Success Rate Exponents for Side-Channel Attacks

Sylvain GUILLEY
Annelie HEUSER
Martial REN
Olivier RIOUL
Simon SELLEM

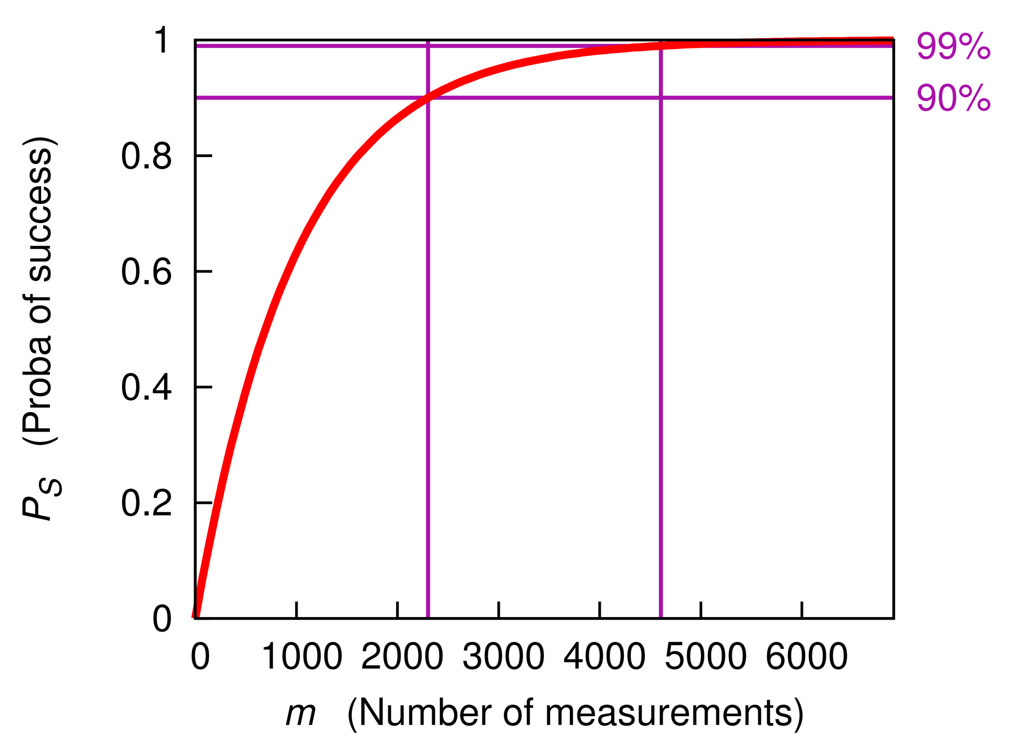
Goal

- Compute the exact probability of success $\mathbb{P}_S = \mathbb{P}(\hat{K} = K^\star)$
- Rigorous mathematical computation of its first order exponent of success rate:

$$\mathbb{P}_S \approx 1 - e^{-mE} \quad \text{for some } E\text{, where } m \text{ is the number of measurements.} \tag{1}$$

