What Can Information Guess ?

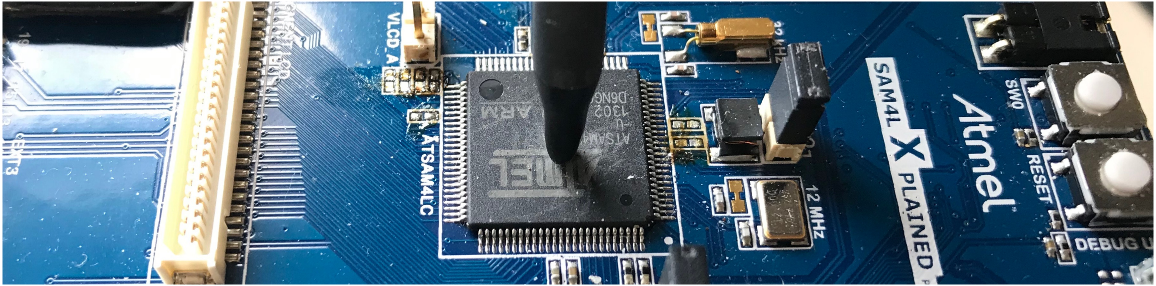
Guessing Advantage vs. Rényi Entropy for Small Leakages

Julien Béguinot, Olivier Rioul

LTCI, Télécom Paris, Institut Polytechnique de Paris

France PhD IT Workshop, Palaiseau, `https://arxiv.org/pdf/2401.17057`

Side-Channel Analysis



Side-Channel Analysis

- Cryptographic algorithm don’t run on paper. . .

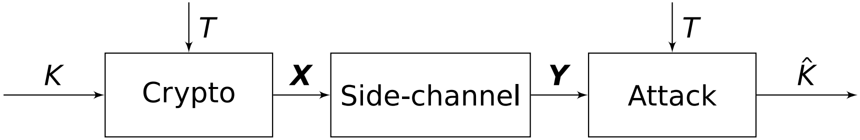
Side-Channel Analysis

- Cryptographic algorithm don't run on paper. . .
- . . . they run on physical device !

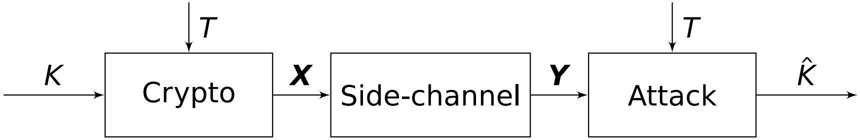
Side-Channel Analysis

- Cryptographic algorithm don't run on paper. . .
- . . . they run on physical device !
- Cryptographic sensitive variables : may physically leak through side-channels (accoustic noise, timing, power consumption, electromagnetic emannation etc...).
- IT perspective : an unintended communication channel of the secret key from the hardware to the attacker.

Theoretical Model

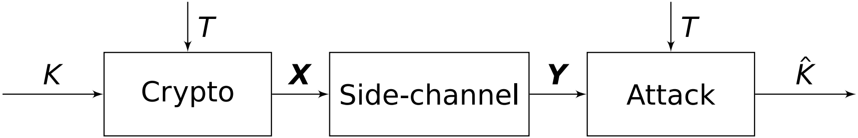


Theoretical Model



- $K = (K_1 \ldots, K_r)$: the secret key ; $K \sim \mathcal{U}(M = 2^{nr})$ is composed of r bytes of n bits ;
- $T = (T_1, \ldots, T_r)$: a public information (plaintext or ciphertext)
- X : a sensitive variable ; $(X_1, \ldots, X_r) = (f(K_1, T_1), \ldots, f(K_r, T_r))$;

Theoretical Model



- $K = (K_1 \ldots, K_r)$: the secret key ; $K \sim \mathcal{U}(M = 2^{nr})$ is composed of r bytes of n bits ;
- $T = (T_1, \ldots, T_r)$: a public information (plaintext or ciphertext)
- X : a sensitive variable ; $(X_1, \ldots, X_r) = (f(K_1, T_1), \ldots, f(K_r, T_r))$;
- $\boldsymbol{Y}$: the corresponding noisy leakage, and the side channel $X_i \longmapsto Y_i$ is stationary and memoryless ; and the adversary performs m measurements to achieve a given guessing entropy.

Quantifying the Adversary's Advantage : Guessing Entropy

1. Let X be a M-ary random variable with probability mass function $(p_1, \ldots, p_M)$. Without loss of generality we can assume that $p_1 \geqslant \ldots \geqslant p_M$.

