Towards Security Limits in Side-Channel Attacks

(With an Application to Block Ciphers)

F.-X. Standaert, E. Peeters,
C. Archambeau, J.-J. Quisquater

UCL Crypto Group, Université Catholique de Louvain.

CHES 2006

Outline

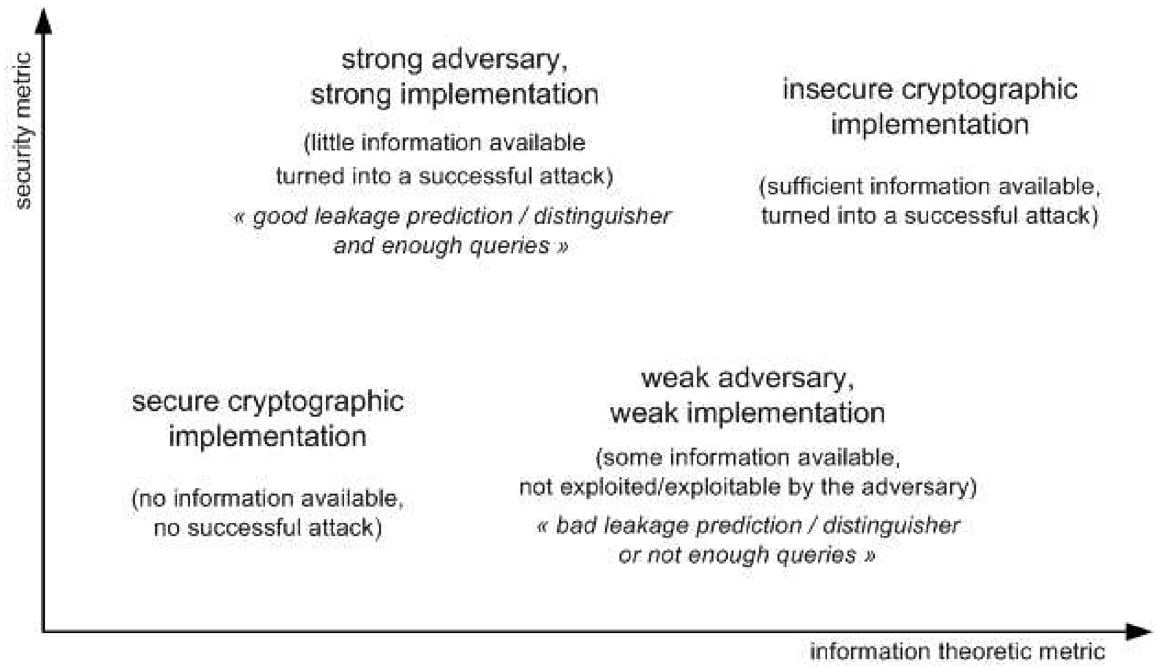
1. Related works
2. Motivations & objectives
3. Model specifications
4. Evaluation criteria
5. Single point leakages
6. Multiple point leakages
7. Masked implementations
8. Conclusions

1. Related works

- Theoretical models for side-channel attacks
  - Micali and Reyzin [TCC2004]
    - Consider physically observable cryptography and define a **physical computer** as a combination of:
      - **An abstract computer** (*i.e.* combination of operations)
      - **A leakage function**
  - Standaert, Malkin, Yung [eprint2006]
    - Additionally attempt to quantify the information leakages with security and information theoretic metrics
    - Practice oriented framework aiming at the evaluation of actual implementations and side-channel adversaries

Main element of the model

- To consider the quality of an implementation and the strength of a side-channel adversary as different (although related) issues

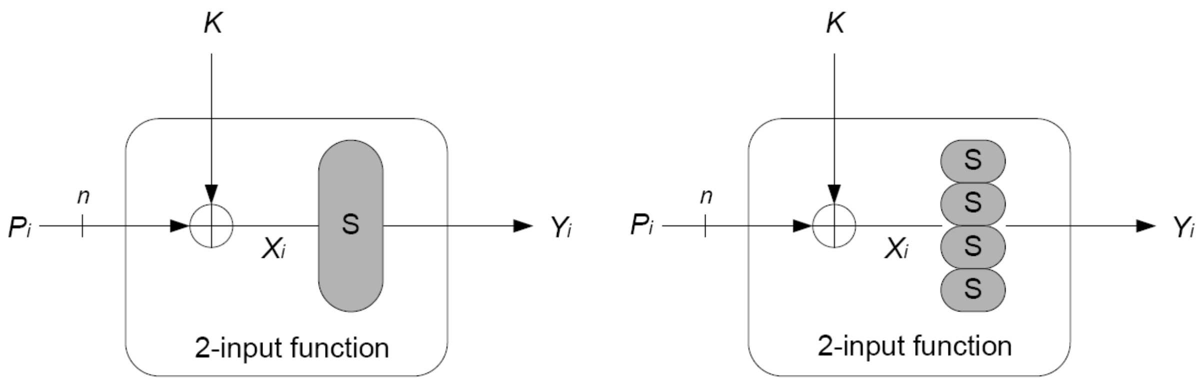


2. Motivations and objectives

- Illustrate the relevance of using combined metrics for the evaluation of side-channel attacks with a practical application
- Derive practical design criteria from a theoretical framework (that cannot be obtained without it)
- Evaluate the security limits of an implementation
  - Because of the IT approach
  - Because we consider (one of) the strongest adversary, namely a Bayesian distinguisher

3. Model specifications

- Target implementation: single *vs.* multiple block



- Hamming weight (+noise) leakage function
- Non adaptive, known plaintext adversary
- Hard strategy *(given some physical observations and a classification of key candidates, select the best classified key only)*

4. Evaluation criteria

- Quality of the implementation:
  - *What is the amount of information provided by a given leakage function?*
    - $\Rightarrow$ IT metric

- Strength of the adversary:
  - *How successfully can an adversary turn this information into a successful attack?*
    - $\Rightarrow$ Security metric

Definitions

- $L^q_{S_g} = \mathcal{L}(S_g)^q$: an observation generated by a secret S_g and q queries to the target device

- $P^q_S = \mathcal{P}(S)^q$: the adversary's predictions

- $\mathcal{D}(L^q_{S_g}, P^q_S)$: the distinguisher used by the adversary to compare an actual observation of a leaking device with its key dependent predictions

Security metric: average success rate

- Keys selected by the adversary (hard strategy):

$$M^q_{S_g} = \{\hat{s} \mid \hat{s} = \underset{S}{argmax}\, \mathcal{D}(L^q_{S_g}, P^q_S)\},$$