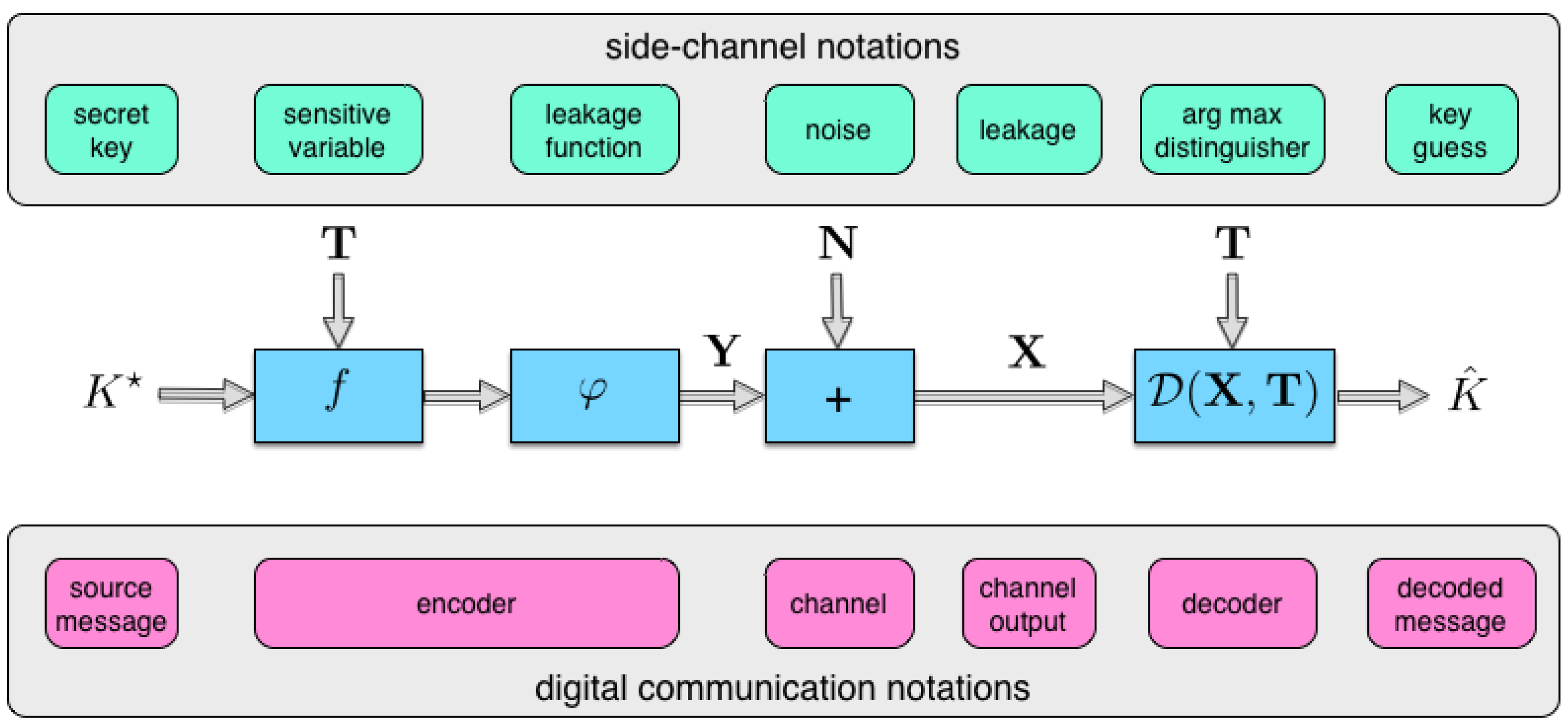
Example (with E independent of m)

- By Eq. (1), if $\mathbb{P}_S = 90\%$, then $m = \frac{\ln(10)}{E}$;
- Doubling the number of measurements $m \longrightarrow 2m \implies \mathbb{P}_S = 99\%$.



$(E = 10^{-3})$

Side-channel analysis as a communication channel [HRG14]



Useful concepts

Definition 1 (First-Order Exponent Equivalence)**.**
A sequence p_m of positive numbers admits a first-order exponent E_m if $\epsilon_m = E_m + \frac{1}{m}\ln p_m$ tends to zero as $m \longrightarrow +\infty$. In this case we write:

$$p_m \approx e^{-mE_m} \ .$$

In practice, "$m = 20$" is already "$m \longrightarrow +\infty$".

Result for Gaussian noise

When $Y = \alpha X(k) + N$, with $N \sim \mathcal{N}(0, \sigma^2)$ is the noise:

$$E = \frac{1}{8\sigma^2} \min_{k \neq k'} \mathbb{E}(Y(k) - Y(k'))^2 \tag{2}$$

$$= \frac{1}{2} \times \text{SNR} \times \min_{k \neq k'} \kappa_{k,k'} \ , \tag{3}$$

- where $\text{SNR} = \frac{\alpha^2}{\sigma^2}$, and
- where $\kappa_{k,k'} = \frac{1 - \rho(Y(k), Y(k'))}{2}$ is the confusion coefficient [FLD12].

