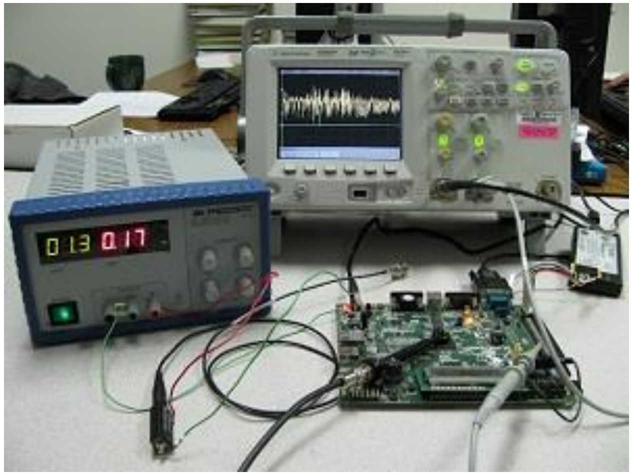
High (Physical) Security & Lightweight (Symmetric) Cryptography



François-Xavier Standaert

UCL Crypto Group, Belgium

HIGHLIGHT – LIGHTCRYPTO, November 2016

Outline

- Preliminary questions / definitions
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- Mitigating hardware defaults (is hard)
- Transparency is needed (open source)
- Summary and conclusions

Outline

- Preliminary questions / definitions
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- Mitigating hardware defaults (is hard)
- Transparency is needed (open source)
- Summary and conclusions

intro

secure design

eval.

Outline

- **Preliminary questions / definitions**
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- Mitigating hardware defaults (is hard)
- Transparency is needed (open source)
- Summary and conclusions

What does secure mean? (I)

- For block ciphers, best attack has:
  - Time complexity 2^{n_1}
  - Data complexity 2^{n_2}
  - Memory complexity 2^{n_3}

What does secure mean? (I)

- For block ciphers, best attack has:
  - Time complexity 2^{n_1}
  - Data complexity 2^{n_2}
  - Memory complexity 2^{n_3}

- With typical security parameters:
  - $n_L = 80, n_S = 128, n_{PQ} = 256$
  - https://www.keylength.com/en/
- Function of the algorithms' deployment time and the adversary's computational power

What does secure mean? (II)

- When also considering physical attacks:
  - Measurement complexity 2^{m_1}
  - Fault complexity 2^{m_2}
- Typical security parameters: ???

What does secure mean? (II)

- When also considering physical attacks:
  - Measurement complexity 2^{m_1}
  - Fault complexity 2^{m_2}
- Typical security parameters: ???

Q1. Deployment time of implementations?

- IMO not much less (minimum 5-10 years)
- So we can gain a factor 2 to 4 (i.e., 1,2 bits)

Yuanyuan Zhou, Yu Yu, François-Xavier Standaert, Jean-Jacques Quisquater: *On the Need of Physical Security for Small Embedded Devices: A Case Study with COMP128-1 Implementations in SIM Cards*. Financial Cryptography 2013: 230-238.
Junrong Liu, Yu Yu, François-Xavier Standaert, Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, Xinjun Xie: *Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards*. ESORICS (1) 2015: 468-480

What does secure mean? (III)

Q2. What's the adversary's measurement power?

What does secure mean? (III)

Q2. What's the adversary's measurement power?

- Generic answer:
  - "Cost" of collecting one side-channel meas. vs. cost of collecting one *pt*/*ct* pair?
    - Min. $\times 2^{10}$, avg. $\times 2^{20}$, opt. $\times 2^{30}$
  - Roughly assume ≈ the same for faults
  - So we can gain 10 to 30 bits (roughly)

$\Rightarrow m_L > 60$ and $m_S > 100$ (no clue about m_{PQ})

Amir Moradi, Alessandro Barenghi, Timo Kasper, Christof Paar: *On the vulnerability of FPGA bitstream encryption against power analysis attacks: extracting keys from xilinx Virtex-II FPGAs*. ACM Conference on Computer and Communications Security 2011: 111-124. Amir Moradi, Axel Poschmann, San Ling, Christof Paar, Huaxiong Wang: *Pushing the Limits: A Very Compact and a Threshold Implementation of AES*. EUROCRYPT 2011: 69-88

What does secure mean? (IV)

- Specific answer (if physical access is limited):
  - $m_{VL} > 40$ (≈ some days/weeks)
  - $m_{UL} > 20$ (≈ some hours)
  - Excluding network access (timing attacks)!

