., probability of success $\mathbb{P}_s = \mathbb{P}_s(K|\mathbf{Y}^m)$ given by the MAP rule.

Evaluation Context: High Dimension Traces

A Trace Sample from the DPA Contest



Duc+*al* Evaluation Bound

"Making Masking Security Proofs Concrete," Duc, Faust & Standaert, Eurocrypt2015

Theorem (Duc+al evaluation bound)

$$m \geqslant \frac{\log \frac{1-1/M}{1-\mathbb{P}_s}}{-\log(1-(\frac{M}{\sqrt{2\log e}})^{d+1}\prod_{i=0}^{d}\sqrt{I(X_i;Y_i)})} \quad (1)$$

For high noise, the denominator is $\approx (\frac{M}{\sqrt{2\log e}})^{d+1} \prod_{i=0}^{d} I(X_i;Y_i)^{1/2}$ which is too large even for moderate SNR.

Duc+*al* Long Standing Conjecture

"Making Masking Security Proofs Concrete," Duc, Faust & Standaert, Eurocrypt2015

Conjecture (Duc+*al*, revisited)

$$m \geqslant f(SR)\left(\prod_{i=0}^{d} \frac{I(X_i;Y_i)}{\tau}\right)^{-\gamma}$$

where

- *f is a function independent (or mildly depending) on the field size M;*
- *$\tau = 1$[1] is a noise amplification threshold;*
- *$\gamma = 1$ is the exponent yielding an effective masking order $d' = \gamma d$.*

[1] When the mutual information is expressed in bits.

Masure+*al* Evaluation Bound

"A Nearly Tight Proof of Duc et al.'s Conjectured Security Bound for Masked Implementations," Masure, Rioul & Standaert CARDIS2022

Theorem (Masure+*al*)

$$m \geqslant \frac{d(\mathbb{P}_s || \frac{1}{M})}{\log(1 + \frac{M}{2} \prod_{i=0}^{d} \frac{2}{\log e} I(X_i; Y_i))}$$

- independently, "On the Success Rate of Side-Channel Attacks on Masked Implementations," Ito, Ueno & Homma, CCS2022 derived the same expression with $M-1$ instead of $M/2$. Their proof uses Pinsker inequality and the Fourier transform on $\mathcal{G} = \mathbb{Z}_2^n$ (Parseval)

TELECOM Paris IP PARIS

Masure+*al* Evaluation Bound

"A Nearly Tight Proof of Duc et al.'s Conjectured Security Bound for Masked Implementations," Masure, Rioul & Standaert CARDIS2022

Theorem (Masure+*al*)

$$m \geqslant \frac{d(\mathbb{P}_s || \frac{1}{M})}{\log(1 + \frac{M}{2} \prod_{i=0}^{d} \frac{2}{\log e} I(X_i; Y_i))}$$

- independently, "On the Success Rate of Side-Channel Attacks on Masked Implementations," Ito, Ueno & Homma, CCS2022 derived the same expression with $M-1$ instead of $M/2$. Their proof uses Pinsker inequality and the Fourier transform on $\mathcal{G} = \mathbb{Z}_2^n$ (Parseval)
- for high noise, the denominator is $\approx M(\frac{2}{\log e})^d \prod_{i=0}^{d} I(X_i; Y_i)$ which improves upon $(\frac{M}{\sqrt{2\log e}})^{d+1} \prod_{i=0}^{d} I(X_i; Y_i)^{1/2}$. Yet it still gives loose security guarantees compared to actual attacks (factor 256 for AES)

Revisiting Mrs. Gerber's Lemma

"A Theorem on the Entropy of Certain Binary Sequences and Applications: Part I," Wyner & Ziv,

Transaction Information Theory, 1973

Lemma (MGL)

$h(h^{-1}(x) \star h^{-1}(y))$ is convex in x for fixed y, where $h(p) = -p\log p - (1-p)\log(1-p)$ and $p \star q = p(1-q) + (1-p)q$.