Quantifying the Adversary's Advantage : Guessing Entropy

1. Let X be a M-ary random variable with probability mass function $(p_1, \ldots, p_M)$. Without loss of generality we can assume that $p_1 \geqslant \ldots \geqslant p_M$.
2. A guessing strategy is a permutation $\sigma \in \mathcal{S}_M$ that specify in which order to guess the key hypothesis

Quantifying the Adversary's Advantage : Guessing Entropy

1. Let X be a M-ary random variable with probability mass function $(p_1, \ldots, p_M)$. Without loss of generality we can assume that $p_1 \geqslant \ldots \geqslant p_M$.
2. A guessing strategy is a permutation $\sigma \in \mathcal{S}_M$ that specify in which order to guess the key hypothesis
3. The guesswork is the average number of guesses of such strategy given by

$$G_\sigma(X) = \sum_{i=1}^{M} \sigma(i) p_i.$$

Quantifying the Adversary's Advantage : Guessing Entropy

1. Let X be a M-ary random variable with probability mass function $(p_1, \ldots, p_M)$. Without loss of generality we can assume that $p_1 \geqslant \ldots \geqslant p_M$.
2. A guessing strategy is a permutation $\sigma \in \mathcal{S}_M$ that specify in which order to guess the key hypothesis
3. The guesswork is the average number of guesses of such strategy given by

$$G_\sigma(X) = \sum_{i=1}^{M} \sigma(i) p_i.$$

4. The guessing entropy is the guesswork of the optimal guessing strategy

$$G(X) = \min_\sigma G_\sigma(X).$$

Guessing Entropy

Lemma

The guessing entropy is given by

$$G(X) = \sum_{i=1}^{M} i p_i.$$

Démonstration.

Assume that the minimum in the definition of guessing entropy is achieved for $\sigma \neq (1, \ldots, M)$. Then tere exists $i < j$ such that $\sigma(i) > \sigma(j)$. Let $\tilde{\sigma} = (i\ j) \circ \sigma$ then $G_\sigma(X) - G_{\tilde{\sigma}}(X) = (\sigma(i) - \sigma(j))(p_i - p_j) \geqslant 0$. □

Given side-information Y the conditional guessing entropy is obtained by averaging the guessing entropies $G(X|Y=y)$ for each y :

$$G(X|Y) = \mathbb{E}_y G(X|Y=y) \qquad (= \mathbb{E}[X] \text{ if } p_1 \geqslant p_2 \ldots \geqslant p_M).$$

TELECOM Paris

Blind Guess and Clear Guess

When the side-information Y is independent of the secret key K then for every $Y = y$ the key is uniform hence

$$G(K|Y) = \mathbb{E}_y \left(\sum_{i=1}^{M} \frac{i}{M} \right) = \frac{M+1}{2}.$$

When the side-information complety reveals the secret key K then then for every $Y = y$ the key is a Dirac hence

$$G(K|Y) = \mathbb{E}_y 1 = 1.$$

The guessing entropy should range from $\frac{M+1}{2}$ to 1 as information leakage increases.

But Guessing Entropy Is Not Scalable. . .

Liron David and Avishai Wool. A bounded-space near-optimal key enumeration algorithm for multi-dimensional side-channel attacks.

For a full AES key $M = 2^{nr}$ where $n = 8$ and $r = 16$ is so huge that computing $\sum_{i=1}^{M} ip_i$ is not computationally feasible. We only know the crude :

$$\prod_{i=1}^{r} G(K_i|Y_i) \leqslant G(K|Y) \leqslant 2^{nr} - \prod_{i=1}^{r} (2^n - G(K_i|Y_i)).$$

Informational Leakage Measure

Instead we evaluate a scalable leakage measure and lower bound the guessing entropy. Perhaps the most natural is mutual information :

$$I(K;Y) = D_{\mathrm{KL}}(P_{KY} \| P_K P_Y) = \sum_{i=1}^{r} I(K_i;Y_i) = nr \log 2 - \sum_{i=1}^{r} H(K_i|Y_i). \quad (1)$$

We need to evaluate each equivocation separately which reduces the complexity from $O(2^{nr})$ to $O(r2^n)$.