What does secure mean? (IV)

- Specific answer (if physical access is limited):
  - $m_{VL} > 40$ (≈ some days/weeks)
  - $m_{UL} > 20$ (≈ some hours)
  - Excluding network access (timing attacks)!

- Fact 1. Currently, we mostly design for VL/UL physical security / Fact 2. Current physical security evaluations are limited to VL security

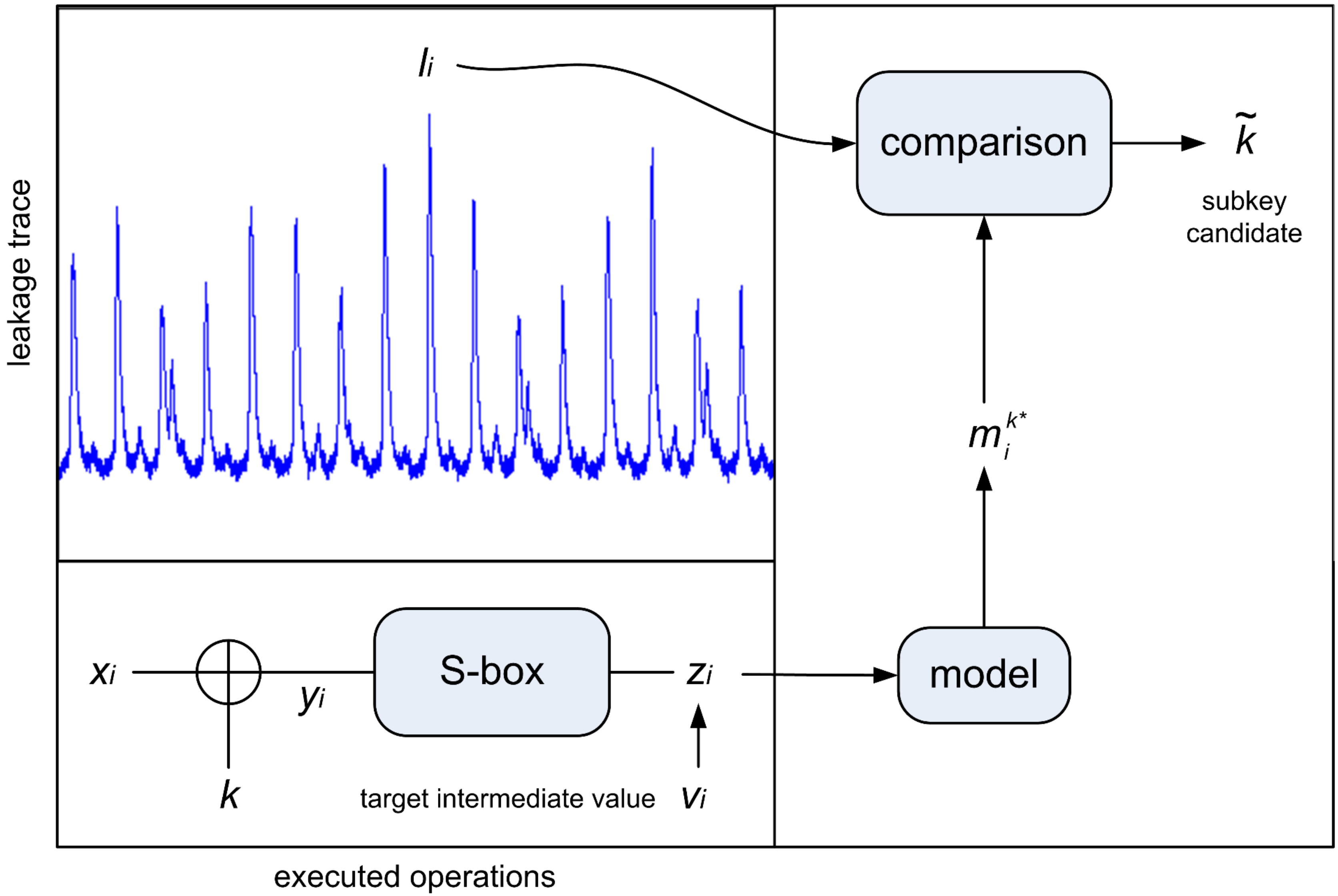
What does secure mean? (IV)

