Evaluation of Side-Channel Attacks Using α-Information

CryptArchi Workshop 2022

Yi Liu[1], Wei Cheng[2,1], Sylvain Guilley[2,1], and Olivier Rioul[1]

[1]Télécom Paris, IP Paris; [2]Secure-IC

May 31st, 2022

Outline

Outline

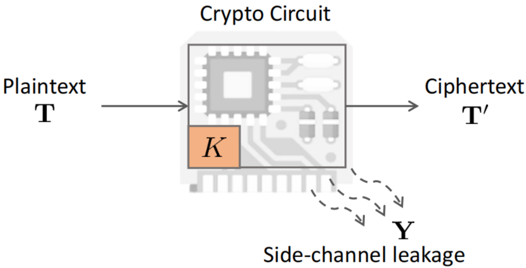
Motivation

α-Information Theory

Evaluation of Side-Channel Attacks

Motivation

- Side-Channel Attacks:



- **Information-theoretic tools** have been frequently used in the side-channel analysis.

Motivation

Chérisey et al. (CHES'19) establish some universal inequalities between **the probability of success** of a side-channel attack and **the minimum number of queries** to reach a given success rate.

This result is:

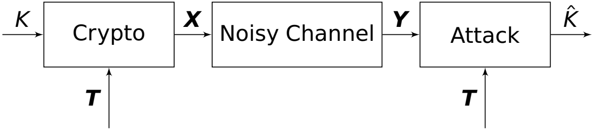
- valid for **any** leakage model, **any** kind of attack.
- with the best possible knowledge on the attacker's side.

They mainly use two information measures:

- **Mutual Information**: $I(K;Y) = \mathbb{E}_Y \sum_k p(k|y) \log \frac{p(k|y)}{p(k)}$
  (k: the secret, y: the leakage.)
- **Bianry Divergence**: $d(p\|q) = p \log \frac{p}{q} + (1-p) \log \frac{1-p}{1-q}$
  (where p, q are two probability distributions.)

TELECOM Paris

Side-Channel Model



- K: a secret key; normally we assume $K \sim \mathcal{U}(M)$;
- $\boldsymbol{T} = (T_1, T_2, \ldots, T_q)$: a q-element vector, each element T_i is a plain or cypher text;
- $\boldsymbol{X} = (X_1, X_2, \ldots, X_q)$: the output of the side-channel; the leakage function $\boldsymbol{X} = f(K, \boldsymbol{T})$ is deterministic;
- $\boldsymbol{Y} = (Y_1, Y_2, \ldots, Y_q)$: traces measured by the attacker;
- $\hat{K}$: the guess of the secret key;
- $\mathbb{P}_S$: the probability of success, defined as $\mathbb{P}_S = \mathbb{P}(K = \hat{K})$; it's different from **success rate**.

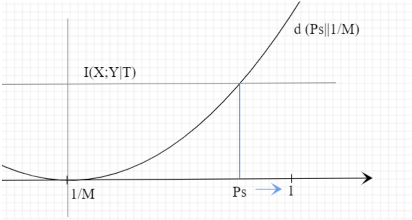
Evaluation of Side-Channel Attack

Main Theorem

One has the following upper bound on the probability of success $\mathbb{P}_s$:

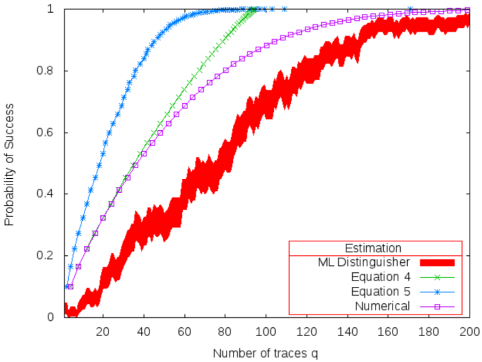
$$I(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{T}) \geq d(\mathbb{P}_s \| \frac{1}{M})$$

- As shown in the following figure, $d(\mathbb{P}_s \| \frac{1}{M})$ is increasing in $\mathbb{P}_s$. Hence this inequality gives an upper bound on $\mathbb{P}_S$ when $\mathbb{P}_S \geq 1/M$.