- Index matrix:

$$\mathrm{I}^q_{S_g,S} = \frac{1}{|M^q_{S_g}|} \ \textbf{if}\ S \in M^q_{S_g}, \quad \textbf{else}\ 0$$

- Success rate:

$$\mathbf{S_R}(S_g, q) = \underset{L^q_{S_g}}{\mathbf{E}}\ \mathrm{I}^q_{S_g,S_g}, \qquad \overline{\mathbf{S_R}}(q) = \underset{S_g}{\mathbf{E}}\ \underset{L^q_{S_g}}{\mathbf{E}}\ \mathrm{I}^q_{S_g,S_g}$$

Example: Bayesian classifier

S=0	S=1	S_g=2	S=3	Index
1/9	1/9	2/3	1/9	1
1/3	1/3	1/3	0	1/3
1/8	1/2	1/4	1/8	0
1/5	1/5	2/5	1/5	1

$$\mathbf{S_R}(S_g = 2, q) \simeq 58\%$$

Information theoretic metric: mutual information

- Entropy matrix: $$\mathsf{H}^q_{S_g,S} = \mathop{\mathsf{E}}_{L^q_{S_g}} -\log_2 \mathbf{P}[S|L^q_{S_g}]$$
- Conditional entropy: $$\mathbf{H}[S_g|L^q_{S_g}] = \mathop{\mathsf{E}}_{S_g} \mathsf{H}^q_{S_g,S_g}$$
- Leakage matrix: $$\Lambda^q_{S_g,S} = \mathbf{H}[S_g] - \mathsf{H}^q_{S_g,S}$$
- Mutual information:

$$\mathbf{I}(S_g; L^q_{S_g}) = \mathbf{H}[S_g] - \mathbf{H}[S_g|L^q_{S_g}] = \mathop{\mathsf{E}}_{S_g} \Lambda^q_{S_g,S_g}$$

Example

$S=0$	$S=1$	$S_g=2$	$S=3$
1/9	1/9	2/3	1/9
2/7	2/7	2/7	1/7
1/5	1/5	2/5	1/5
-0.43	-0.43	0.77	-0.76

$$\Lambda^q_{S_g,S} = 2 - \mathsf{H}^q_{S_g,S}$$

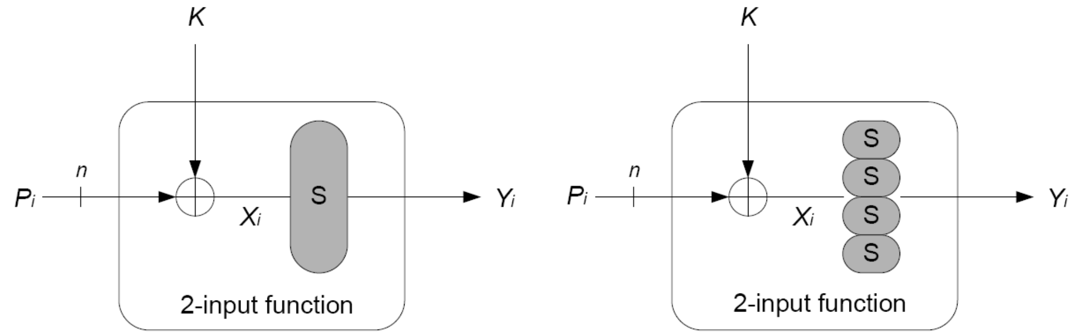
- Definition: a leakage function is sound

$$\Longleftrightarrow \max_S \Lambda^q_{S_g,S} = \Lambda^q_{S_g,S_g}, \; \forall \; S_g, q.$$

- If provided with a sound leakage function, a Bayesian adversary with unlimited queries to the target device will eventually be successful
  – Intuitive meaning: there is *enough* information in the side-channel observations

5. Single point leakages

- Context:
  - Microcontroller
  - 8-bit data bus
  - Gaussian noise



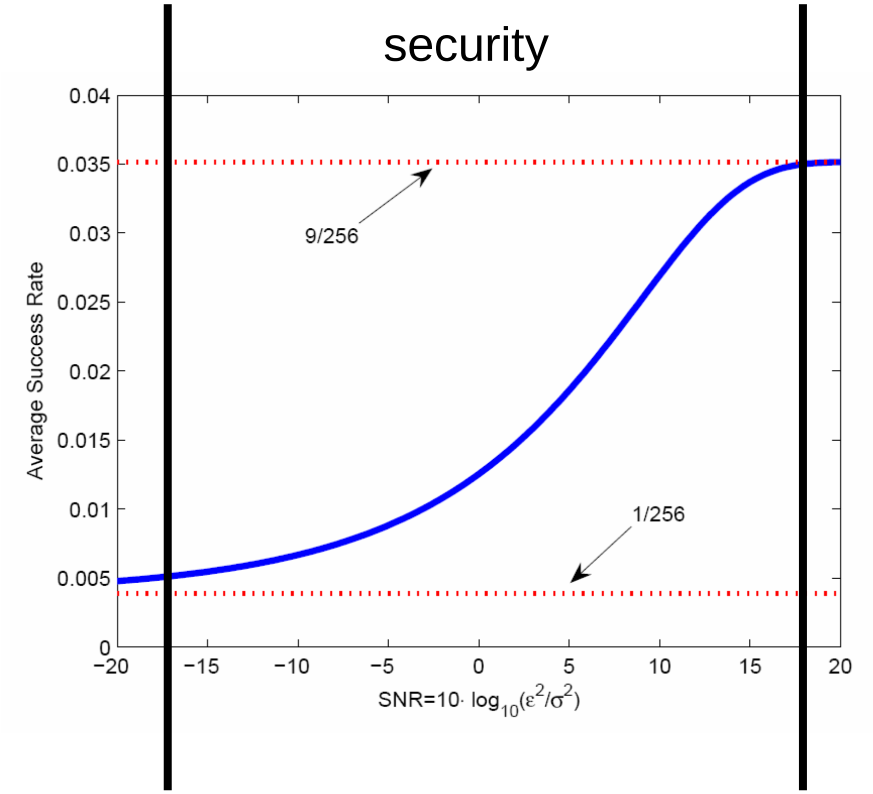
$$L^1_{S_g} = W_H(Y_i) + N(0, \sigma^2)$$