- Specific answer (if physical access is limited):
  - $m_{VL} > 40$ (≈ some days/weeks)
  - $m_{UL} > 20$ (≈ some hours)
  - Excluding network access (timing attacks)!
- Fact 1. Currently, we mostly design for VL/UL physical security / Fact 2. Current physical security evaluations are limited to VL security
-  VL or UL security ≈ no security

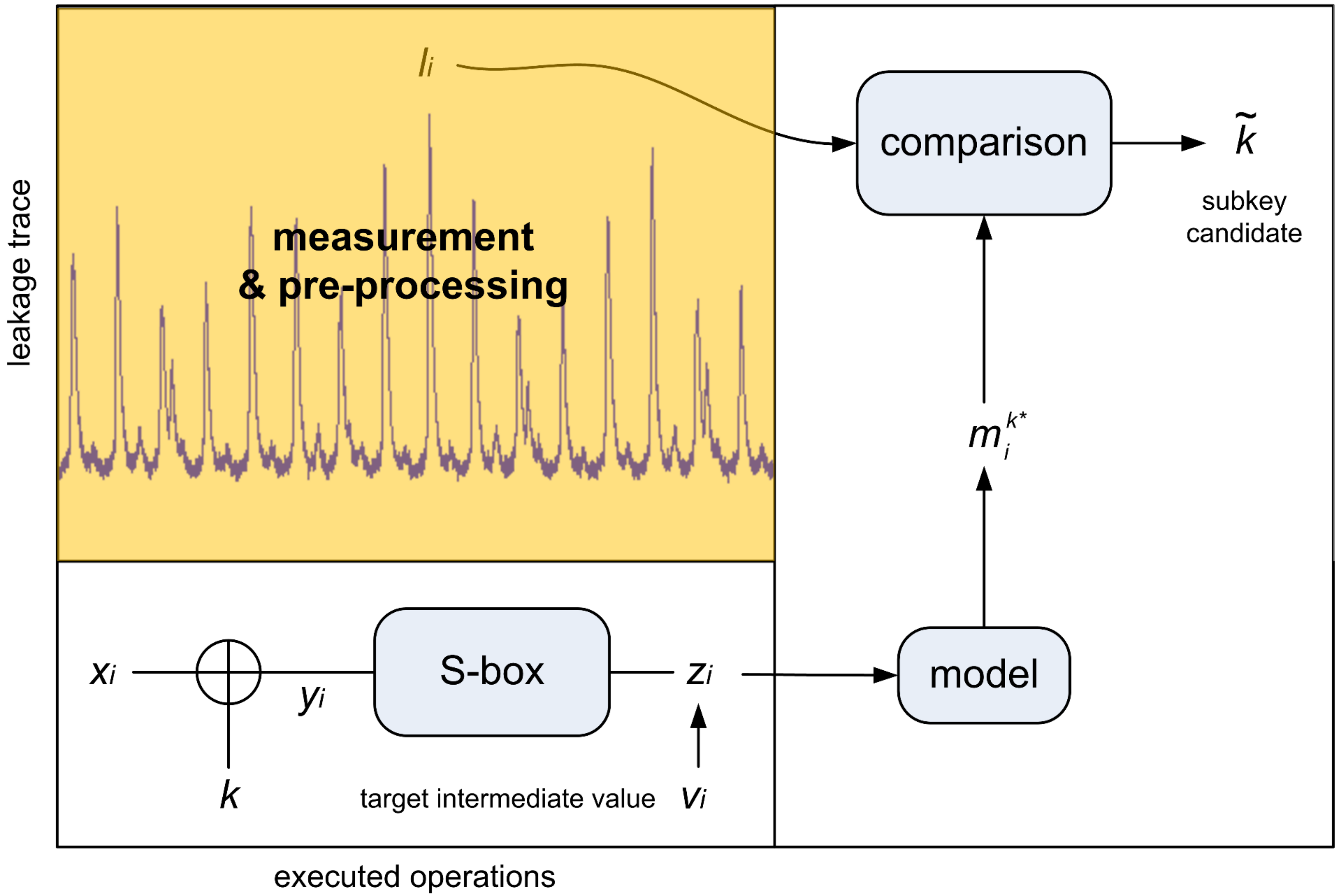
Outline

- Preliminary questions / definitions
- **Side-channel basics (attack steps)**
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- Mitigating hardware defaults (is hard)
- Transparency is needed (open source)
- Summary and conclusions