- One can evaluate $\mathbb{P}_s$ by calculating the numerical value of $I(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{T})$.

Bounds on Probability of Success



In this figure(Chérisey et al., CHES'19):

- the purple line: the numerical value of $I(X, Y|T)$;
- the blue and green lines: some explicit formula bounds.
- ML distinguisher is optimal if leakage modle is known.

Properties

To prove the main theorem, the following properties of mutual information turn out to be essential:

- **Conditional Consistency (CC):** If T is independent of (X, Y) then
$$I(X; Y|T) = I(X; Y)$$
- **Uniform Expansion Property (UEP):** If $K \sim \mathcal{U}(M)$ and it is independent of T, then
$$I(K; Y|T) = H(K) - H(K|YT) = \log M - H(K|YT)$$
- **Data Processing Inequality (DPI):** If $W - X - Y - Z$ forms a conditional Markov chain given T, then
$$I(X; Y|T) \geq I(W; Z|T)$$
- **Fano's Inequality**: $H(K|\hat{K}) \leq H_2(\mathbb{P}_e) + \mathbb{P}_e \log_2(M-1)$
$$\iff \qquad I(K; \hat{K}) \geq d(\mathbb{P}_s \| \frac{1}{M})$$

Objective

Our aims:

- make it more flexible by introducing a Rényi parameter α;
- extend the work of Chérisey et al. to α-information quantities depending on a parameter α;
- obtain tighter bounds by changing the value of α.

$\Longrightarrow$ need an appropriate definition of $I_\alpha(X;Y|T)$ with four properties :

CC + UEP + DPI + Fano's inequality

Outline

TELECOM Paris

α-Information Theory

Let p, q be two probability distributions. We use the following notations:

$$\|p\|_\alpha = \left(\sum p^\alpha\right)^{1/\alpha}$$

$$\langle p\|q\rangle_\alpha = \left(\sum p^\alpha q^{1-\alpha}\right)^{1/\alpha}$$

- **α-entropy** (Rényi, 1961):

$$H_\alpha(P) = \tfrac{\alpha}{1-\alpha} \log \|p\|_\alpha$$

- **α-divergence** (Rényi, 1961):

$$D_\alpha(P\|Q) = \tfrac{1}{\alpha-1} \log \langle p\|q\rangle_\alpha^\alpha$$

α-Information Theory

Their conditional versions:

- **Conditional α-entropy** (Arimoto, 1975):

$$H_\alpha(X|Y) = \frac{\alpha}{1-\alpha} \log \mathbb{E}_Y \|p_{X|Y}\|_\alpha$$

- **Conditional α-divergence** (Verdú,2015):

$$D_\alpha(P_{Y|X}\|Q_{Y|X}|P_X) = \frac{1}{\alpha-1} \log \mathbb{E}_X \langle p_{Y|X}\|q_{Y|X}\rangle_\alpha^\alpha$$

Among several definitions of α-information, Sibson's proposal seems to be the most appropriate one (Verdú,2015).

- **α-information** (Sibson, 1969):

$$I_\alpha(X;Y) = \frac{\alpha}{\alpha-1} \log \mathbb{E}_Y \langle p_{X|Y}\|p_X\rangle_\alpha$$

- **Conditional α-information** (Liu et al., ITW'21): our proposal of conditional α-information is

$$I_\alpha(X;Y|Z) = \frac{\alpha}{\alpha-1} \log \mathbb{E}_Z \mathbb{E}_{Y|Z} \langle p_{X|YZ}\|p_{X|Z}\rangle_\alpha$$

Conditional α-Information

Among many proposed definitions in the literature, our definition is the only one that satisfies the following properties:

