Colloque de l'Institut Mines Télécom IMT Risques&Cyber 2023

Institut Mines-Télécom

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Side-Channel Security.

How Much Are You Secure ?

Mrs. Gerber's Lemma and Majorization

Institutions

TELECOM Paris

IP PARIS

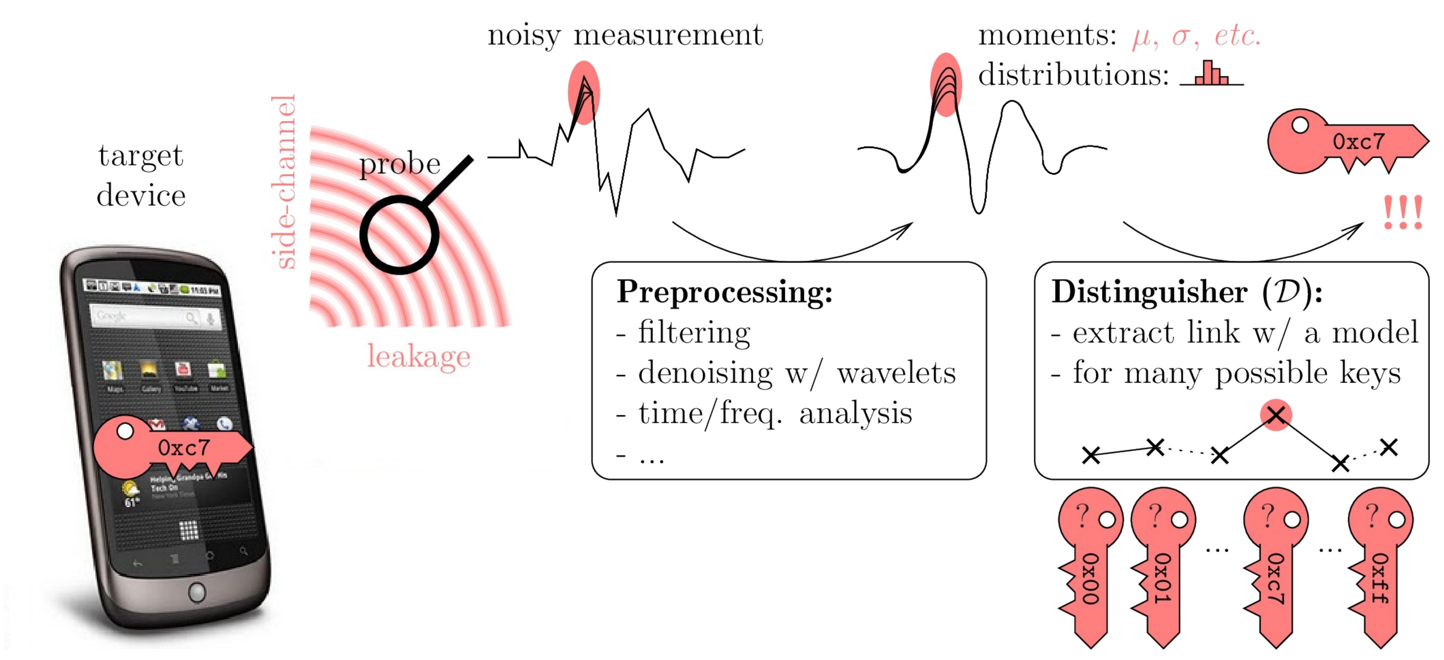
Authors :