Also

$$I(K;Y^m) \leqslant mI(X;Y).$$

Mc Eliece and Yu's Inequality

Robert J McEliece and Zhong Yu. An inequality on entropy. ISIT'95

Theorem (Mc Eliece & Yu Inequality)

$$G(X|Y) \leqslant 1 + \frac{M-1}{2}\frac{H(X|Y)}{\log M} \tag{2}$$

This inequality is optimal i.e. achived everywhere e.g. for when X is uniform and the channel $X \to Y$ is an erasure channel.

Massey's Inequality

J. Massey. Guessing and Entropy. ISIT'94

Theorem (Massey's Inequality)

$$G(X) \geqslant 2^{H(X)-2} + 1 \tag{3}$$

provided that $H(X) \geqslant 2$ bits.

Rioul's Inequality

O. Rioul. Variations on a Theme by Massey. TIT'22

Theorem (Rioul's Inequality)

$$G(K|Y) \geqslant \frac{2^{H(K|Y)}}{e} + \frac{1}{2} \tag{4}$$

Other improved bounds exist see e.g., Sason and Verdù, Improved Bounds on Lossless Source Coding and Guessing Moments via Rényi Measures

Problem with These Inequalities

When $H(K|Y) = \log M$ i.e. $I(K;Y) = 0$ bits the Rioul's bound saturates to

$$\frac{M}{e} + \frac{1}{2} < \frac{M+1}{2}.$$

There is a multiplicative gap of $\frac{2}{e}$.

$\implies$ Let's derive the optimal bound !

$$D_{\mathrm{KL}}(P\|Q) \geqslant 0$$

Key Tool : Gibbs Inequality

Theorem

For any distribution P and Q with respective pmf p, q,

$$D_{\mathrm{KL}}(P||Q) = \sum p \log \frac{p}{q} = \underbrace{\sum p \log \frac{1}{q}}_{C(P||Q)} - \underbrace{\sum p \log \frac{1}{p}}_{H(P)} \geqslant 0.$$

That is

$$H(P) \leqslant C(P||Q)$$

with equality if and only if $P = Q$. Or equivalently

$$H(X) \leqslant \mathbb{E}_X \log \frac{1}{q(X)}.$$

Example

Let X be a M-ary random variable. Let $q(x) = \frac{1}{M}$ then

$$H(X) \leqslant \mathbb{E}_X \log M = \log M.$$

Back To Guessing

Fix $G(X) = G$. We need to choose $q(X)$ such that $\log \frac{1}{q(x)} = ax + b$ that is $q(x) = c_\gamma \gamma^x$ where $c_\gamma = \left(\sum_{x=1}^M \gamma^x\right)^{-1}$. Let $\gamma \in (0, 1]$ so that $q(x)$ deacreases wrt x then

$$H(X) \leqslant -\mathbb{E}_X \log(c_\gamma \gamma^x) = -\log c_\gamma - \gamma \mathbb{E}_X X = \log \left(\sum_{x=1}^{M} \gamma^x \right) - \gamma G.$$

Since the bound is linear it directly extends to the conditional case :

$$H(X|Y) \leqslant \log \left(\sum_{x=1}^{M} \gamma^x \right) - \gamma G(X|Y).$$

1. If $\gamma = 1$, q is the uniform distribution and $H(Q) = \log M$
2. As $\gamma \to 0$, q is a Dirac and $H(Q) \to 0$

Back to Guessing II

Equality is achived in the inequality when $X|Y = y \sim q$ for every y in which case

$$H(X|Y) = -\sum_{x=1}^{M} c_\gamma \gamma^x \log\left(c_\gamma \gamma^x\right) \tag{5}$$

$$= -\sum_{x=1}^{M} c_\gamma \gamma^x \log c_\gamma - \sum_{x=1}^{M} c_\gamma \gamma^x \log \gamma^x \tag{6}$$

$$= -\log c_\gamma - c_\gamma \log \gamma \sum_{x=1}^{M} \gamma^x x \tag{7}$$

Now

$$c_\gamma = \gamma \frac{1-\gamma^M}{1-\gamma} \quad \text{and} \quad \sum_{x=1}^{M} \gamma^x x = \frac{\gamma(1-\gamma^M)}{(1-\gamma)^2} + M\frac{\gamma^{M+1}}{1-\gamma}. \tag{8}$$