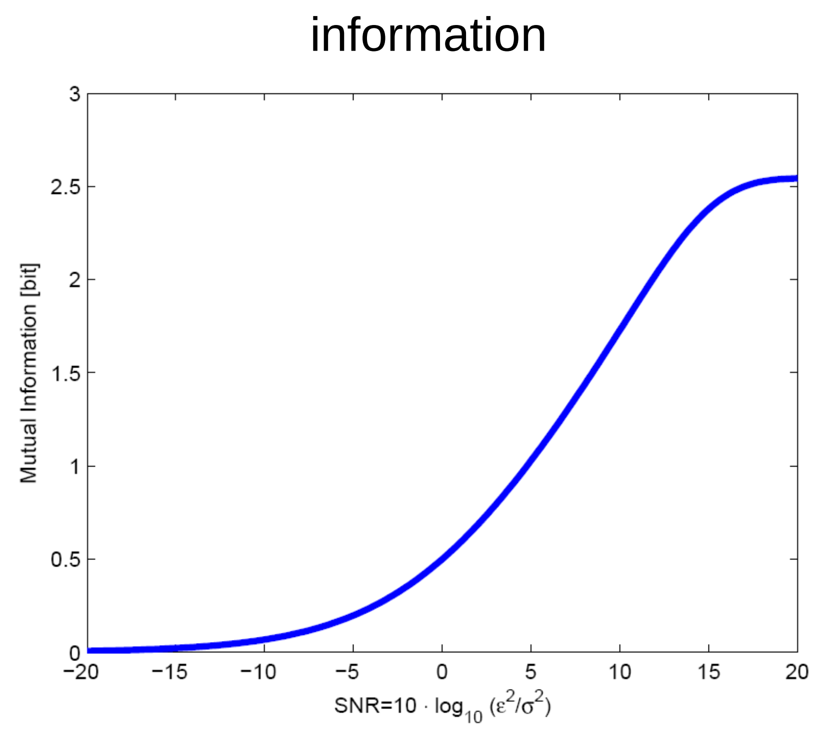
- Definitions:

$$\overline{\mathbf{S}_{\mathbf{R}}} = \underset{S_g}{\mathbf{E}} \; \underset{L^1_{S_g}}{\mathbf{E}} \; \mathrm{I}^1_{S_g,S_g} = \sum_{h=0}^{n} \frac{\binom{n}{h}}{2^n} \cdot \int_{-\infty}^{+\infty} \mathbf{P}[L^1_{S_g}|h] \cdot \mathrm{I}^1_{S_g,S_g} \; dl,$$

$$\mathbf{H}[S_g|L^1_{S_g}] = \underset{S_g}{\mathbf{E}} \; \mathrm{H}^1_{S_g,S_g} = \sum_{h=0}^{n} \frac{\binom{n}{h}}{2^n} \cdot \int_{-\infty}^{+\infty} \mathbf{P}[L^1_{S_g}|h] \cdot -\log_2(\mathbf{P}[S_g|L^1_{S_g}]) \; dl,$$

In function of the SNR



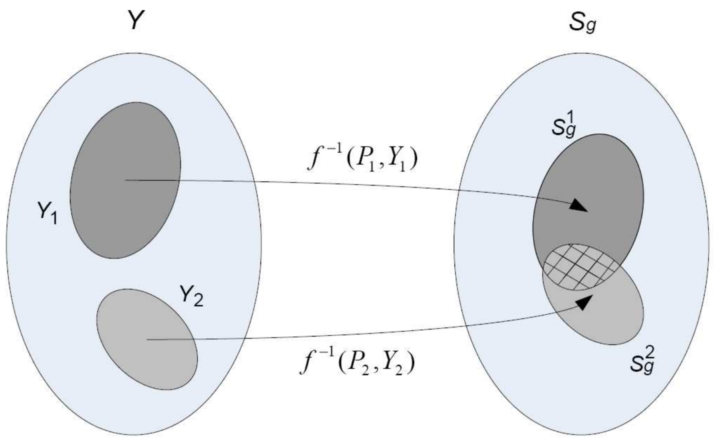


high measurement noise

low (Gaussian) measurement noise

6. Multiple point leakages

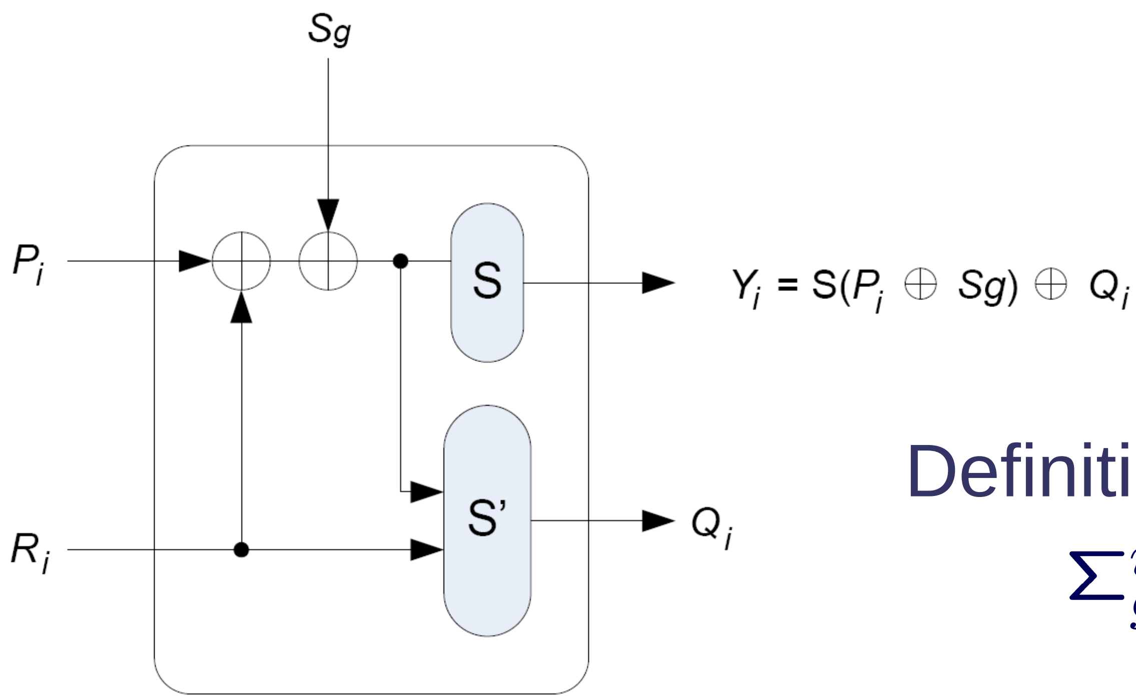
- Similar intuition
- Similar curves
- Slightly more difficult
  to compute (see the paper)



- Dependency on the block cipher components (*e.g*. the paper compares random and actual S-boxes)