Julien Béguinot
Olivier Rioul
Sylvain Guilley
Wei Cheng
Yi Liu

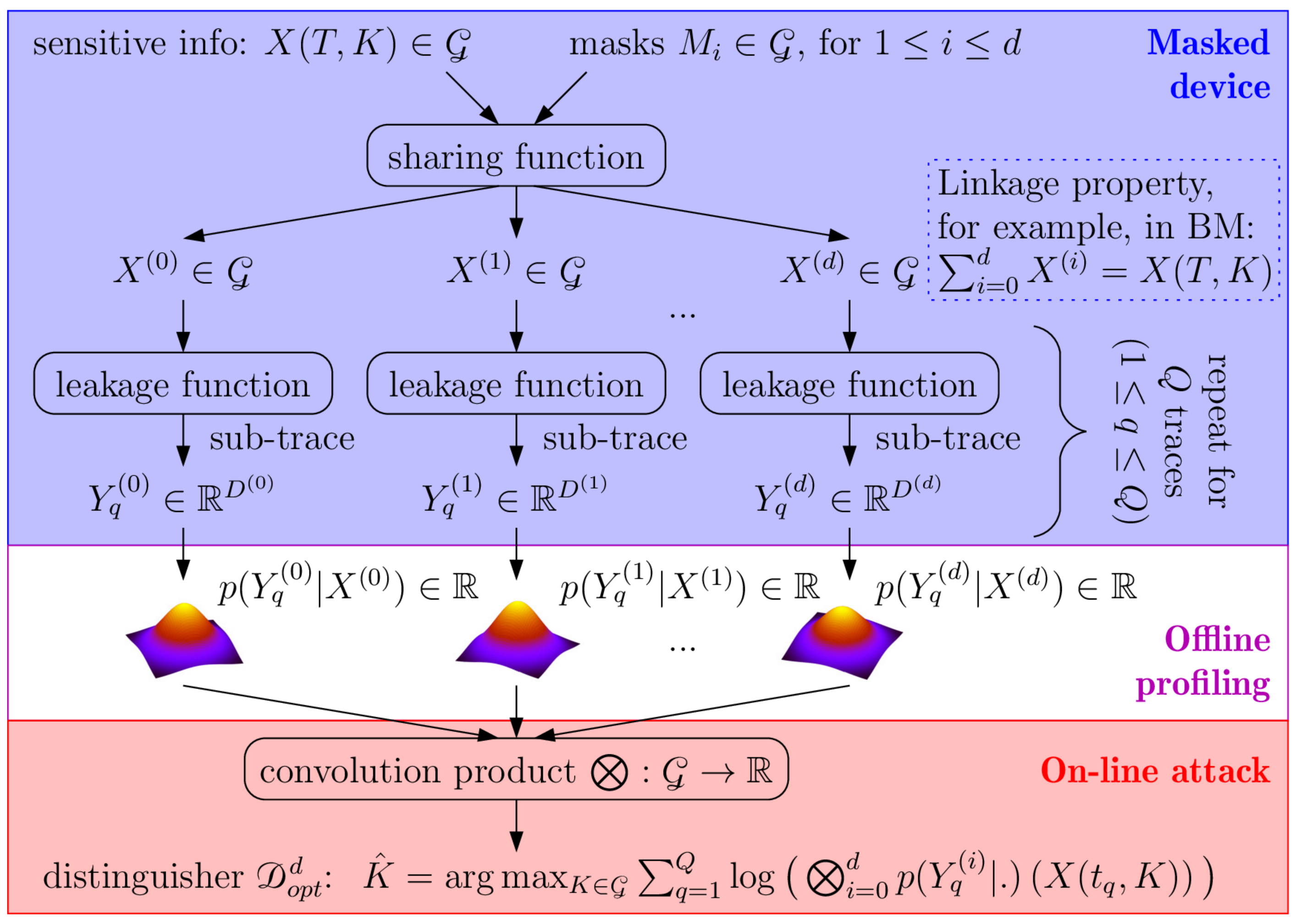
Partners