Back to Guessing III

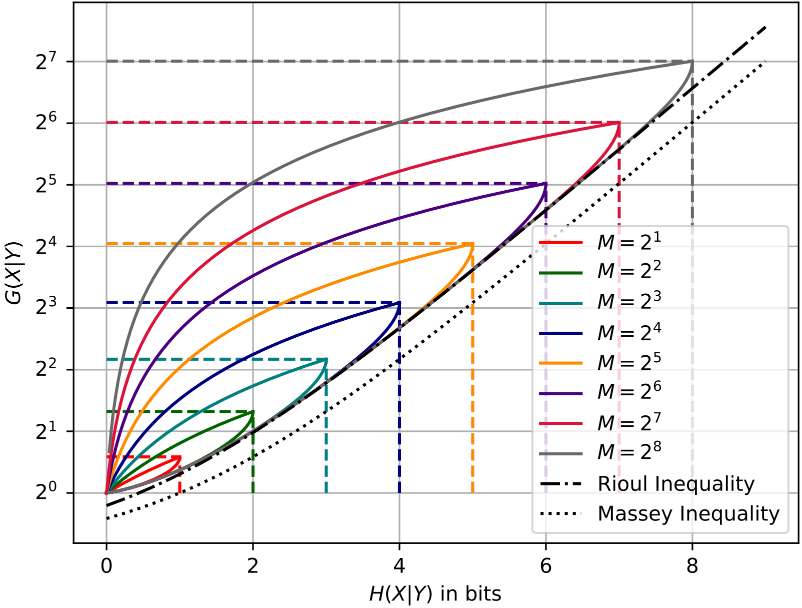
Theorem

The lower bound on $G(X|Y)$ vs. $H(X|Y)$ is given by the parametric curve for $\gamma \in (0,1)$:

$$\begin{cases} G(X|Y) = \frac{1}{1-\gamma} - \frac{M\gamma^M}{1-\gamma^M} H(X|Y) = \log(\gamma \frac{1-\gamma^M}{1-\gamma}) \\ -(\log\gamma)(\frac{1}{1-\gamma} - \frac{M\gamma^M}{1-\gamma^M}) \end{cases} \tag{9}$$

The parametric curve can be reparametrized for $-\frac{1}{2}\ln\gamma \triangleq \mu \in (0,+\infty)$:

$$\begin{cases} \frac{M+1}{2} - G(X|Y) = \frac{1}{2}\Big(M\coth(M\mu) - \coth(\mu)\Big) \\ \log M - H(X|Y) = \log\frac{M\sinh\mu}{\sinh(M\mu)} + 2\mu(\log e)(\frac{M+1}{2} - G(X|Y)). \end{cases} \tag{10}$$



2^7
2^6
2^5
2^4
2^3
2^2
2^1
2^0
$G(X|Y)$
0
2
4
6
8
$H(X|Y)$ in bits
$M = 2^1$
$M = 2^2$
$M = 2^3$
$M = 2^4$
$M = 2^5$
$M = 2^6$
$M = 2^7$
$M = 2^8$
Rioul Inequality
Massey Inequality

Guessing Moments

Let $\rho > 0$, the ρ-th guessing momment is given by

$$G_\rho(X) = \min_{\sigma \in \mathcal{S}_M} \sum_{i=1}^{M} \sigma(i)^\rho p_i = \sum_{i=1}^{M} i^\rho p_i.$$

This time we need $\log q(x) = ax^\rho + b$. That is $q(x) = c_\gamma \gamma^{x^\rho}$ where $c_\gamma^{-1} = \sum_{x=1}^M \gamma^{x^\rho}$ and $\gamma \in (0,1]$. q decreases with respect to x, if $\gamma = 1$ it is uniform and as $\gamma \to 0$ it approaches the Dirac distribution.

Theorem

The optimal lower bound of $G_\rho(X|Y)$ vs. $H(X|Y)$ is given by the parametric curve for $\gamma \in (0,1]$:

$$\begin{cases} G_\rho(X|Y) = (\sum_{i=1}^M i^\rho \gamma^{i^\rho})(\sum_{i=1}^M \gamma^{i^\rho})^{-1} \\ H(X|Y) = \log(\sum_{i=1}^M \gamma^{i^\rho}) - (\log \gamma)\frac{\sum_{i=1}^M i^\rho \gamma^{i^\rho}}{\sum_{i=1}^M \gamma^{i^\rho}} \end{cases} \quad (11)$$

