Best Information is Most Successful

CHES, Atlanta, GA, USA,

Aug 27, 2019

Authors

Éloi de Chérisey — TELECOM Paris, IP PARIS

Sylvain Guilley — SECURE-IC THE SECURITY SCIENCE COMPANY, TELECOM Paris, IP PARIS

Olivier Rioul — TELECOM Paris, IP PARIS

Pablo Piantanida — CentraleSupélec

Setup ....remember CHES 2014 [HRG14]?

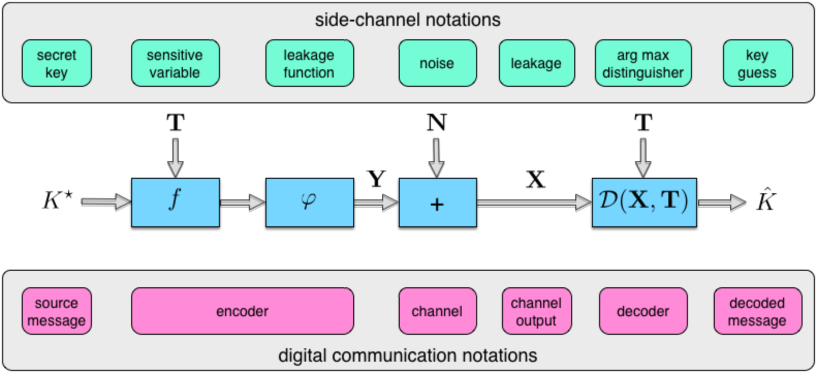
Good Is Not Good Enough

Deriving Optimal Distinguishers from Communication Theory

Annelie Heuser[1⋆], Olivier Rioul[1], and Sylvain Guilley[1,2]

[1] Télécom ParisTech, Institut Mines-Télécom, CNRS LTCI,
Department Comelec46 rue Barrault, 75 634 Paris Cedex 13, France
firstname.lastname@telecom-paristech.fr
[2] Secure-IC S.A.S.,
80 avenue des Buttes de Coësmes, 35 700 Rennes, France

Setup . . . . remember CHES 2014 [HRG14]?



Side-Channel Analysis Setup

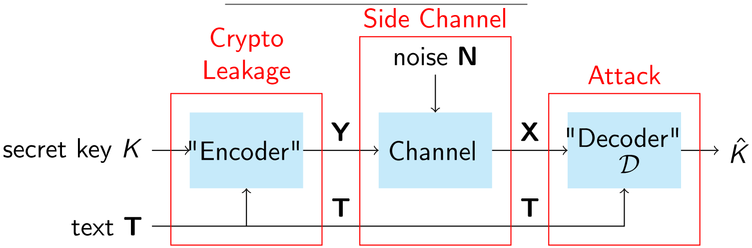


Figure: Side-channel leakage seen as a communication channel

The attacker makes q queries $\mathbf{X} = (X_1, \ldots, X_q)$ which depend on the secret K and on the text $\mathbf{T}$ through a sensitive variable $\mathbf{Y}$, and estimates the secret using a *distinguisher* $\hat{K} = \mathcal{D}(\mathbf{X}, \mathbf{T})$.

Side-Channel Analysis Setup

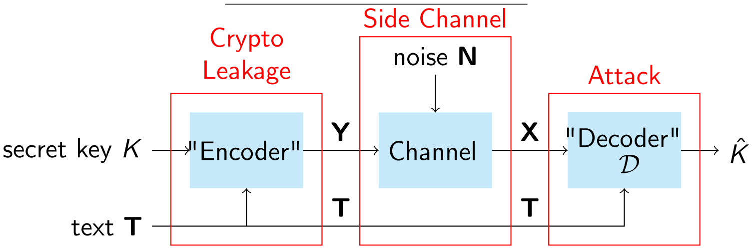
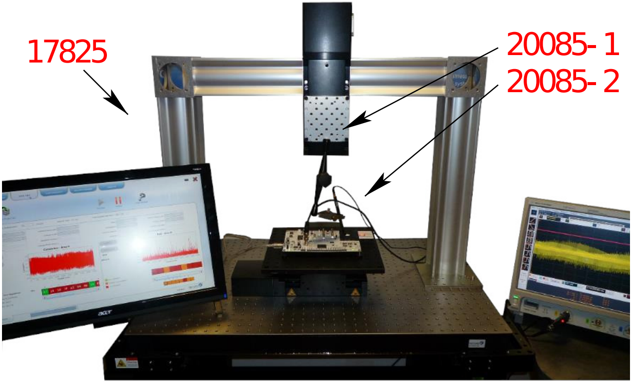


Figure: Side-channel leakage seen as a communication channel

The attacker makes q queries $\mathbf{X} = (X_1, \ldots, X_q)$ which depend on the secret K and on the text $\mathbf{T}$ through a sensitive variable $\mathbf{Y}$, and estimates the secret using a *distinguisher* $\hat{K} = \mathcal{D}(\mathbf{X}, \mathbf{T})$.