- **Conditional Consistency (CC):** If T is independent of (X, Y) then
$$I_\alpha(X; Y|T) = I_\alpha(X; Y)$$
- **Uniform Expansion Property (UEP):** If $K \sim \mathcal{U}(M)$ is uniformly distributed independent of T, then
$$I_\alpha(K; Y|T) = H_\alpha(K) - H_\alpha(K|YT) = \log M - H_\alpha(K|YT)$$
- **Data Processing Inequality (DPI):** If $W - X - Y - Z$ forms a conditional Markov chain given T, then
$$I_\alpha(X; Y|T) \geq I_\alpha(W; Z|T)$$
- **Rioul's Generalized Fano Inequality (GFI)** (Rioul, GSI'21):
$$I_\alpha(X; Y) \geq d_\alpha\big(\mathbb{P}_s(X|Y) \| \mathbb{P}_s(X)\big)$$

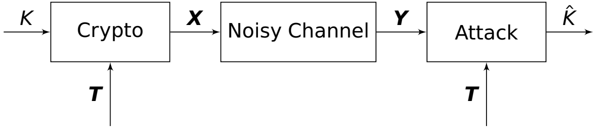
Outline

Motivation

α-Information Theory

Evaluation of Side-Channel Attacks

Evaluation of Side-Channel Attack



Theorem (Upper Bound on $\mathbb{P}_s$)

One has the following upper bound on the probability of success $\mathbb{P}_s$:

$$I_\alpha(\boldsymbol{X}, \boldsymbol{Y} | \boldsymbol{T}) \geq d_\alpha(\mathbb{P}_s \| \frac{1}{M})$$

Evaluation of Side-Channel Attack

Proof.

Because $K - \boldsymbol{X} - \boldsymbol{Y}$ is a Markov chain given $\boldsymbol{T}$,

$$I_\alpha(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{T}) \geq I_\alpha(K, \boldsymbol{Y}|\boldsymbol{T}) \qquad \textbf{(DPI)}$$

Because $\boldsymbol{X}$ is a deterministic function of K and $\boldsymbol{T}$, $\boldsymbol{X} - K - \boldsymbol{Y}$ is a Markov chains given $\boldsymbol{T}$, which gives us

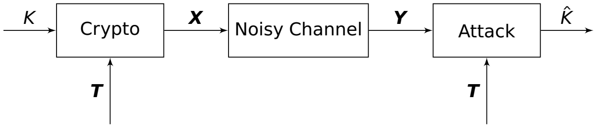
$$I_\alpha(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{T}) \leq I_\alpha(K, \boldsymbol{Y}|\boldsymbol{T}) \qquad \textbf{(DPI)}$$

So $I_\alpha(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{T}) = I_\alpha(K, \boldsymbol{Y}|\boldsymbol{T})$. Then one has

$$\begin{aligned}
I_\alpha(\boldsymbol{X}, \boldsymbol{Y}|\boldsymbol{T}) = I_\alpha(K, \boldsymbol{Y}|\boldsymbol{T}) &\geq I_\alpha(K; \hat{K}|\boldsymbol{T}) && \textbf{(DPI)} \\
&= \log M - H_\alpha(K|\hat{K}, \boldsymbol{T}) && \textbf{(UEP)} \\
&\geq \log M - H_\alpha(K|\hat{K}) && (*) \\
&= I_\alpha(K, \hat{K}) && \textbf{(UEP)} \\
&\geq d_\alpha(\mathbb{P}_s(K|\boldsymbol{Y}) \| \mathbb{P}_s(K)) && \textbf{(GFI)}
\end{aligned}$$

$*$: condition reduce α-entropy. □

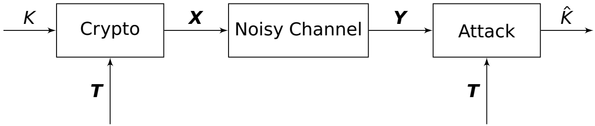
Evaluation of Side-Channel Attack



Theorem (Upper Bound on $\mathbb{P}_s$)

$$I_\alpha(\boldsymbol{X}, \boldsymbol{Y} | \boldsymbol{T}) \geq d_\alpha(\mathbb{P}_s \| \frac{1}{M})$$

Evaluation of Side-Channel Attack



Theorem (Upper Bound on $\mathbb{P}_s$)

$$I_\alpha(\boldsymbol{X},\boldsymbol{Y}|\boldsymbol{T}) \geq d_\alpha(\mathbb{P}_s\|\frac{1}{M})$$