- At this point, it is not clear why 2 metrics are necessary

7. Masked implementations

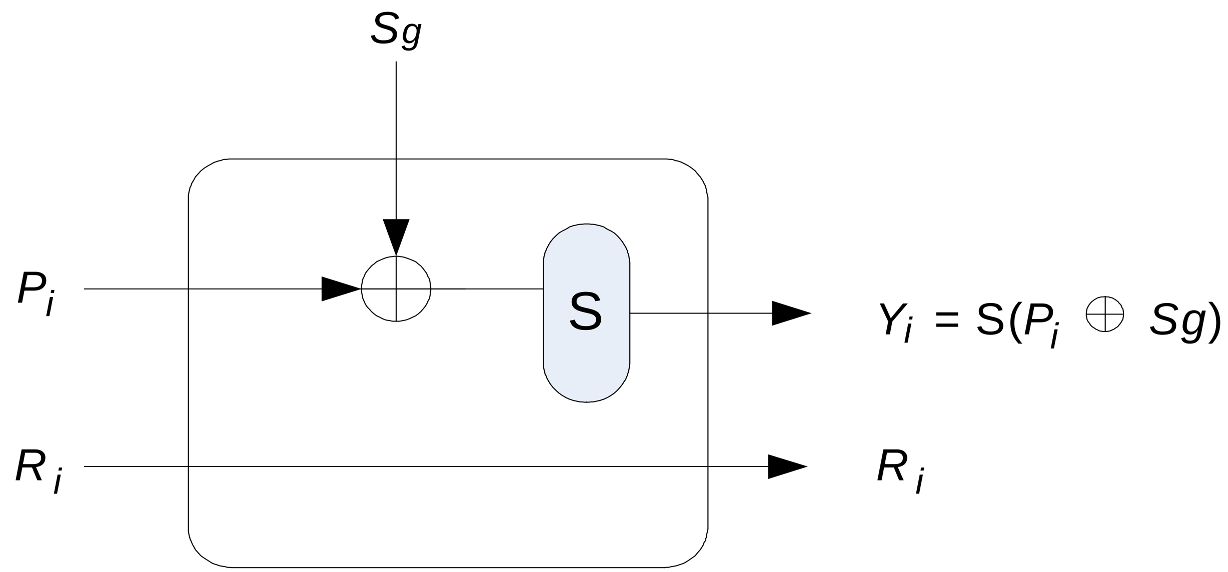


Definition of a secret state:

$$\Sigma_g^i = \mathsf{S}(P_i \oplus S_g)$$

$$L^q_{\Sigma_g^i} = W_H[\Sigma_g^i \oplus Q_i] + W_H[Q_i] + N(0, \sigma^2)$$

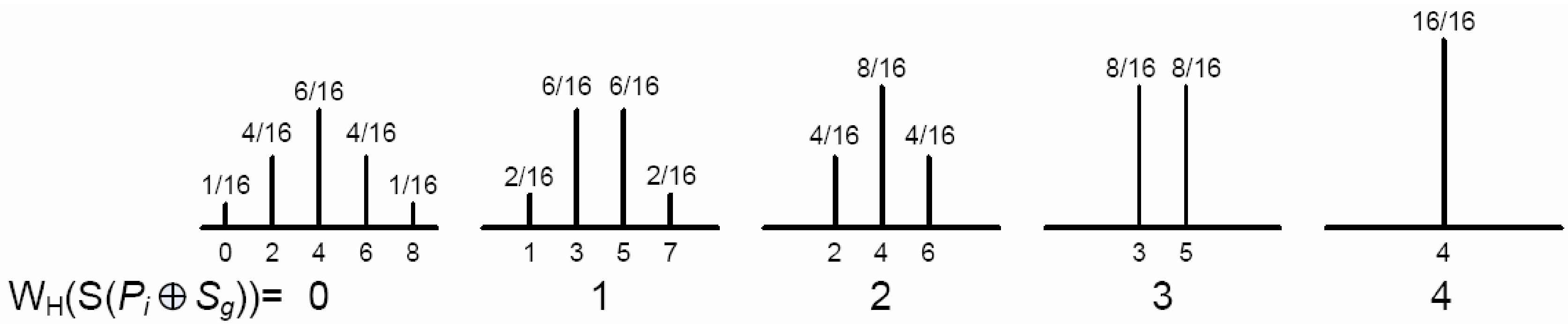
vs. algorithmic noise addition



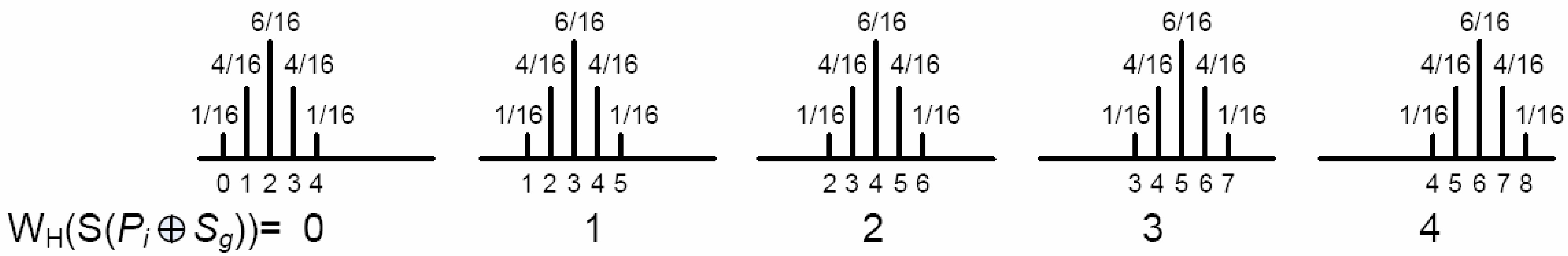
$$L^q_{S_g} = W_H(Y_i) + W_H(R_i) + N(0, \sigma^2)$$

Of course less efficient than masking? Not so sure…

Compute the PDFs
[PSDQ,CHES2005]