- any noisy measurement channel;
- *countermeasures* can protect $\mathbf{Y}$ = random funct. of $(K, \mathbf{T})$.

Test and evaluation tool (ISO/IEC 19790 & 15408)



Catalyzr®, Virtualyzr®, Analyzr® tools.

Best attack (MAP, ML)

The best distinguisher maximizes likelihood for uniformly distributed K [HRG14]:

$$\hat{K} = \mathcal{D}(\mathbf{X}, \mathbf{T}) = \arg\max_{k \in \mathcal{K}} \mathbb{P}(\mathbf{X} | \mathbf{T}, k) \qquad \text{where } \mathbf{X} = \text{noisy } \mathbf{Y}$$

Side-Channel Attacks on Hardware

Best attack (MAP, ML)

The best distinguisher maximizes likelihood for uniformly distributed K [HRG14]:

$$\hat{K} = \mathcal{D}(\mathbf{X}, \mathbf{T}) = \arg\max_{k \in \mathcal{K}} \mathbb{P}(\mathbf{X} | \mathbf{T}, k) \qquad \text{where } \mathbf{X} = \text{noisy } \mathbf{Y}$$

- This is a *template* attack which requires estimation of unknown conditional distributions with a leakage *model*, e.g.,

$$\mathbf{Y}(K, \mathbf{T}) = w_H\big(\mathrm{S}_{\text{box}}(\mathbf{T} \oplus K)\big) \qquad (\textit{unprotected})$$

$$\mathbf{Y}(K, \mathbf{T}) = \Big[w_H\big(\mathrm{S}_{\text{box}}(\mathbf{T} \oplus K) \oplus \mathbf{M}\big), w_H(\mathbf{M})\Big] \qquad (\textit{masked})$$

Side-Channel Attacks on Hardware

Best attack (MAP, ML)

The best distinguisher maximizes likelihood for uniformly distributed K [HRG14]:

$$\hat{K} = \mathcal{D}(\mathbf{X}, \mathbf{T}) = \arg\max_{k \in \mathcal{K}} \mathbb{P}(\mathbf{X} | \mathbf{T}, k) \qquad \text{where } \mathbf{X} = \text{noisy } \mathbf{Y}$$

- This is a *template* attack which requires estimation of unknown conditional distributions with a leakage *model*, e.g.,

$$\mathbf{Y}(K, \mathbf{T}) = w_H\left(\mathrm{S}_{\text{box}}(\mathbf{T} \oplus K)\right) \qquad (\textit{unprotected})$$

$$\mathbf{Y}(K, \mathbf{T}) = \left[w_H\left(\mathrm{S}_{\text{box}}(\mathbf{T} \oplus K) \oplus \mathbf{M}\right), w_H(\mathbf{M})\right] \qquad (\textit{masked})$$

- Many practical attacks exist (CPA, MIA, KSA, M. Learning)

Side-Channel Attacks on Hardware

Best attack (MAP, ML)

The best distinguisher maximizes likelihood for uniformly distributed K [HRG14]:

$$\hat{K} = \mathcal{D}(\mathbf{X}, \mathbf{T}) = \arg\max_{k \in \mathcal{K}} \mathbb{P}(\mathbf{X} | \mathbf{T}, k) \qquad \text{where } \mathbf{X} = \text{noisy } \mathbf{Y}$$

- This is a *template* attack which requires estimation of unknown conditional distributions with a leakage *model*, e.g.,

$$\mathbf{Y}(K, \mathbf{T}) = w_H\big(\mathrm{S}_{\text{box}}(\mathbf{T} \oplus K)\big) \qquad (\textit{unprotected})$$

$$\mathbf{Y}(K, \mathbf{T}) = \Big[w_H\big(\mathrm{S}_{\text{box}}(\mathbf{T} \oplus K) \oplus \mathbf{M}\big), w_H(\mathbf{M})\Big] \qquad (\textit{masked})$$

- Many practical attacks exist (CPA, MIA, KSA, M. Learning)
- The attacker will eventually always succeed as $q \to \infty$.