We consider an **implementation of the AES**, with the **Hamming weight leakage model** and **additive white Gaussian noise (AWGN) channel**.

$$\boldsymbol{Y} = \boldsymbol{X} + \boldsymbol{N} = w_H(S(\boldsymbol{T} \oplus K)) + \boldsymbol{N} \qquad (i = 1, 2, \ldots, q) \tag{1}$$

- w_H: the Hamming weight
- S: an S-box permutation
- $\mathbf{N} = (N_1, \ldots, N_q)$, N_i are i.i.d $\sim \mathcal{N}(0, \sigma^2)$

Numerical Simulations

$$\boldsymbol{Y} = w_H(S(\boldsymbol{T} \oplus K)) + \boldsymbol{N} \qquad (i = 1, 2, \ldots, q)$$

Aim: compute

$$I_\alpha(\mathbf{X}, \mathbf{Y}|\mathbf{T}) = I_\alpha(K, \mathbf{Y}|\mathbf{T}) = \frac{\alpha}{\alpha - 1} \log \mathbb{E}_{\boldsymbol{T}} \mathbb{E}_{\boldsymbol{Y}|\boldsymbol{T}} \Big(\sum_k p_{K|\boldsymbol{YT}}^{\alpha} p_{K|\boldsymbol{T}}^{1-\alpha} \Big)^{\frac{1}{\alpha}} \tag{2}$$

We compute $I_\alpha(\mathbf{X}, \mathbf{Y}|\mathbf{T})$ using **Monte Carlo simulation**.

Monte Carlo methods rely on **repeated random sampling** to obtain numerical results.

By the law of large numbers, **integrals described by the expected value of some random variable** can be approximated by taking the empirical mean (a.k.a. the sample mean) of independent samples of the variable.

Numerical Simulations

$I_\alpha(\mathbf{X},\mathbf{Y}|\mathbf{T})$ can be writen as

$$I_\alpha(\mathbf{X},\mathbf{Y}|\mathbf{T}) = \frac{\alpha}{\alpha-1}\log\left(\mathbb{E}_{YT}\frac{\left(\sum_k p(k|\mathbf{t})p^\alpha(\mathbf{y}|\mathbf{t},k)\right)^{\frac{1}{\alpha}}}{p(\mathbf{y}|\mathbf{t})}\right). \tag{3}$$

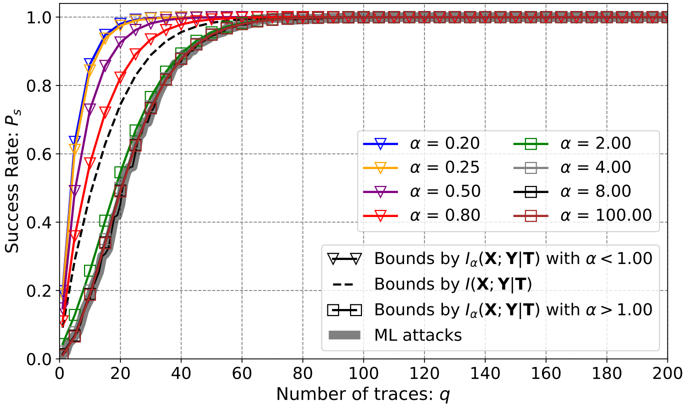
Therefore, it can be estimated by using Monte-Carlo simulation in the following way:

$$\begin{aligned}\exp\left(\frac{\alpha-1}{\alpha}I_\alpha(\mathbf{X},\mathbf{Y}|\mathbf{T})\right) &\approx \lim_{N_C\to\infty}\frac{1}{N_C}\sum_{j=1}^{N_C}\frac{\left(\sum_k p(k|\mathbf{t}^j)p^\alpha(\mathbf{y}^j|\mathbf{t}^j,k)\right)^{\frac{1}{\alpha}}}{p(\mathbf{y}^j|\mathbf{t}^j)}\\ &= \lim_{N_C\to\infty}\frac{1}{N_C}\sum_{j=1}^{N_C}\frac{\left(\sum_k p(k)p^\alpha(\mathbf{y}^j|\mathbf{t}^j,k)\right)^{\frac{1}{\alpha}}}{\sum_k p(k)p(\mathbf{y}^j|\mathbf{t}^j,k)},\end{aligned}$$