Proof (for the optimal distinguisher when the noise is Gaussian, i.e., the opposite norm-2)

$$D_k^{\text{opt}}(\mathbf{x}, \mathbf{t}) = -\|\mathbf{x} - \mathbf{y}(k)\|_2 \ . \tag{4}$$

Nota bene: bold letters $\mathbf{x}$ *represent series:* $\mathbf{x} = (x_i)_{1 \leq i \leq m}$.

We define the *marginal pairwise probability of failure*:

$$\mathbb{P}_{k \to k' | \mathbf{t}} = \mathbb{P}(\|\mathbf{X} - \mathbf{Y}(k)\| \leq \|\mathbf{X} - \mathbf{Y}(k')\| \mid \mathbf{T} = \mathbf{t}) \ . \tag{5}$$

Lemma 1 (Q-expression of the Pairwise Failure Probability)**.**
Let $Q(x) = \frac{1}{2}\operatorname{erf}\left(\frac{x}{\sqrt{2}}\right) = \frac{1}{\sqrt{2\pi}}\int_x^{+\infty} e^{-t^2/2}\,dt$ *be the complementary cdf of a standard normal* $\mathcal{N}(0,1)$. *We have:*

$$\mathbb{P}_{k \to k' | \mathbf{t}} = Q\left(\frac{\|\mathbf{y}(k) - \mathbf{y}(k')\|}{2\sigma}\right) \ .$$

Lemma 2 (first-order Gaussian Q exponent)**.**
As $x \longrightarrow +\infty$, $Q(x) \lessapprox e^{-x^2/2}$, *in the sense that* $Q(x) \leq e^{-x^2/2}$ *for all* $x \geq 0$ *and* $\frac{\ln Q(x)}{x^2} \longrightarrow -\frac{1}{2}$.

Dominated convergence theorem: $\mathbb{E}[\ln \mathbb{P}_{k \to k' | \mathbf{T}} / m] \longrightarrow -\frac{\mathbb{E}(Y(k) - Y(k'))^2}{8\sigma^2}$, when $m \longrightarrow +\infty$. Combining yields the result. □

Relationship with the state-of-the-art

At CRYPTO '99 [CJRR99], Chari, Jutla, Rao and Rohatgi gave a lower bound on the probability of success of mono-bit side-channel attacks. The bound is exponential in the number of queries.

Our results generalize the closed-form expressions of the success probability recently obtained in the case of normal noise when correlation is used as a distinguisher [FLD12, TPR13, DZFL14].

First order exponents are an alternative to the *relative distinguishing margin* (RDM [WO11]) because:

- they are completely related to the ideal criterion (namely, the success rate) for large (even moderately large) number of measurements m,
- they can be computed explicitly for many distinguishers to indicate how performance relates to noise power, model, etc. without resorting to experimentation.

Bibliographical references

[CJRR99] Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards Sound Approaches to Counteract Power-Analysis Attacks. In *CRYPTO*, volume 1666 of *LNCS*. Springer, August 15-19 1999. Santa Barbara, CA, USA. ISBN: 3-540-66347-9.

[DZFL14] A. Adam Ding, Liwei Zhang, Yunsi Fei, and Pei Luo. A Statistical Model for Higher Order DPA on Masked Devices. Cryptology ePrint Archive, Report 2014/433, June 2014. http://eprint.iacr.org/2014/433/ (to appear at CHES 2014).

[FLD12] Yunsi Fei, Qiasi Luo, and A. Adam Ding. A Statistical Model for DPA with Novel Algorithmic Confusion Analysis. In Emmanuel Prouff and Patrick Schaumont, editors, *CHES*, volume 7428 of *LNCS*, pages 233–250. Springer, 2012.

[HRG14] Annelie Heuser, Olivier Rioul, and Sylvain Guilley. Good is Not Good Enough — Deriving Optimal Distinguishers from Communication Theory. In Lejla Batina and Matt Robshaw, editors, *CHES*, Lecture Notes in Computer Science. Springer, 2014.

[TPR13] Adrian Thillard, Emmanuel Prouff, and Thomas Roche. Success through Confidence: Evaluating the Effectiveness of a Side-Channel Attack. In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES*, volume 8086 of *Lecture Notes in Computer Science*, pages 21–36. Springer, 2013.