(a) 4-bit masked value



(b) 4-bit value and 4 noisy bits

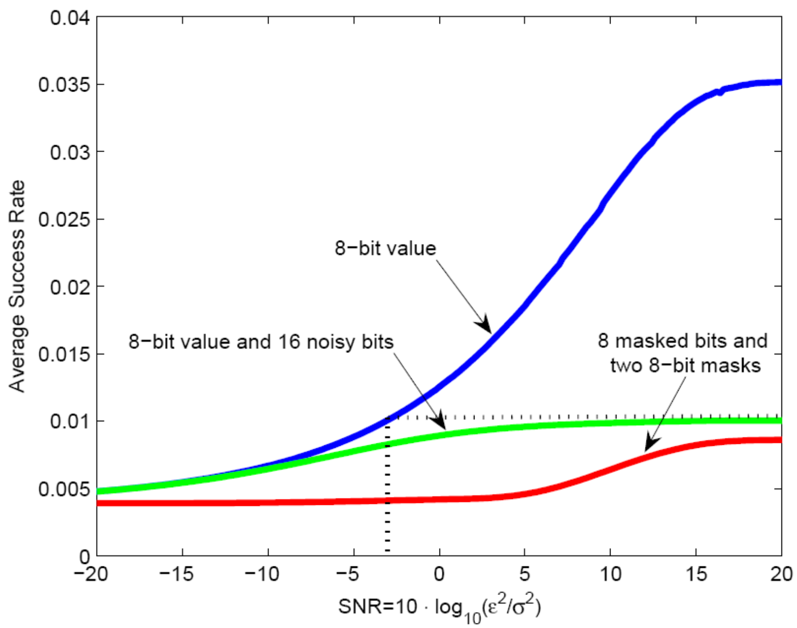
And use the same definitions again…

$$\overline{\mathbf{S_R}} = \mathop{\mathbf{E}}_{\Sigma_g^i} \; \mathop{\mathbf{E}}_{L^1_{\Sigma_g^i}} \mathrm{I}^1_{\Sigma_g^i,\Sigma_g^i} = \sum_{h=0}^{n} \frac{\binom{n}{h}}{2^n} \cdot \int_{-\infty}^{+\infty} \mathbf{P}[L^1_{\Sigma_g^i}|h] \cdot \mathrm{I}^1_{\Sigma_g^i,\Sigma_g^i} \; dl,$$

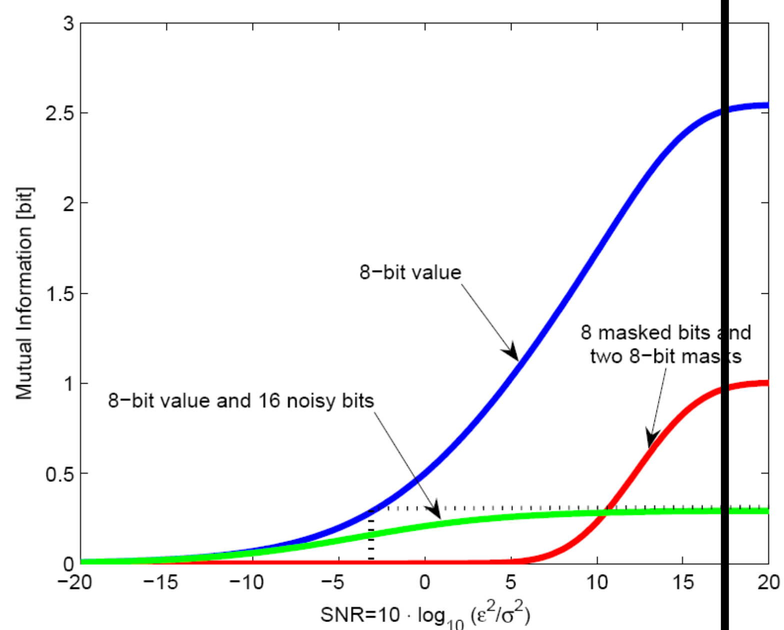
$$\mathbf{H}[S_g|L^1_{S_g}] = \mathop{\mathbf{E}}_{\Sigma_g^i} \; \mathrm{H}^1_{\Sigma_g^i,\Sigma_g^i} = \sum_{h=0}^{n} \frac{\binom{n}{h}}{2^n} \cdot \int_{-\infty}^{+\infty} \mathbf{P}[L^1_{\Sigma_g^i}|h] \cdot -\log_2(\mathbf{P}[\Sigma_g|L^1_{\Sigma_g^i}]) \; dl,$$

Example: 8-bit values, second-order masking

security



information



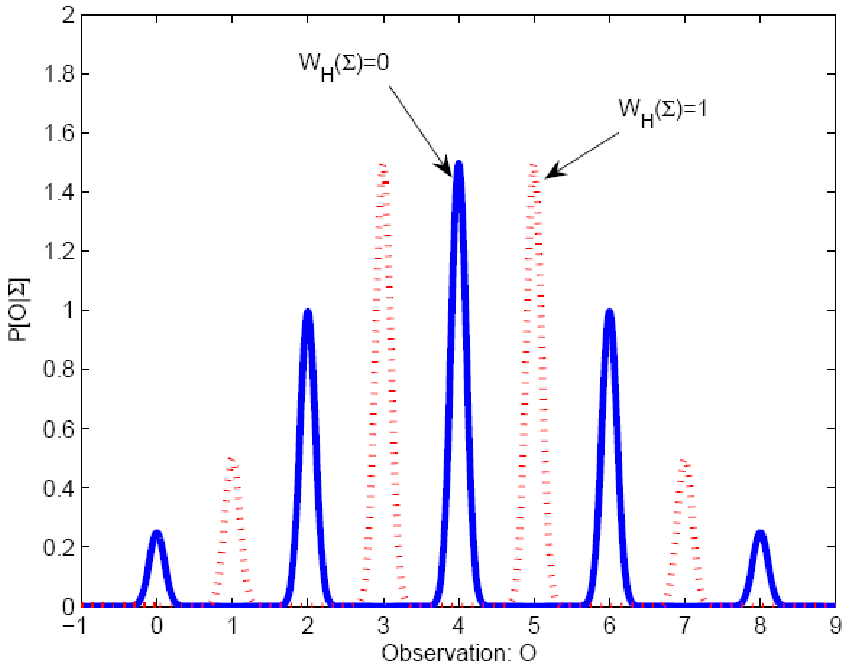
Security and IT metrics do not agree !