Arimoto α-Equivocation and Sibson's α-Information

Let $\alpha > 0$, $\alpha \neq 1$, α' the Hölder conjugate ($\frac{1}{\alpha} + \frac{1}{\alpha'} = 1$),

$$H_\alpha(X|Y) = -\alpha' \log \underbrace{\mathbb{E}_Y \|P_{X|Y}\|_\alpha}_{K_\alpha(X|Y)} = -\alpha' \log \sum_y P_Y(y) \left(\sum_x P_{X|Y}(x|y)^\alpha \right)^{\frac{1}{\alpha}}$$

$$I_\alpha(X;Y) = \alpha' \log \mathbb{E}_Y \langle P_{X|Y} \| P_X \rangle = \alpha' \log \mathbb{E}_Y \left(\sum_x P_{X|Y}^\alpha(x|y) P_X(x)^{1-\alpha} \right)^{\frac{1}{\alpha}}$$

$$I_\alpha(K;Y) = \log M - H_\alpha(K|Y) = \log M - \sum_{i=1}^r H_\alpha(K_i|Y_i)$$

Also

$$I_\alpha(K;Y^m) \leqslant m I_\alpha(X;Y).$$

Existing Bounds

The upper bound is due to Serder Bostaz (TIT'97) while the lower bound is due to Rioul (TIT'22) which slightly improves the original inequality of Arikan (TIT'96).

$$\frac{\exp H_{\frac{1}{2}}(K|Y)}{\ln(2M+1)} \leqslant G(X|Y) \leqslant \frac{1+\exp H_{\frac{1}{2}}(K|Y)}{2} \tag{12}$$

Arikan's inequality (An Inequality on Guessing and its Application to Sequential Decoding) is :

$$G_\rho(X|Y) \geqslant \frac{\exp(H_{\frac{1}{1+\rho}}(X|Y))}{(1+\ln M)^\rho}. \tag{13}$$

Rényi Divergence

Rényi Entropy Power and Normal Transport, O.Rioul, ISITA 2020

- Let P, Q be two distributions with respective pmf p, q. Rényi's divergence is positive

$$D_\alpha(P\|Q) = \frac{1}{\alpha - 1} \sum_x p(x)^\alpha q(x)^{1-\alpha} \geqslant 0.$$

Rényi Divergence

Rényi Entropy Power and Normal Transport, O.Rioul, ISITA 2020

- Let P, Q be two distributions with respective pmf p, q. Rényi's divergence is positive

$$D_\alpha(P\|Q) = \frac{1}{\alpha - 1} \sum_x p(x)^\alpha q(x)^{1-\alpha} \geqslant 0.$$

- Relative Rényi-entropy (Lapidoth and Pfister) is positive

$$\Delta_\alpha(P\|Q) = D_{\frac{1}{\alpha}}(P_\alpha \| Q_\alpha) \geqslant 0$$

where P_α, Q_α are α-escort distributions of P, Q (i.e. $P_\alpha = P^\alpha / \|P\|_\alpha^\alpha$).

Rényi Divergence

Rényi Entropy Power and Normal Transport, O.Rioul, ISITA 2020

- Let P, Q be two distributions with respective pmf p, q. Rényi's divergence is positive

$$D_\alpha(P\|Q) = \frac{1}{\alpha - 1} \sum_x p(x)^\alpha q(x)^{1-\alpha} \geqslant 0.$$

- Relative Rényi-entropy (Lapidoth and Pfister) is positive

$$\Delta_\alpha(P\|Q) = D_{\frac{1}{\alpha}}(P_\alpha\|Q_\alpha) \geqslant 0$$

where P_α, Q_α are α-escort distributions of P, Q (i.e. $P_\alpha = P^\alpha / \|P\|_\alpha^\alpha$).

- $$H_\alpha(X) = -\alpha' \log \mathbb{E}_X q_\alpha^{1/\alpha'}(X) - \Delta_\alpha(P_X\|Q) \leqslant -\alpha' \log \mathbb{E}_X q_\alpha^{1/\alpha'}(X).$$

α-Gibbs Inequality

Lemma (Generalized Gibbs Inequality)

For any pmf q,

$$H_\alpha(X) \leqslant -\alpha' \log \mathbb{E}_X q_\alpha^{1/\alpha'}(X) \tag{14}$$

with equality iff $p_X = q$. Here q_α is the escort distribution of q, defined by $q_\alpha(x) = q^\alpha(x)/\|q\|_\alpha^\alpha$.