SECURE-IC THE SECURITY SCIENCE COMPANY

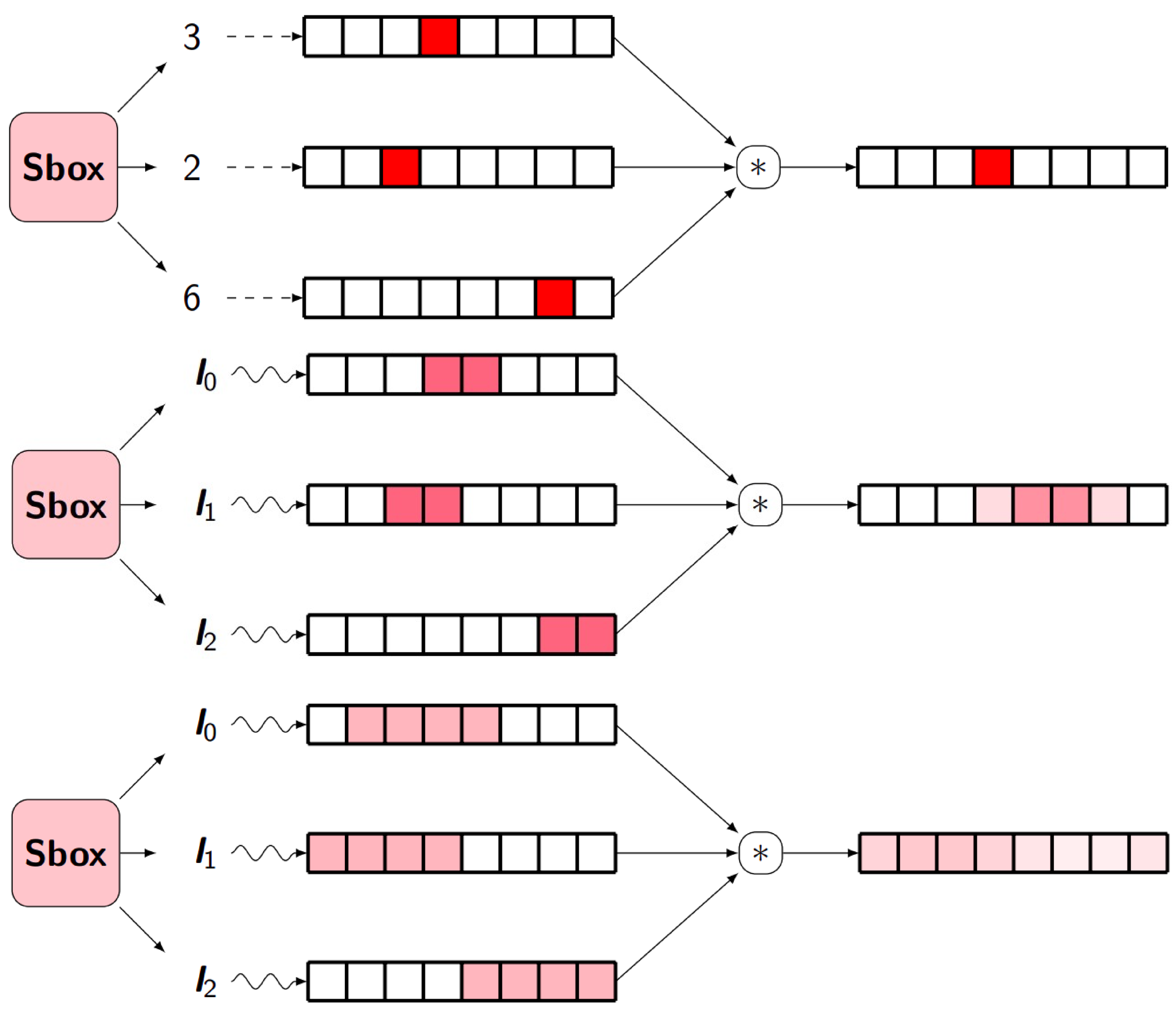
Side-Channel Analysis (SCA)



Countermeasure : Boolean Masking (BM)