The Defender (Chip Designer)'s Viewpoint

Question

Assuming any possible attack, possibly with an omniscient attacker, (which knows everything except K (Kerckhoffs principle), noise and masks)
what is the least number of queries to achieve a given key recovery success rate?

$$q(P_s) = \min\{q \quad \text{s.t.} \quad \mathbb{P}(\hat{K} = K) \geq P_s\}$$

The Defender (Chip Designer)'s Viewpoint

Question

Assuming any possible attack, possibly with an omniscient attacker, (which knows everything except K (Kerckhoffs principle), noise and masks)
what is the least number of queries to achieve a given key recovery success rate?

$$q(P_s) = \min\{q \quad \text{s.t.} \quad \mathbb{P}(\hat{K} = K) \geq P_s\}$$

Practical significance:

- *any* attacker with budget $< q(P_s)$ cannot recover the key with probability $> P_s$;
- when $q > q(P_s)$, there only *might* be an attack with success P_s.

Information Theoretic Background

Notations:

- H is Shannon entropy, e.g., $H(K) = n$ bit
- $H_2(p) = -p \log p - (1-p) \log(1-p)$ is the binary entropy
- $D(\mathbb{P}_A \| \mathbb{P}_B)$ is the Kullback-Leibler divergence
- $D_2(p_A \| p_B) = p_A \log \frac{p_A}{p_B} + (1-p_A) \log \frac{1-p_A}{1-p_B}$ binary divergence
- $I(A; B) = D(\mathbb{P}_{A,B} \| \mathbb{P}_A \otimes \mathbb{P}_B)$ is mutual info btw A and B
- $I(A; B \mid C)$ is mutual info btw A and B conditionned by C

DPI: Data Processing Inequality

- $A \to B \to C \to D : I(B; C) \geq I(A; D)$
- $\mathbb{P}_A \to \mathbb{Q}_A$ and $\mathbb{P}_B \to \mathbb{Q}_B$ for same processing: $D(\mathbb{P}_A \| \mathbb{P}_B) \geq D(\mathbb{Q}_A \| \mathbb{Q}_B)$

Application of Data Processing Inequality

First, we notice that:

$$
\begin{aligned}
I(K;\hat{K}) &= D(\mathbb{P}_{K,\hat{K}} \| \underbrace{\mathbb{P}_K \otimes \mathbb{P}_{\hat{K}}}_{K \perp\!\!\!\perp \hat{K}}) \\
&\geq D(\mathbb{P}(K=\hat{K}) \| \underbrace{\mathbb{P}'(K=\hat{K})}_{K \perp\!\!\!\perp \hat{K}}) \quad // \text{ DPI for } f:(K,\hat{K}) \mapsto \mathbf{1}_{K=\hat{K}} \\
&= \mathbb{P}_s \log \frac{\mathbb{P}_s}{1/2^n} + \mathbb{P}_e \log \frac{\mathbb{P}_e}{1-1/2^n} \\
&= n - H_2(\mathbb{P}_s) - \mathbb{P}_e \log(2^n - 1). \qquad // \text{ Fano's inequality}
\end{aligned}
$$

Since K—$\mathbf{Y}$—$\mathbf{X}$—$\hat{K}$ for a given $\mathbf{T}$ is a Markov chain:

$$I(K;\hat{K}) \leq I(\mathbf{X};\mathbf{Y} \mid \mathbf{T}). \qquad \square$$

Application of Data Processing Inequality

First, we notice that:

$$
\begin{aligned}
I(K;\hat{K}) &= D(\mathbb{P}_{K,\hat{K}} \| \underbrace{\mathbb{P}_K \otimes \mathbb{P}_{\hat{K}}}_{K \perp\!\!\!\perp \hat{K}}) \\
&\geq D_2(\mathbb{P}(K=\hat{K}) \| \underbrace{\mathbb{P}'(K=\hat{K})}_{K \perp\!\!\!\perp \hat{K}}) \quad \text{// DPI for } f:(K,\hat{K}) \mapsto \mathbf{1}_{K=\hat{K}} \\
&= \mathbb{P}_s \log \frac{\mathbb{P}_s}{1/2^n} + \mathbb{P}_e \log \frac{\mathbb{P}_e}{1-1/2^n} \\
&= n - H_2(\mathbb{P}_s) - \mathbb{P}_e \log(2^n - 1). \qquad \text{// Fano's inequality}
\end{aligned}
$$