Since $\frac{1}{\alpha} + \frac{1}{\alpha'} = 1$ we have $\frac{\alpha}{\alpha'} = \alpha - 1$. The distribution in Gibbs inequality depends on the relative position of α with respect to 1.
Now depending on the sign of α',

$$K_\alpha(X) \lesseqgtr \mathbb{E}_X q_\alpha^{1/\alpha'}(X)$$

which shows that it extends to the conditional setting.

$\alpha \in (0,1)$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^{\rho} + b$.

$\alpha \in (0, 1)$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^{\rho} + b$.
2. $q(x) = (ax^{\rho} + b)^{\frac{1}{\alpha-1}} = (ax^{\rho} + b)^{\alpha'-1}$.

$\alpha \in (0, 1)$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 < 0$ we want $ax^\rho + b$ to increase with x that is $a \geqslant 0$ and since $ax^\rho + b > 0$, $a > -b$.

$\alpha \in (0, 1)$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 < 0$ we want $ax^\rho + b$ to increase with x that is $a \geqslant 0$ and since $ax^\rho + b > 0$, $a > -b$.
4. $ax^\rho + b = a(x^\rho - 1) + a + b$

$\alpha \in (0, 1)$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^{\rho} + b$.
2. $q(x) = (ax^{\rho} + b)^{\frac{1}{\alpha-1}} = (ax^{\rho} + b)^{\alpha'-1}$.
3. Since $\alpha - 1 < 0$ we want $ax^{\rho} + b$ to increase with x that is $a \geqslant 0$ and since $ax^{\rho} + b > 0$, $a > -b$.
4. $ax^{\rho} + b = a(x^{\rho} - 1) + a + b$
5. $q(x) = (a + b)^{\alpha'-1}(\frac{a}{a+b}(x^{\rho} - 1) + 1)^{\alpha'-1}$

$\alpha \in (0,1)$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 < 0$ we want $ax^\rho + b$ to increase with x that is $a \geqslant 0$ and since $ax^\rho + b > 0$, $a > -b$.
4. $ax^\rho + b = a(x^\rho - 1) + a + b$
5. $q(x) = (a+b)^{\alpha'-1}(\frac{a}{a+b}(x^\rho - 1) + 1)^{\alpha'-1}$
6. $q(x) = c_\gamma(\gamma(x^\rho - 1) + 1)^{\alpha'-1}$ where $\gamma \in [0,\infty)$.

$\alpha \in (0, 1)$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 < 0$ we want $ax^\rho + b$ to increase with x that is $a \geqslant 0$ and since $ax^\rho + b > 0$, $a > -b$.
4. $ax^\rho + b = a(x^\rho - 1) + a + b$
5. $q(x) = (a+b)^{\alpha'-1}(\frac{a}{a+b}(x^\rho - 1) + 1)^{\alpha'-1}$
6. $q(x) = c_\gamma(\gamma(x^\rho - 1) + 1)^{\alpha'-1}$ where $\gamma \in [0, \infty)$.
7.

$$\begin{cases} G_\rho(X|Y) = 1 + \gamma^{-1}\left(\frac{\sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'}}{\sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'-1}} - 1\right) \\ H_\alpha(X|Y) = \alpha' \log \sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'-1} + (1-\alpha') \log \sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'}. \end{cases} \tag{15}$$

$\alpha > 1$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^{\rho} + b$.

$\alpha > 1$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^{\rho} + b$.
2. $q(x) = (ax^{\rho} + b)^{\frac{1}{\alpha-1}} = (ax^{\rho} + b)^{\alpha'-1}$.

$\alpha > 1$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 > 0$ we want $ax^\rho + b$ to decrease with x that is $b < 0$ and $a \geqslant -b$.

$\alpha > 1$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 > 0$ we want $ax^\rho + b$ to decrease with x that is $b < 0$ and $a \geqslant -b$.
4. $q(x) = b^{\alpha'-1}(\frac{a}{b}x^\rho + 1)_+^{\alpha'-1}$

$\alpha > 1$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 > 0$ we want $ax^\rho + b$ to decrease with x that is $b < 0$ and $a \geqslant -b$.
4. $q(x) = b^{\alpha'-1}(\frac{a}{b}x^\rho + 1)_+^{\alpha'-1}$
5. $q(x) = c_\gamma(1 - \gamma x^\rho)_+^{\alpha'-1}$ where $\gamma \in (0,1)$ and $x_+ = \max(x, 0)$.