Rationale of Masking

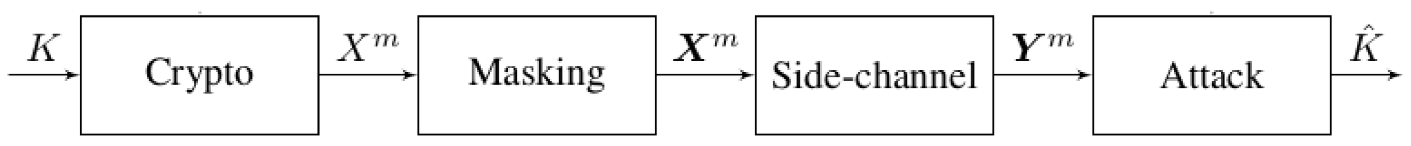


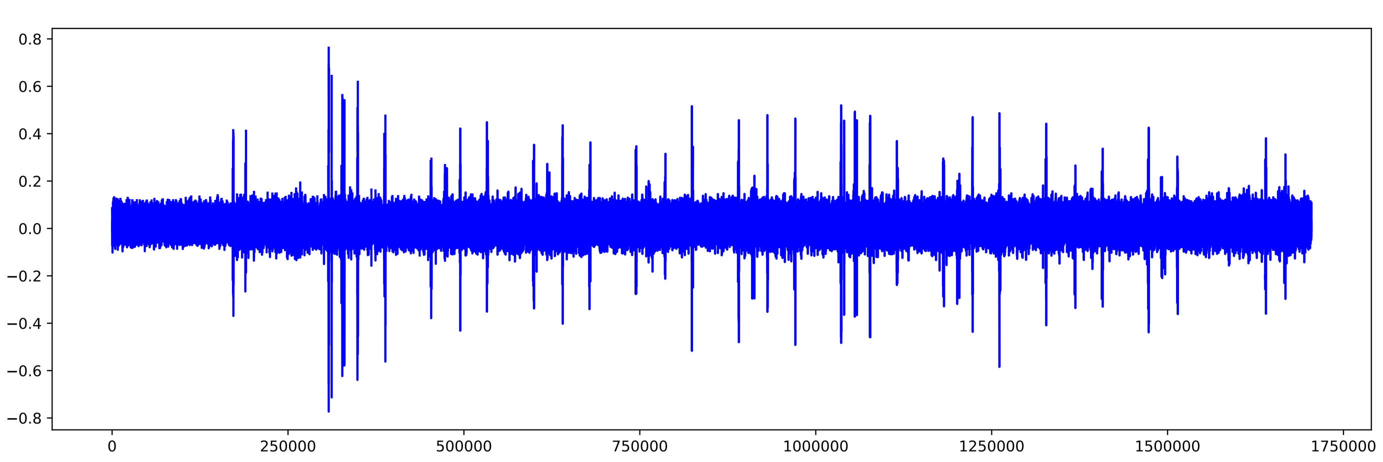
SCA Metrics

Definition (SCA metrics)

There are two main metrics to evaluate SCA :

1. $\mathrm{SR} = \mathbb{P}_s(K|Y)$ the probability of successfuly guessing the secret key ;
2. $G(K|Y)$ the average number of trials to guess the secret key.





Mrs. Gerber Lemma (MGL)

This result is known as "Mrs. Gerber's Lemma" in honor of a certain lady whose presence was keenly felt by the authors at the time this research was done.

Lemma (Revisited Extended MGL [5, 3])

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

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

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

Theorem (MGL for Rényi-Information of order 2 [4])

$$I_2^R(X;Y) \leqslant \log\left(1 + \prod_{i=0}^{d}\left(\exp\left(I_2^R(X_i;Y_i)\right) - 1\right)\right)$$

Theorem (MGL for Maximal Leakages [1])

Let $p_i = \exp(-H_\infty(X_i))$*, without loss of generality we assume* $p_0 \leqslant p_1 \leqslant \ldots \leqslant p_d$*. Let* $k = \lfloor p_0^{-1} \rfloor$, $r = \max\{i | p_i \leqslant \frac{1}{k}\}$.

$$H_\infty(X) \geqslant \begin{cases} -\log\left(\frac{1}{k+1} + \frac{1}{k+1}\prod_{j=0}^{r}((k+1)p_i - 1)\right) & \text{if } r \text{ is even,} \\ -\log\left(\frac{1}{k+1} + \frac{k}{k+1}\prod_{j=0}^{r}((k+1)p_i - 1)\right) & \text{if } r \text{ is odd.} \end{cases}$$

Number of Traces

Theorem (Masking Security [2])

For alphabet size $M = 2^n$,

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

Theorem (Alpha-Rényi Information of order 2 [4])

$$m \geqslant \frac{d_2(\mathbb{P}_s \| \frac{1}{M})}{\log\left(1 + \prod_{i=0}^{d}\left(e^{I_2^R(X_i;Y_i)} - 1\right)\right)}$$