Lemma (Revisited MGL)

For $\mathcal{G} = \mathbb{Z}_2$,

$$I(X, \mathbf{Y}) \leqslant \varphi\left(\prod_{i=0}^{d} \varphi^{-1}(I(X_i, Y_i))\right)$$

where $\varphi(x) = \log(2) - h(\frac{1-x}{2})$ is the binary DFT of h.

Revisiting Mrs. Gerber's Lemma

"The EPI and MGL for Groups of Order 2n," Jog & Anantharam, **Transaction Information Theory, 2014**

Lemma (Revisited Extended MGL)

For $|\mathbb{G}| = 2^n$,

$$I(X, \mathbf{Y}) \leqslant \varphi(\prod_{i=0}^{d} \varphi^{-1}(I(X_i, Y_i)))$$

where $\varphi(x) = \log(2) - h(\frac{1-x}{2})$ *and the product is taken only over* $I(X_i; Y_i) < \log 2$.

The number $d' \leqslant d$ of shares such that $I(X_i; Y_i) < \log 2$ can be seen as the effective masking order of the implementation. For correct masking implementation and under high noise $d' = d$.

Consequence for Masking Security (Our Contribution)

With the condition that there exists at least one $I(X_i; Y_i) < \log(2)$:

Theorem (Main Theorem)

For alphabet size $M = 2^n$,

$$m \geqslant \frac{d(\mathbb{P}_s || \frac{1}{M})}{\varphi(\prod_i \varphi^{-1}(I(X_i; Y_i)))}$$

For high noise (all $I(X_i; Y_i) < \log(2)$), since $\varphi(x) \approx (\frac{\log e}{2})x^2$ as $x \to 0$, the denominator is $\approx (\frac{1}{\log e})^d \prod_{i=0}^{d} I(X_i; Y_i)$

The derived bound is optimal without further assumption.

TELECOM Paris IP PARIS

High Noise Regime

Theorem (Main Theorem with High Noise)

For alphabet size $M = 2^n$, and high noise

$$m \gtrsim \frac{d(\mathbb{P}_s || \frac{1}{M})}{(\frac{2}{\log e})^d \prod_{i=0}^{d} I(X_i; Y_i)}$$

Proof.

$\varphi(x) \approx (\frac{\log e}{2})x^2$ as $x \to 0$ □

This proves Duc's conjecture except for the noise threshold $\tau \approx 0.72$ and not 1. Though this is only with the Taylor expansion in zero, it seems that there is no real "noise threshold".

TELECOM Paris IP PARIS

Illustration for $M = 256$

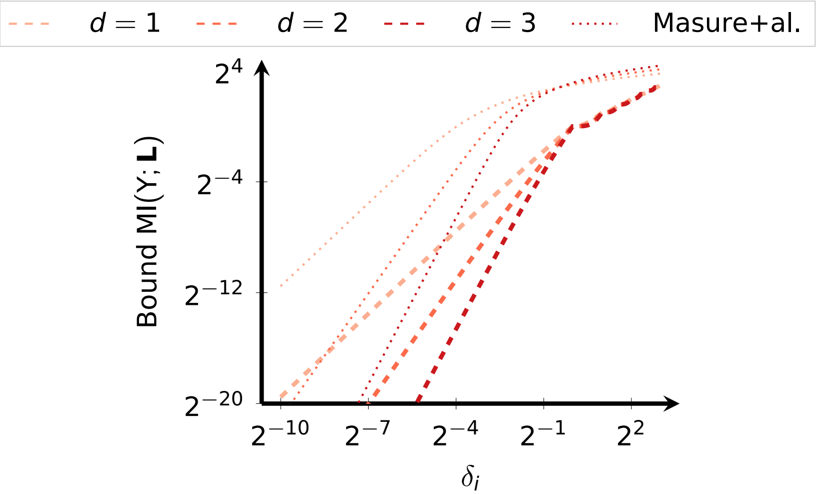
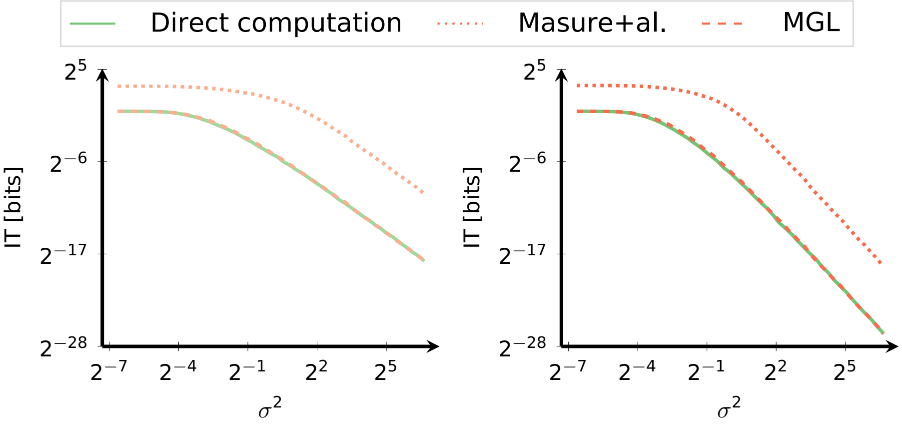