where $\mathbf{t}^j \sim \mathcal{U}(\mathbb{F}_{2^8}^q)$ and $\mathbf{y}^j \sim \mathcal{N}(f(\mathbf{t}^j,k^j),\sigma^2\mathbf{I}_q) \in \mathbb{R}^q$ by choosing $k^j \sim \mathcal{U}(\mathbb{F}_{2^8})$ and $f(\mathbf{t}^j,k^j) = w_H(S(\mathbf{t}^j \oplus k^j))$.

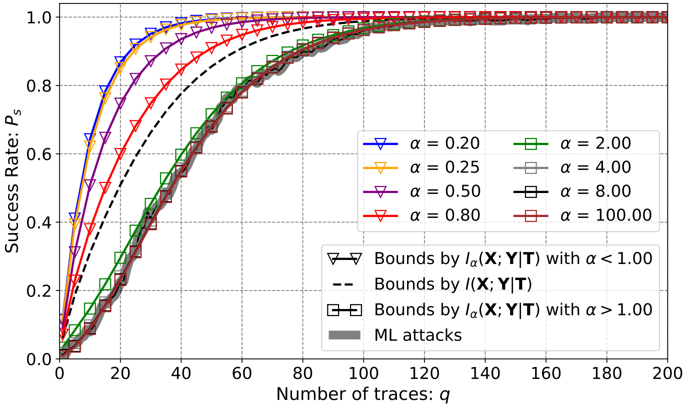
TELECOM Paris

Numerical Result



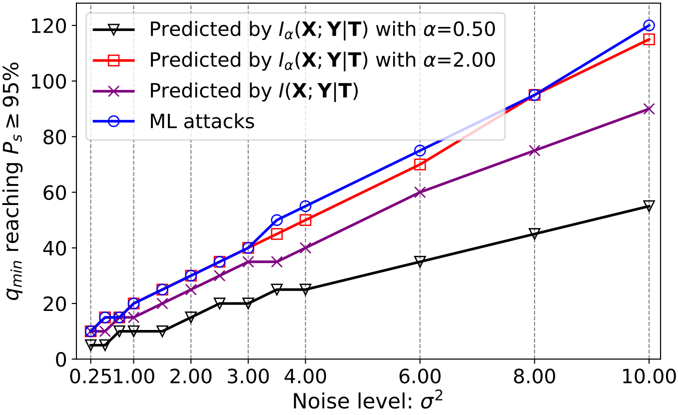
Noise level: $\sigma = 4$.

Numerical Result

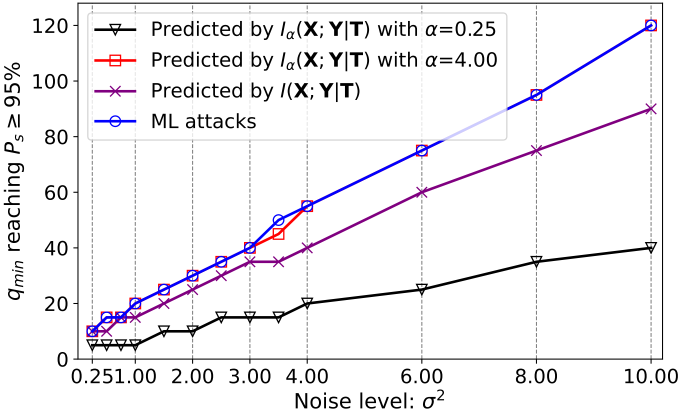


Noise level: $\sigma = 8$

Numerical Result



Numerical Result



Evaluation of Side-Channel Attacks Using α-Information

CryptArchi Workshop 2022

Thanks for your attention!

Yi Liu[1], Wei Cheng[2,1], Sylvain Guilley[2,1], and Olivier Rioul[1]

[1]Télécom Paris, IP Paris; [2]Secure-IC

May 31st, 2022