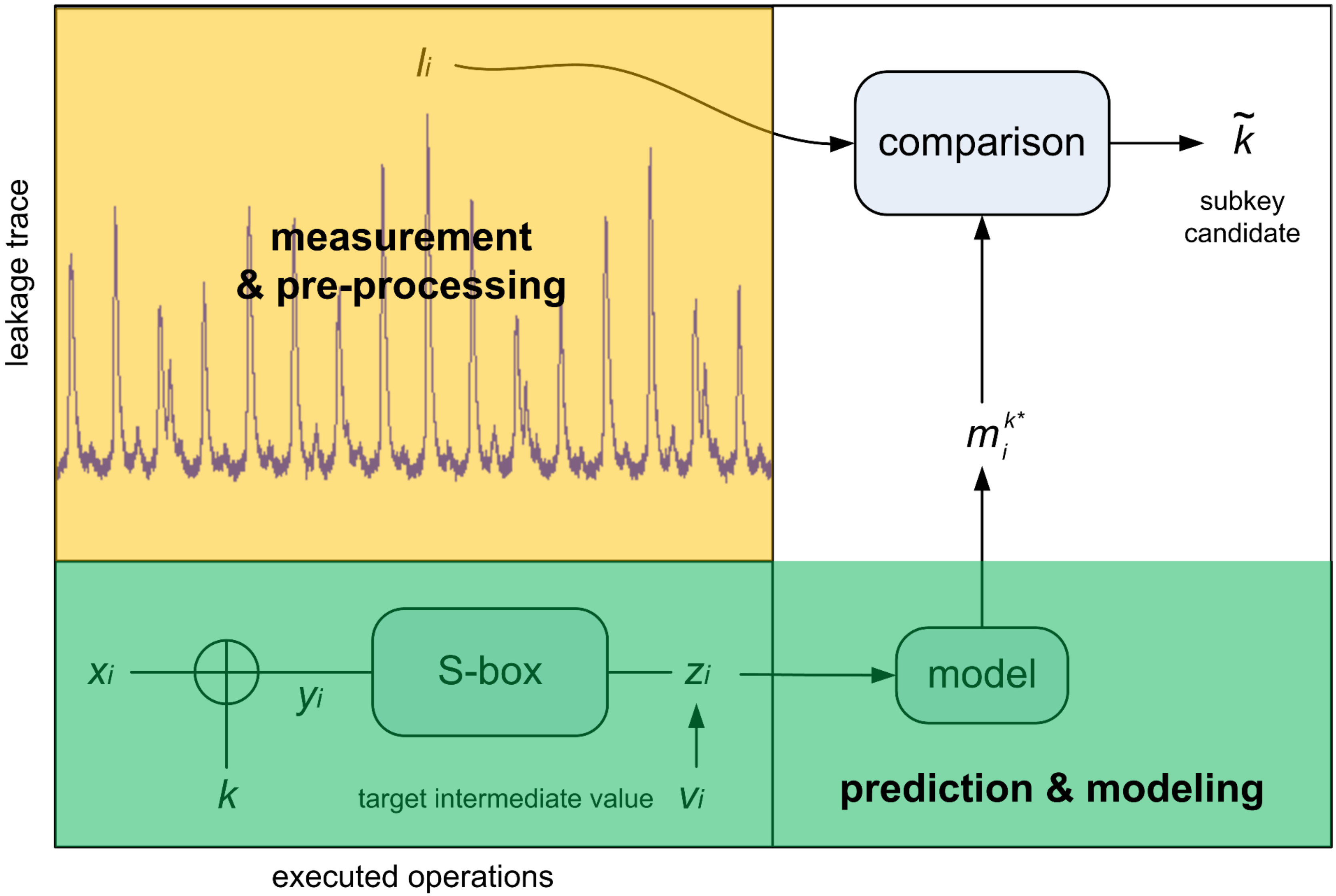
Standard DPA



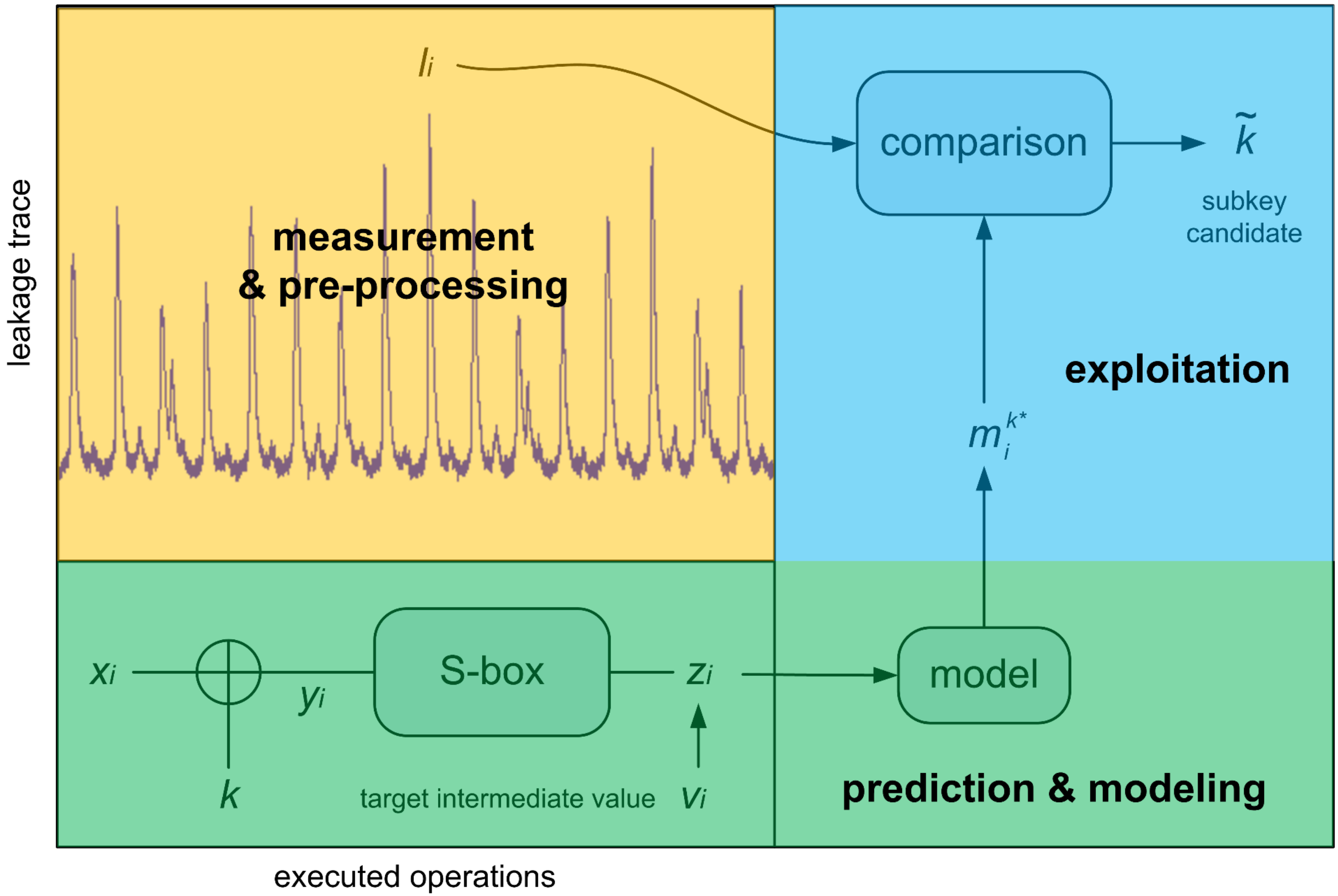
Standard DPA



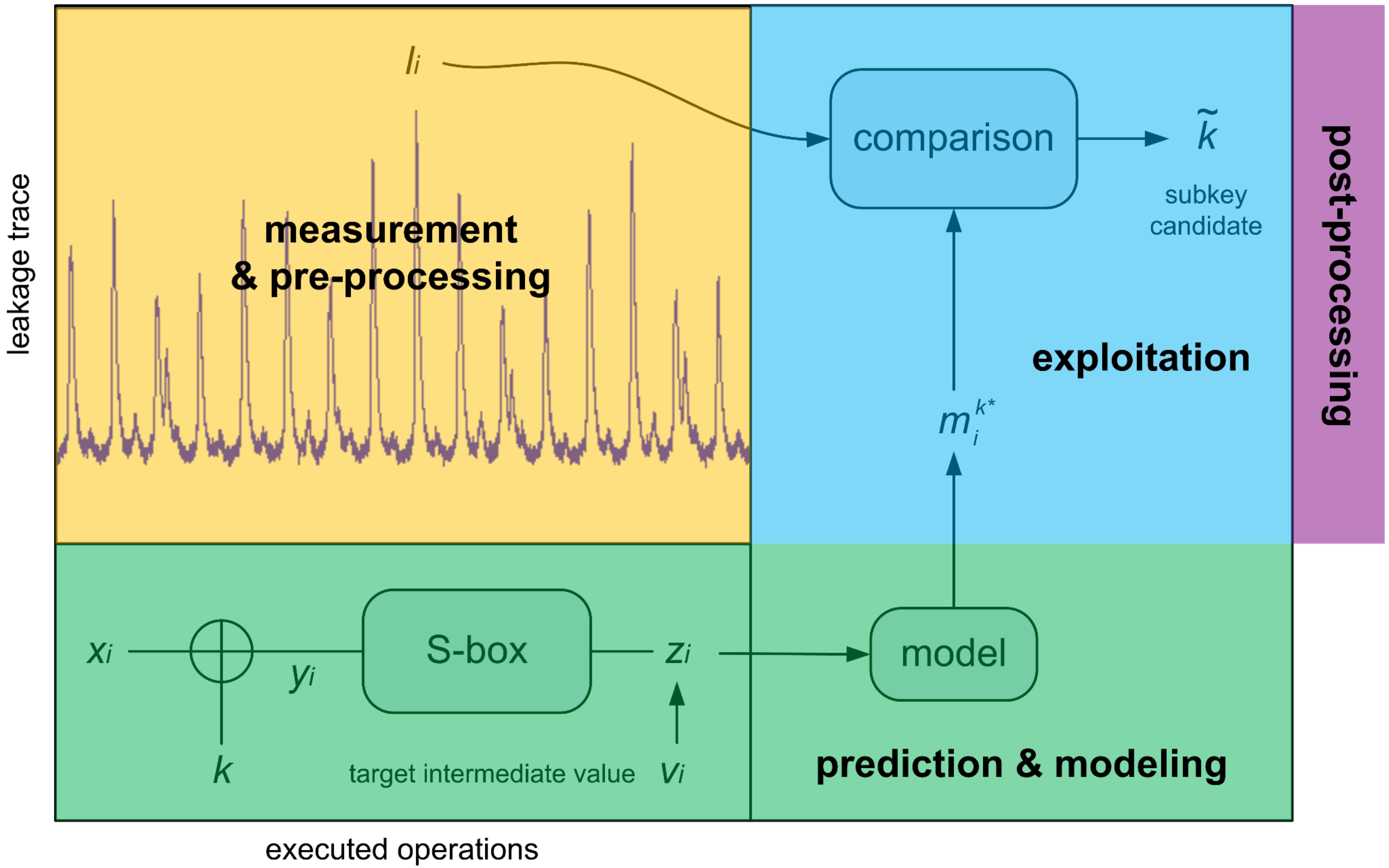
Standard DPA



Standard DPA



Standard DPA



Measurement & pre-processing

- Noise reduction via good setups
- Filtering, averaging (FFT, SSA, …)
- Detection of Points-Of-Interest (POI)
- Dimensionality reduction (PCA, LDA,…)
- …

Victor Lomné, Emmanuel Prouff, Thomas Roche: *Behind the Scene of Side Channel Attacks.* ASIACRYPT (1) 2013: 506-525. Santos Merino Del Pozo, François-Xavier Standaert: *Blind Source Separation from Single Measurements Using Singular Spectrum Analysis*. CHES 2015: 42-59. Oscar Reparaz, Benedikt Gierlichs, Ingrid