Since K—$\mathbf{Y}$—$\mathbf{X}$—$\hat{K}$ for a given $\mathbf{T}$ is a Markov chain:

$$
I(K;\hat{K}) \leq I(\mathbf{X};\mathbf{Y} \mid \mathbf{T}).
$$

□

Fundamental Lower Bound on $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T})$

Proposition

For any n-bit key K:

$$n - H_2(\mathbb{P}_s) - (1 - \mathbb{P}_s)\log_2(2^n - 1) \le I(\mathbf{X};\mathbf{Y} \mid \mathbf{T}).$$

Fundamental Lower Bound on $I(\mathbf{X};\mathbf{Y}\mid\mathbf{T})$

Proposition

For any n-bit key K:

$$n - H_2(\mathbb{P}_s) - (1-\mathbb{P}_s)\log_2(2^n - 1) \leq I(\mathbf{X};\mathbf{Y}\mid\mathbf{T}).$$

- $I(\mathbf{X};\mathbf{Y}\mid\mathbf{T})$ depends on q

Fundamental Lower Bound on $I(\mathbf{X};\mathbf{Y}\mid\mathbf{T})$

Proposition

For any n-bit key K:

$$n - H_2(\mathbb{P}_s) - (1-\mathbb{P}_s)\log_2(2^n-1) \leq I(\mathbf{X};\mathbf{Y}\mid\mathbf{T}).$$

- $I(\mathbf{X};\mathbf{Y}\mid\mathbf{T})$ depends on q
- When $q=0$ (blind attacker) $I(\mathbf{X};\mathbf{Y}\mid\mathbf{T})=0$ and $\mathbb{P}_s = 1/2^n$.

Fundamental Lower Bound on $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T})$

Proposition

For any n-bit key K:

$$n - H_2(\mathbb{P}_s) - (1-\mathbb{P}_s)\log_2(2^n-1) \leq I(\mathbf{X};\mathbf{Y} \mid \mathbf{T}).$$

- $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T})$ depends on q
- When $q=0$ (blind attacker) $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T}) = 0$ and $\mathbb{P}_s = 1/2^n$.
- In the context of cryptanalysis, $\mathbb{P}_s$ should be high enough (divide and conquer approach, e.g., 16 bytes for AES [NIS01]). In such regime, Fano's inequality is fairly tight.

First Upper Bound on $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T})$

Linear Bound

For q queries:

$$I(\mathbf{X},\mathbf{Y} \mid \mathbf{T}) \leq q \cdot I(X;Y \mid T)$$

Proof.

Memoryless channel assumption. $\square$

- However, the same K is used q times (huge repetition !)

First Upper Bound on $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T})$

Linear Bound

For q queries:

$$I(\mathbf{X},\mathbf{Y} \mid \mathbf{T}) \leq q \cdot I(X;Y \mid T)$$

Proof.

Memoryless channel assumption. $\square$

- However, the same K is used q times (huge repetition !)
- Therefore, $I(\mathbf{X},\mathbf{Y} \mid \mathbf{T}) \leq H(\mathbf{Y}|\mathbf{T}) \leq H(K) = n$ should be bounded by n bits as $q \to +\infty$.

Second Upper Bound on $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T})$

Divergence Bound (novel non-trivial bound)

$$I(\mathbf{X};\mathbf{Y} \mid \mathbf{T}) \leq -\mathbb{E}_{\mathbf{T}}\mathbb{E}_K \log \mathbb{E}_{K'} \exp\left[-\mathrm{D}(\mathbb{P}_{\mathbf{X}|K,\mathbf{T}} \parallel \mathbb{P}_{\mathbf{X}|K',\mathbf{T}})\right]$$

where K' is an independent copy of K.

Proof.
Apply the (equivalent) inequalities

$$-\mathbb{E}_Y \log \mathbb{E}_X[\exp(f(X,Y))] \leq -\log \mathbb{E}_X[\exp(\mathbb{E}_Y f(X,Y))].$$

$$\exp \mathbb{E}_Y \log \mathbb{E}_X[g(X,Y)] \geq \mathbb{E}_X[\exp(\mathbb{E}_Y \log g(X,Y))] \qquad \square$$

This upper bound is **bounded** by n bits as $q \to \infty$.