$\alpha > 1$

1. We need $q^{\frac{\alpha}{\alpha'}}(x) = q^{\alpha-1}(x) = ax^\rho + b$.
2. $q(x) = (ax^\rho + b)^{\frac{1}{\alpha-1}} = (ax^\rho + b)^{\alpha'-1}$.
3. Since $\alpha - 1 > 0$ we want $ax^\rho + b$ to decrease with x that is $b < 0$ and $a \geqslant -b$.
4. $q(x) = b^{\alpha'-1}(\frac{a}{b}x^\rho + 1)_+^{\alpha'-1}$
5. $q(x) = c_\gamma(1 - \gamma x^\rho)_+^{\alpha'-1}$ where $\gamma \in (0,1)$ and $x_+ = \max(x,0)$.
6.
$$\begin{cases} G_\rho(X|Y) = \gamma^{-1}\big(1 - \frac{\sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'}}{\sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'-1}}\big) \\ H_\alpha(X|Y) = \alpha' \log \sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'-1} + (1-\alpha') \log \sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'} \end{cases} \tag{16}$$

General Statement

When $0 < \alpha < 1$, the optimal lower bound of $G_\rho(X|Y)$ vs. $H_\alpha(X|Y)$ is given by the parametric curve for $\gamma \in (0, \infty)$:

$$\begin{cases} G_\rho(X|Y) = 1 + \gamma^{-1}\big(\frac{\sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'}}{\sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'-1}} - 1\big) \\ H_\alpha(X|Y) = \alpha' \log \sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'-1} + (1-\alpha') \log \sum_{i=1}^M (1-\gamma+\gamma i^\rho)^{\alpha'}. \end{cases} \tag{17}$$

When $\alpha > 1$, the optimal lower bound of $G_\rho(X|Y)$ in terms of $H_\alpha(X|Y)$ is given by the parametric curve for $\gamma \in (0, 1)$:

$$\begin{cases} G_\rho(X|Y) = \gamma^{-1}\big(1 - \frac{\sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'}}{\sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'-1}}\big) \\ H_\alpha(X|Y) = \alpha' \log \sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'-1} + (1-\alpha') \log \sum_{i=1}^M (1-\gamma i^\rho)_+^{\alpha'} \end{cases}. \tag{18}$$

As an important consequence, an explicit first-order upper bound can be obtained, which is easy to compute for any adversary observing small leakages.

Corollary

As $I_\alpha(K;Y) \to 0$, up to first order,

$$G_\rho(K) - G_\rho(K|Y) \lesssim \sqrt{\frac{2(G_{2\rho}(M) - G_\rho^2(M))}{\alpha}} \sqrt{\frac{I_\alpha(K;Y)}{\log e}}. \quad (19)$$

In particular, $G_\rho(K) - G_\rho(K|Y) \lesssim \sqrt{\frac{M^2-1}{6\alpha}}\sqrt{\frac{I(K;Y)}{\log e}}$.

Démonstration.

Taylor expansion about $\gamma = 0$ gives

$$\begin{cases} G_\rho(K) - G_\rho(K|Y) = \gamma|1-\alpha'|(G_{2\rho}(M) - G_\rho^2(M)) + O(\gamma^2) \\ \frac{I_\alpha(K;Y)}{\log e} = \frac{|\alpha'(1-\alpha')|}{2}(G_{2\rho}(M) - G_\rho^2(M))\gamma^2 + O(\gamma^3) \end{cases} \quad (20)$$