$\Rightarrow$ IT metric intuitive meaning

low measurement noise

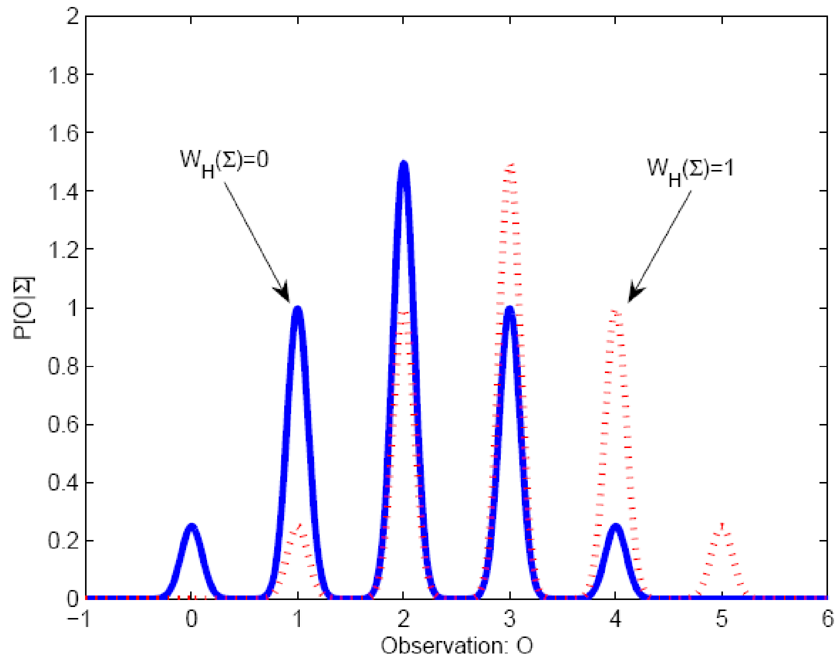
High SNR

Masking

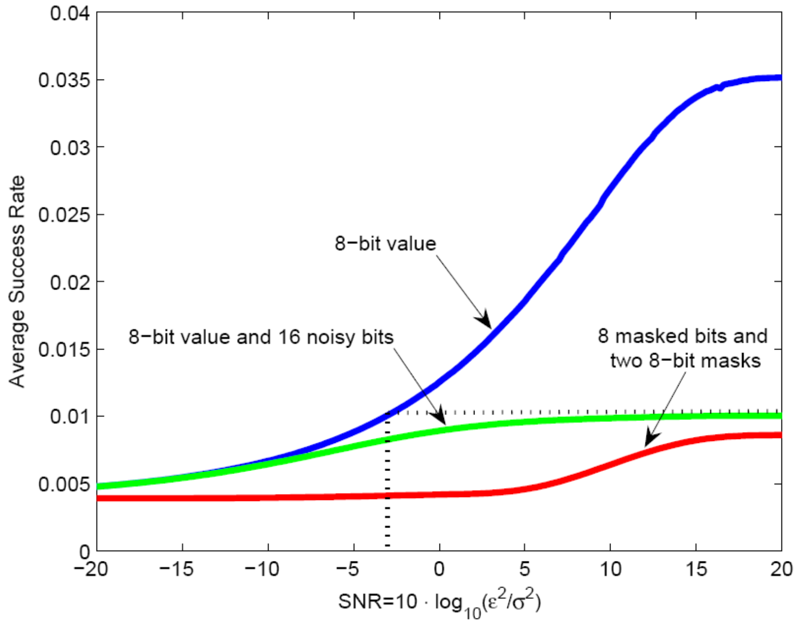


more information

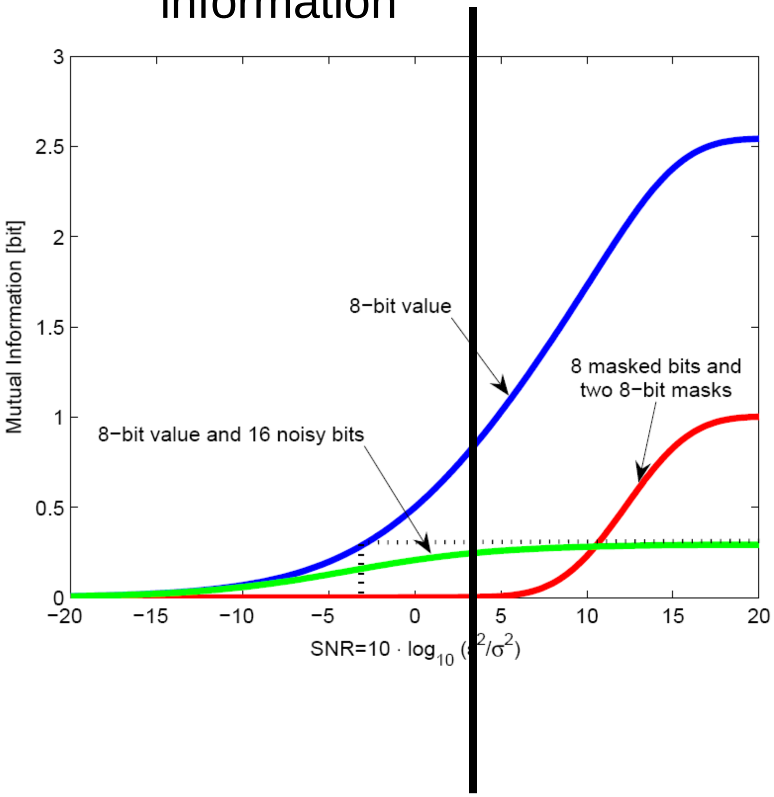
Noise addition



security



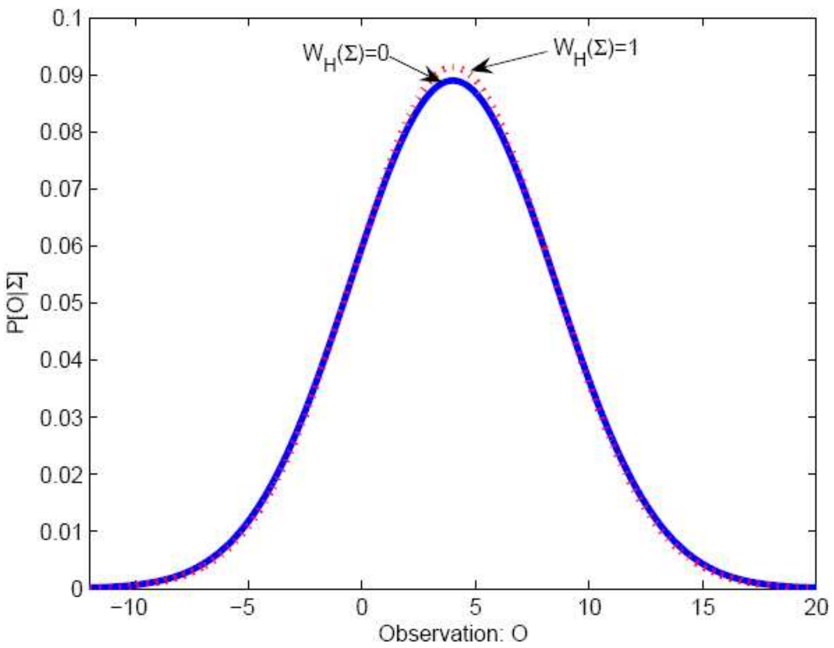
information



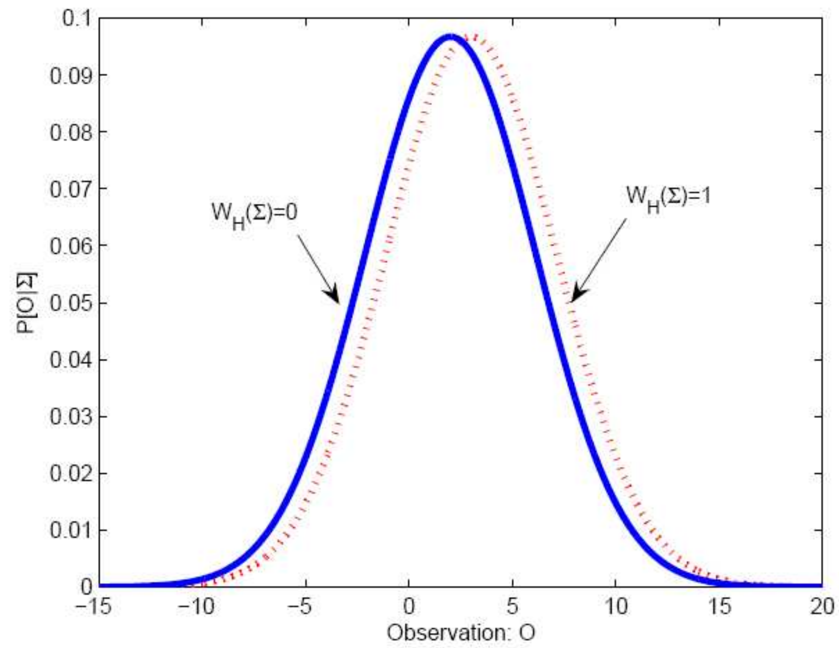
high measurement noise

Low SNR

Masking

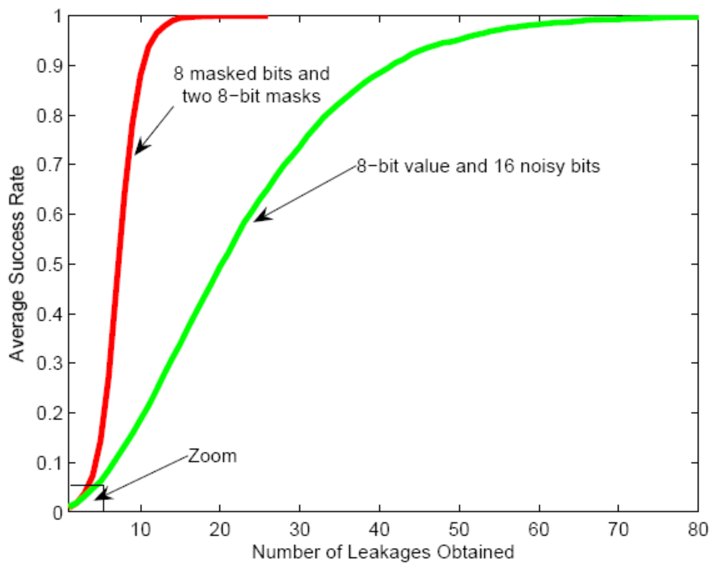


Noise addition

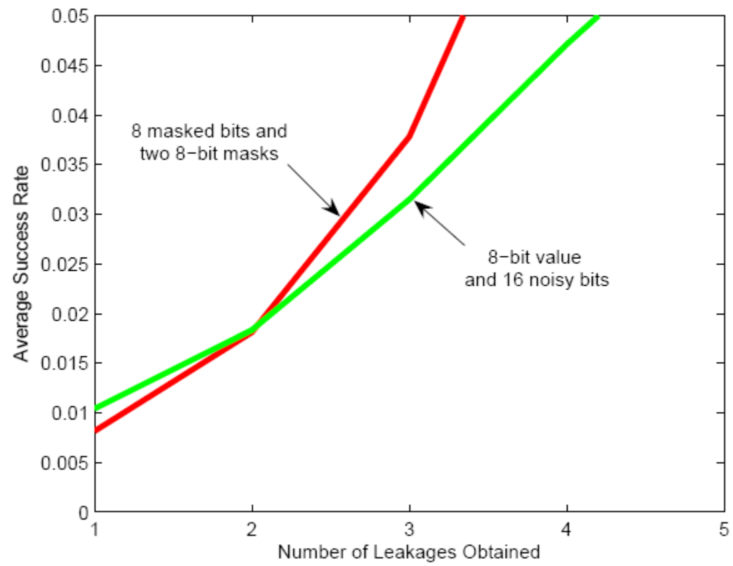


more information

Who said the truth?
Increase the number of queries



(a) Comparison



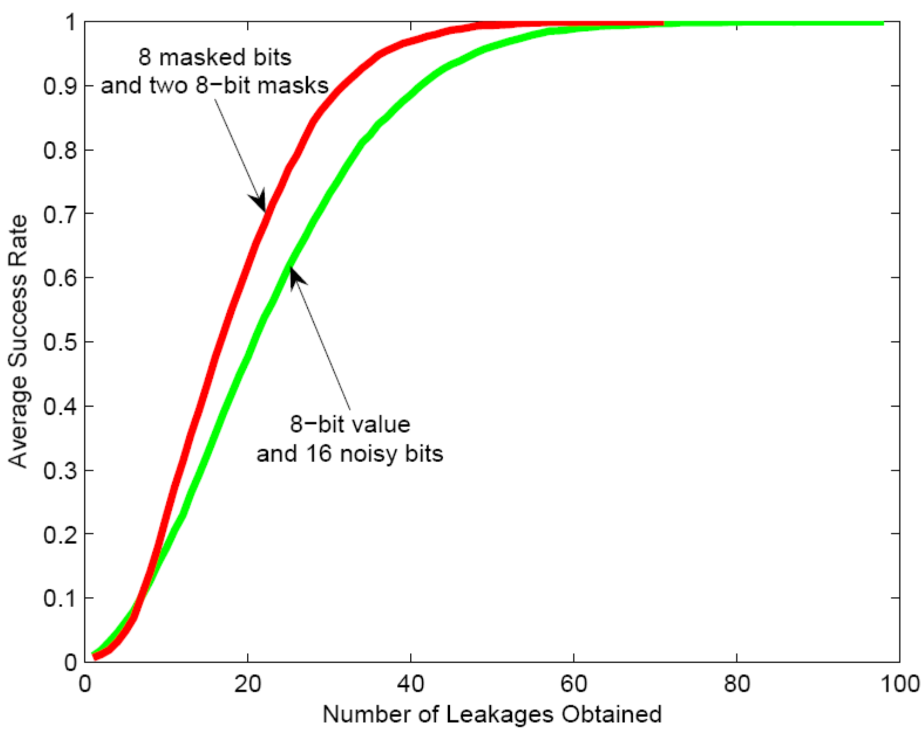
(b) Zoom