Figure: Illustration of the inequality for $M = 256$ (e.g., the AES S-box).

Practical Evaluation LSB

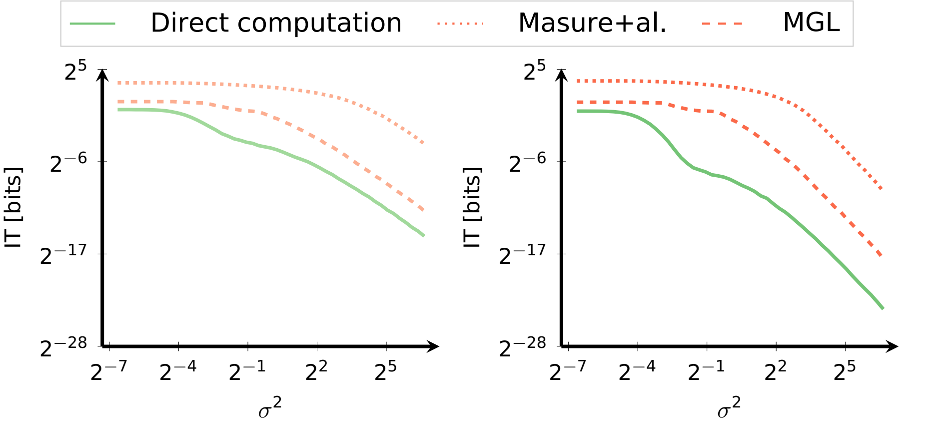


(a) lsb, $d = 1$.

(b) lsb, $d = 2$.

(c) MI in function of the Gaussian noise variance σ^2, for $n = 8$ bits.

Practical Evaluation HW

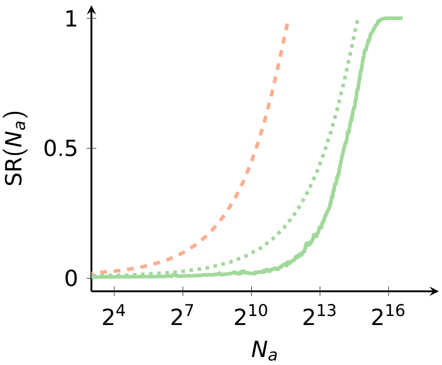


(a) HW, $d = 1$.

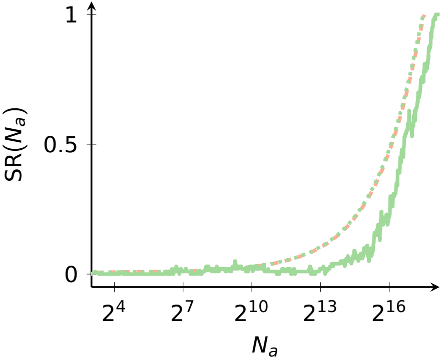
(b) HW, $d = 2$.