Verbauwhede: *Selecting Time Samples for Multivariate DPA Attacks*. CHES 2012: 155-174. François Durvaux, François-Xavier Standaert: *From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces*. EUROCRYPT (1) 2016: 240-262 - 50. Cédric Archambeau, Eric Peeters, François-Xavier Standaert, Jean-Jacques Quisquater: *Template Attacks in Principal Subspaces*. CHES 2006: 1-14. François-Xavier Standaert, Cédric Archambeau: *Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages*. CHES 2008: 411-425

Measurement & pre-processing

- Noise reduction via good setups
- Filtering, averaging (FFT, SSA, …)
- Detection of Points-Of-Interest (POI)
- Dimensionality reduction (PCA, LDA,…)
- …
- Inherently heuristic (!) ⇒ hard to determine what is the optimal solution (≠ next steps)

Victor Lomné, Emmanuel Prouff, Thomas Roche: *Behind the Scene of Side Channel Attacks.* ASIACRYPT (1) 2013: 506-525. Santos Merino Del Pozo, François-Xavier Standaert: *Blind Source Separation from Single Measurements Using Singular Spectrum Analysis*. CHES 2015: 42-59. Oscar Reparaz, Benedikt Gierlichs, Ingrid Verbauwhede: *Selecting Time Samples for Multivariate DPA Attacks*. CHES 2012: 155-174. François Durvaux, François-Xavier Standaert: *From Improved Leakage Detection to the Detection of Points of Interests in Leakage Traces*. EUROCRYPT (1) 2016: 240-262 - 50. Cédric Archambeau, Eric Peeters, François-Xavier Standaert, Jean-Jacques Quisquater: *Template Attacks in Principal Subspaces*. CHES 2006: 1-14. François-Xavier Standaert, Cédric Archambeau: *Using Subspace-Based Template Attacks to Compare and Combine Power and Electromagnetic Information Leakages*. CHES 2008: 411-425

Prediction and modeling

- General case: profiled DPA
  - Build "*templates*", i.e., $\hat{f}(l_i|k, x_i)$
    - e.g. Gaussian, regression-based
  - Which directly leads to $\widehat{\Pr}[k|l_i, x_i]$

Suresh Chari, Josyula R. Rao, Pankaj Rohatgi: *Template Attacks*. CHES 2002: 13-28. Werner Schindler, Kerstin Lemke, Christof Paar: *A Stochastic Model for Differential Side Channel Cryptanalysis*. CHES 2005: 30-46