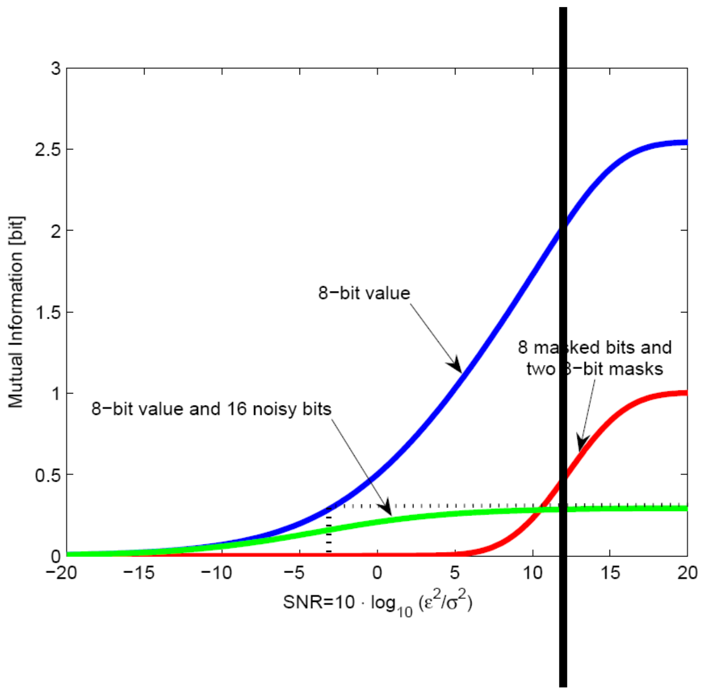
- High SNRs: masking is less efficient than noise addition
- The IT metric discriminates the implementations
- The security metric discriminates the adversaries

8. Conclusions (a)

What cannot be achieved without our metrics?

- A practical design criteria:



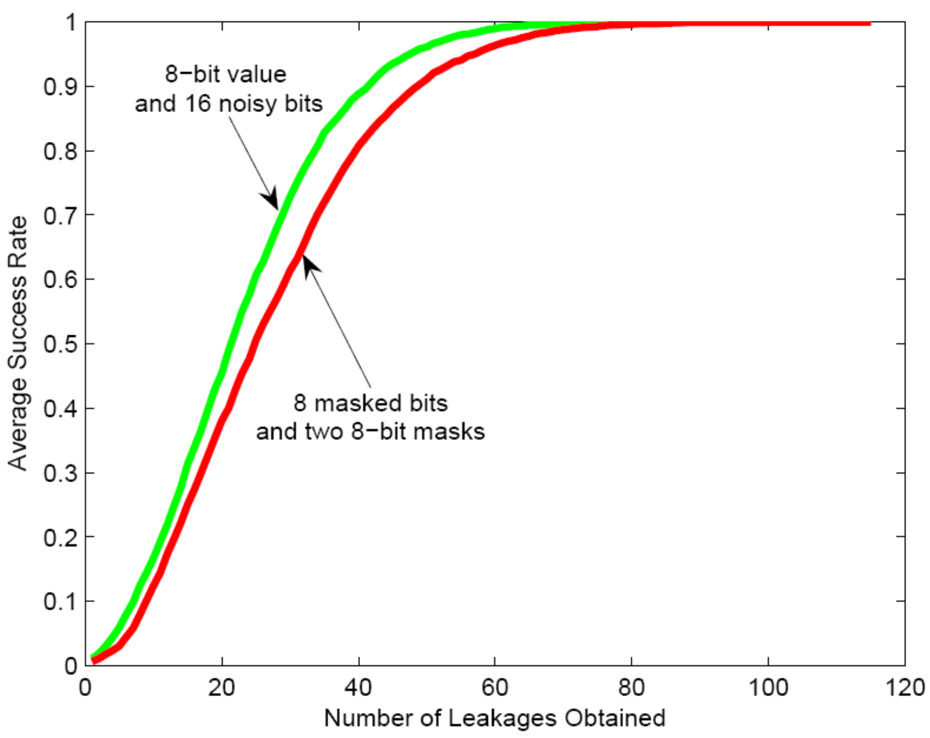


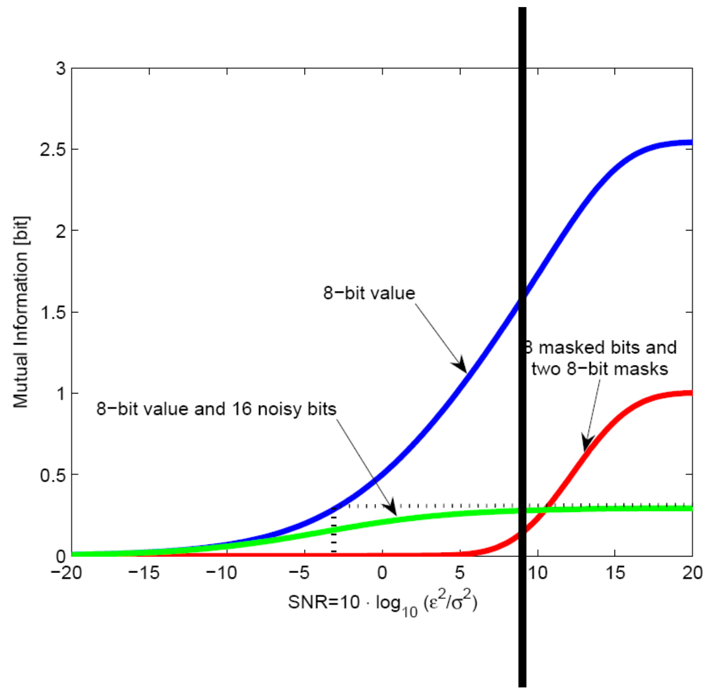
right of the noise threshold
e.g. 8-bit smart card

noise addition better than masking

What cannot be achieved without our metrics?

- A practical design criteria:





left of the noise threshold
e.g. FPGA

masking better than noise addition

Conclusions (b)

- This work confirms
  - The relevance of using combined security and IT metrics for the evaluation of side-channel attacks
  - The importance of considering both the quality of an implementation and the strenght of side-channel adversaries in the physical world
- The limitations of higher-order masking schemes (*vs.* correlation based analyses in CT-RSA 2006)
- The model also allows: the fair comparison of attacks and implementations, the design of provably secure primitives, the development of adaptive attacks, …

-THANKS-

Send comments to:

fstandae@uclouvain.be

More information on:

http://www.dice.ucl.ac.be/~fstandae/tsca/