(c) MI in function of the Gaussian noise variance σ^2, for $n = 8$ bits.

Practical Evaluation $d = 1$



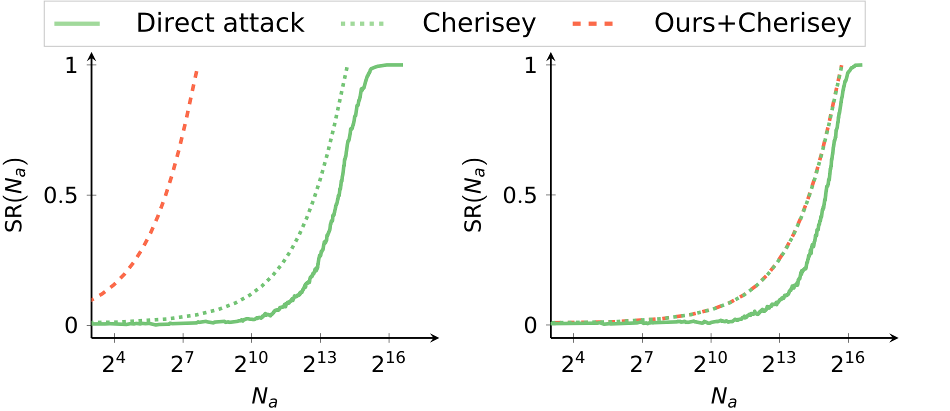
(a) HW.



(b) lsb.

Figure: Extending MI bounds to concrete security bounds for $\sigma^2 = 2^5, d = 1$.

Practical Evaluation $d = 2$



(a) HW. (b) Isb.

Figure: Extending MI bounds to concrete security bounds for $\sigma^2 = 2^2, d = 2$.

Conclusion & Perspectives

- We derived **optimal bounds** removing the field size from Duc+al. conjecture.
- Tighter bounds with mild assumptions ? n^{-d} for "generic leakages"
- Tightness for masked computations (e.g., multiplications) and not only encodings ?
- Extension to $M \neq 2^n$ especially for prime M ? We provide preliminary results using majorization arguments in the article.
- Other metrics (Rényi entropy/information, maximal leakage, etc) ?

Removing the Field Size Loss from Duc et al.'s Conjectured Bound for Masked Encodings

Thank you!

Julien Béguinot, Wei Cheng, Loïc Masure, Sylvain Guilley,
Yi Liu, Olivier Rioul & François-Xavier Standaert

LTCI, Télécom Paris, Institut Polytechnique de Paris
Secure-IC S.A.S.
ICTEAM Institute, Université catholique de Louvain

April 3, 2023

https://eprint.iacr.org/2022/1738.pdf

European Research Council
Established by the European Commission

Supplementary Material: Tighter MGL at the Bit Level ?

$$I(X_0 \star \dots X_d; Y_0 \dots Y_d) = \sum_{i=1}^{n} I((X_0 \star \dots X_d)_i; Y_0 \dots Y_d | (X_0 \star \dots X_d)_1^{i-1}) \quad (2)$$

$$\leqslant \sum_{i=1}^{n} I((X_0 \star \dots X_d)_i; Y_0 \dots Y_d | X_{0,1}^{i-1} \dots X_{d,1}^{i-1}) \quad (3)$$

$$\approx n^{-d} \varphi(\prod_j \varphi^{-1}(I(X_j; Y_j))) \quad (4)$$

Conjecture: We can still gain n^{-d} for "generic leakages"

Using Majorization

Theorem (Improved Bound for Generic Groups)

Let $P = \frac{1}{4}\prod_{i=0}^{d} C\,\mathrm{MI}(Y_i; L_i)$ *where* $C = 2/\log e$ *we have*

$$\mathrm{MI}(Y;\mathbf{L}) \leqslant \min\left(\log(1+M^2(4^{\frac{1}{M}}-1)P), (\frac{1}{M}+\sqrt{P})\log(1+M\sqrt{P})\right). \tag{5}$$