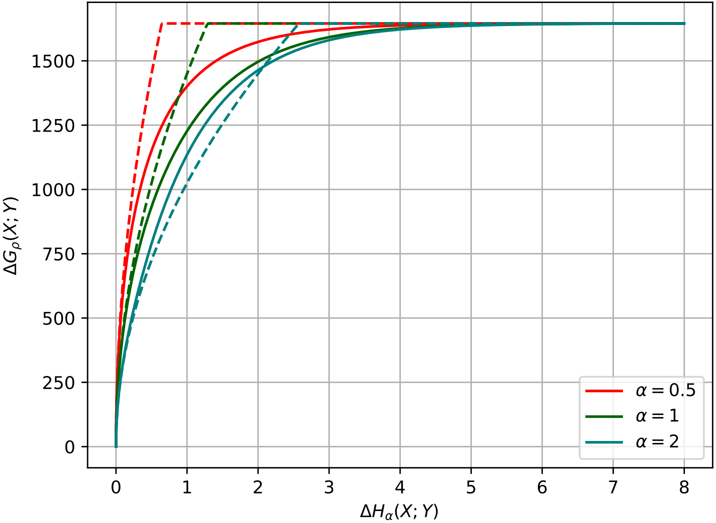


Figure – Validation of the Corollary

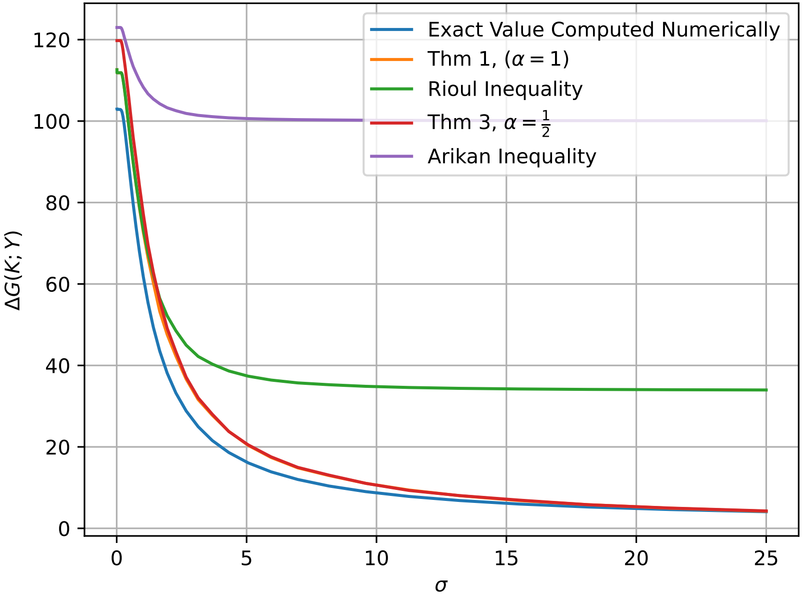


Figure – Hamming weight of a byte leak perturabated by additive Gaussian noise.

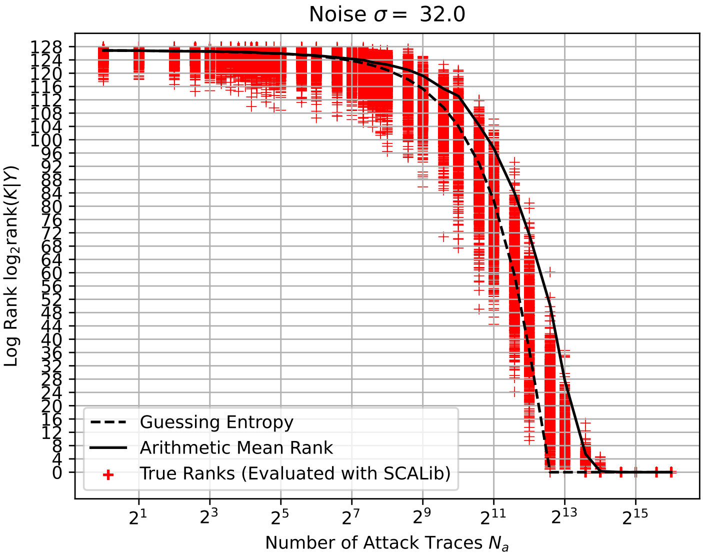
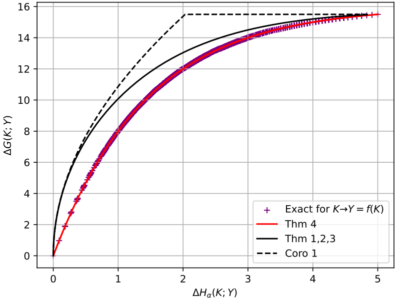


Figure – Hamming Weight of each bytes leak perturbated by addtive Gaussian noise. Increa
number of measurents and fixed noise level.

Random Probing Model

If $K \to Y = (Z, f_Z(K))$ where $\{f_z | z \in \mathcal{Z}\}$ is a given set of function then we can obtain an equality in terms of guessing advantage given by :

$$G(K) - G(K|Y) = \frac{M}{2}(1 - \exp(-I_{\frac{1}{2}}(K;Y))) \approx \frac{M}{2} I_{\frac{1}{2}}(K;Y). \quad (21)$$



Any Question ?

What Can Information Guess ?

Julien Béguinot, Olivier Rioul

LTCI, Télécom Paris, Institut Polytechnique de Paris

https://arxiv.org/pdf/2401.17057