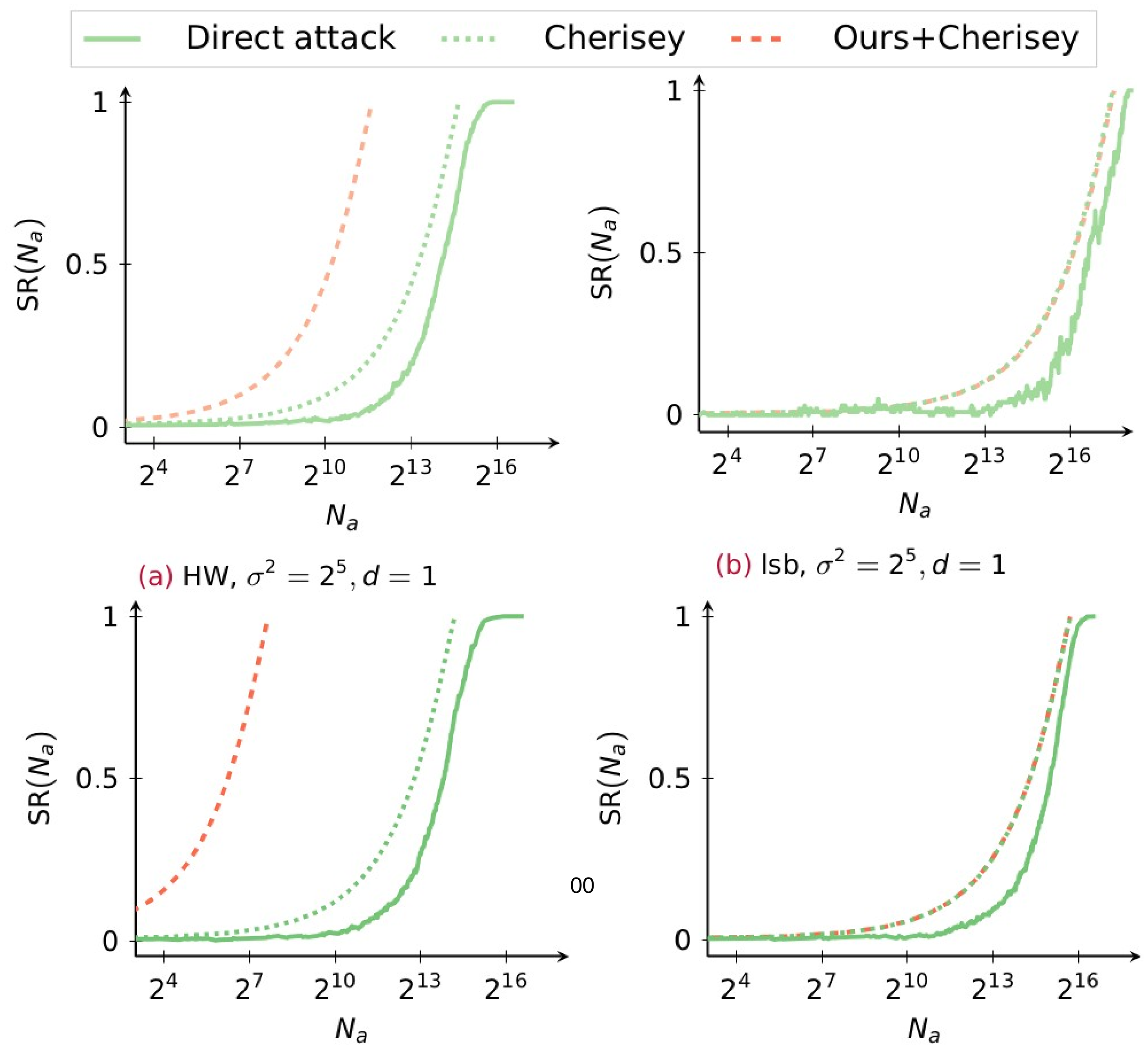
Theorem (Maximal Leakages [1])

At high noise,

$$m \gtrsim \frac{M\mathbb{P}_s - 1}{C_d \prod_{i=0}^{d} I_\infty(X_i;Y_i)}$$

where $C_d = (M-1)(\ln 2)^d$ *if d is odd and* $(\ln 2)^d$ *otherwise.*

Evaluation



(a) HW, $\sigma^2 = 2^5, d = 1$ (b) lsb, $\sigma^2 = 2^5, d = 1$

(a) HW, $\sigma^2 = 2^2, d = 2$ (b) lsb, $\sigma^2 = 2^2, d = 2$

Figure: Extending MI bounds to concrete security bounds.

References

[1] Julien Béguinot et al. "Maximal Leakage of Masked Implementations Using Mrs. Gerbers Lemma for Min-Entropy". In: Submitted to ISIT. 2023.

[2] Julien Béguinot et al. "Removing the field size loss from Duc et al.'s conjectured security bound for masked encodings". In: COSADE. 2023.

[3] Varun S. Jog and Venkat Anantharam. "The Entropy Power Inequality and Mrs. Gerber's Lemma for Groups of Order 2^n". In: IEEE TIT (2014).

[4] Yi Liu et al. "Improved Alpha-Information Bounds for Higher-Order Masked Cryptographic Implementations". In: ITW. 2023.

[5] Aaron D. Wyner and Jacob Ziv. "A theorem on the entropy of certain binary sequences and applications-I". In: IEEE TIT (1973).

Contact : julien.beguinot@telecom-paris.fr