Graphical Comparison

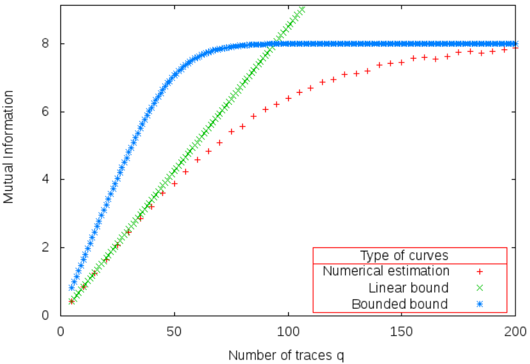


Figure: Mutual information $I(\mathbf{X};\mathbf{Y} \mid \mathbf{T}=\mathbf{t})$, where $\mathbf{t}$ is a fixed balanced vector. Comparison for $n = 8$, assuming Hamming weight leakage model in AES, AWGN with $\sigma = 4$.

Linear bound for AWGN 1/2

(Scalar) mutual info does not exceed Shannon channel's capacity:

$$I(X;Y \mid T) \leq \frac{1}{2}\log_2(1+\mathrm{SNR}).$$

Theorem (Lower bound for AWGN in terms of SNR)

To reach success $\mathbb{P}_s$, q should be at least

$$q \geq \frac{n + (\mathbb{P}_s - 1)\log_2(2^n - 1) - H_2(\mathbb{P}_s)}{\frac{1}{2}\log_2(1+\mathrm{SNR})}. \tag{1}$$

Linear bound for AWGN 2/2

The number of traces q needed to recover the key reliably is lower-bounded by:

$$\lim_{\mathbb{P}_s \to 1} q \geq \frac{n}{\frac{1}{2}\log_2(1+\mathrm{SNR})} \tag{2}$$

where SNR can be measured on the fly (for balanced text $\mathbf{T}$):

$$\mathsf{SNR} = \frac{\mathrm{Var}(\mathbb{E}[X \mid T])}{\mathrm{Var}(X) - \mathrm{Var}(\mathbb{E}[X \mid T])}. \tag{3}$$

No more leakage if SNR$\to 0$.

Divergence bound for AWGN 1/2

In the AWGN model, $\mathbb{P}_{\mathbf{X}|K_i,\mathbf{T}}$ follows a multivariate normal distribution $\mathcal{N}(\mathbf{y}(K_i,\mathbf{T}),\sigma^2 I_q)$.

$$\mathrm{D}(\mathbb{P}_{\mathbf{X}|K,\mathbf{T}}\|\mathbb{P}_{\mathbf{X}|K',\mathbf{T}}) = \frac{\|\mathbf{y}(K,\mathbf{T})-\mathbf{y}(K',\mathbf{T})\|_2^2}{2\sigma^2}.$$

Besides, for balanced $\mathbf{T}$:

$$\frac{1}{q}\left\|\frac{\mathbf{y}(k,\mathbf{t})-\mathbf{y}(k',\mathbf{t})}{2}\right\|_2^2 \xrightarrow[q\to\infty]{} \kappa(k,k'), \qquad // \text{ LLN}$$

where

$$\kappa(k,k') = \frac{1}{2^n}\sum_{t=0}^{2^n-1}\left(\frac{y(k,t)-y(k',t)}{2}\right)^2 \qquad \text{(confusion coefficient)}$$

Divergence bound for AWGN 2/2

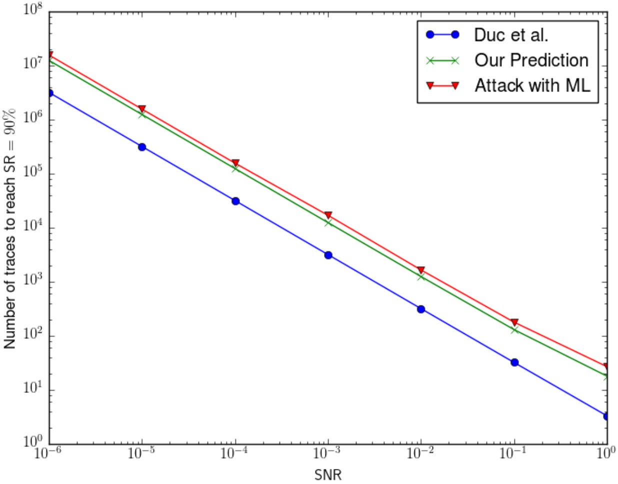
Implicit bound:

$$H_2(\mathbb{P}_s) + (1-\mathbb{P}_s)\log_2(2^n-1) \geq \frac{n_{\min}}{2^n}\exp\left(-\frac{q}{8}\frac{\min_{k\neq k'}\kappa(k,k')}{\sigma^2}\right).$$

where $n_{\min}$ is the number of ex aequo key pairs (k,k') such that $\kappa(k,k')$ is minimum.

Comparison with Duc et al. [DFS15]

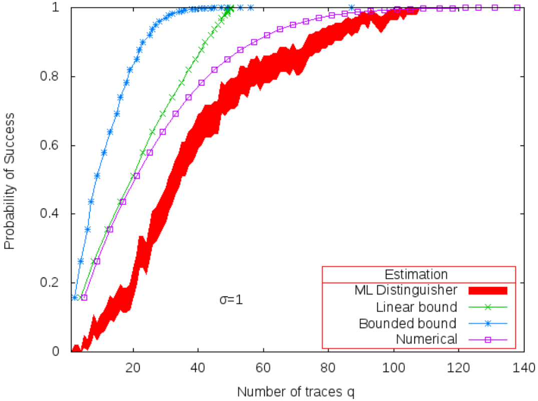
Making Masking Security Proofs Concrete (EC 2015, Duc, Faust, Standaert)



(Duc et al. use **Pinsker's inequality**)

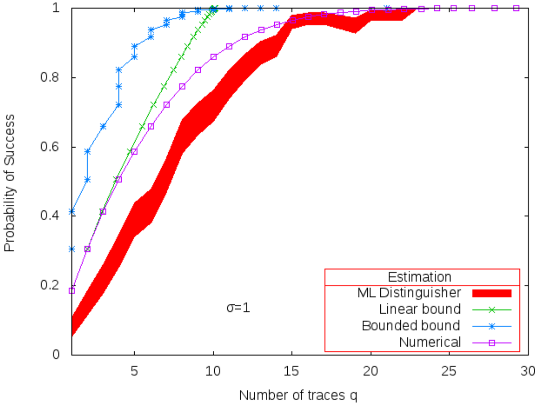
Simulation for Monobit Leakage

Monobit leakage model: $\mathbf{Y}(\mathbf{T}, K) = \mathrm{LSB}(\mathrm{S}_{\mathrm{box}}(\mathbf{T} \oplus K))$
where $\mathrm{S}_{\mathrm{box}}$ = AES substitution box and LSB = least significant bit.



Simulation for Hamming Weight Leakage

AES SubBytes based on bytes: $\mathbf{Y}(\mathbf{T}, K) = w_H(\mathrm{S}_{\mathrm{box}}(\mathbf{T} \oplus K))$
where $\mathrm{S}_{\mathrm{box}}$ = AES substitution box and w_H is the Hamming weight.



Conclusion

- We obtained *universal* bounds to the success probability in terms of mutual information, in the sense that they are independent of the channel and leakage models;
- Our results were presented within the specific framework of "power-line attacks" (e.g., monobit leakage or Hamming weight leakage);
- The resulting bounds were found to be empirically tight.

Announcements

Secure-IC recruits:

- R&D team director, based in Paris (10 people in Paris, Rennes, Singapour and Tokyo)
- Tokyo "Security Science Factory" laboratory manager

TELECOM-Paris recruits (Palaiseau, France):

- PhD candidate in IT-powered SCA
- Researcher in embedded security, in Jean-Luc Danger's team

Bibliographical references I

[DFS15] Alexandre Duc, Sebastian Faust, and François-Xavier Standaert.
Making Masking Security Proofs Concrete - Or How to Evaluate the Security of Any Leaking Device.
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 401–429. Springer, 2015.

Bibliographical references II

[HRG14] Annelie Heuser, Olivier Rioul, and Sylvain Guilley.
Good Is Not Good Enough - Deriving Optimal Distinguishers from Communication Theory.
In Lejla Batina and Matthew Robshaw, editors, *Cryptographic Hardware and Embedded Systems - CHES 2014 - 16th International Workshop, Busan, South Korea, September 23-26, 2014. Proceedings*, volume 8731 of *Lecture Notes in Computer Science*, pages 55–74. Springer, 2014.

[NIS01] NIST/ITL/CSD.
Advanced Encryption Standard (AES). FIPS PUB 197, Nov 2001.
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (also ISO/IEC 18033-3:2010).

Best Information is Most Successful

CHES, Atlanta, GA, USA,

Aug 27, 2019