Prediction and modeling

- General case: profiled DPA
  - Build "*templates*", i.e., $\hat{f}(l_i|k, x_i)$
    - e.g. Gaussian, regression-based
  - Which directly leads to $\widehat{\Pr}[k|l_i, x_i]$
- "Simplified" case: non-profiled DPA
  - Just assumes some model
  - e.g., $m_i^{k^*} = \mathrm{HW}(z_i)$

Suresh Chari, Josyula R. Rao, Pankaj Rohatgi: *Template Attacks*. CHES 2002: 13-28. Werner Schindler, Kerstin Lemke, Christof Paar: *A Stochastic Model for Differential Side Channel Cryptanalysis*. CHES 2005: 30-46

Prediction and modeling

- General case: profiled DPA
  - Build "*templates*", i.e., $\hat{f}(l_i|k, x_i)$
    - e.g. Gaussian, regression-based
  - Which directly leads to $\widehat{\Pr}[k|l_i, x_i]$
- "Simplified" case: non-profiled DPA
  - Just assumes some model
  - e.g., $m_i^{k^*} = \mathrm{HW}(z_i)$
- Separation: only profiled DPA is guaranteed to succeed against any leaking device (!)

Suresh Chari, Josyula R. Rao, Pankaj Rohatgi: *Template Attacks*. CHES 2002: 13-28. Werner Schindler, Kerstin Lemke, Christof Paar: *A Stochastic Model for Differential Side Channel Cryptanalysis*. CHES 2005: 30-46. Carolyn Whitnall, Elisabeth Oswald, François-Xavier Standaert: *The Myth of Generic DPA...and the Magic of Learning*. CT-RSA 2014: 183-205

Exploitation

- Profiled case: maximum likelihood

Omar Choudary, Markus G. Kuhn: *Efficient Template Attacks.* CARDIS 2013: 253-270

Exploitation

- Profiled case: maximum likelihood
- Unprofiled case:
  - Difference-of-Means
  - Correlation (CPA)
  - « On-the-fly » regression
  - Mutual Information Analysis (MIA)

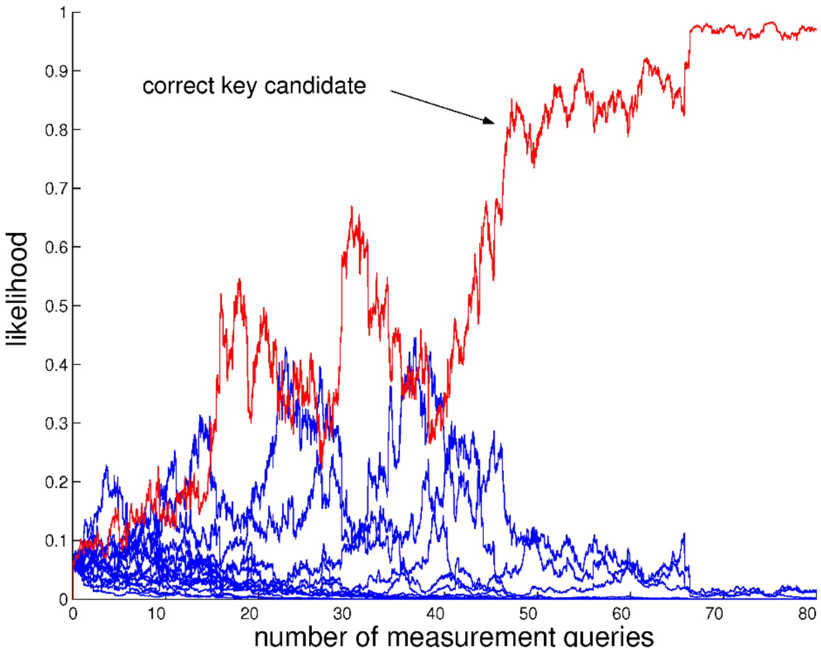
Omar Choudary, Markus G. Kuhn: *Efficient Template Attacks.* CARDIS 2013: 253-270. Paul C. Kocher, Joshua Jaffe, Benjamin Jun: *Differential Power Analysis*. CRYPTO 1999: 388-397. Eric Brier, Christophe Clavier, Francis Olivier: *Correlation Power Analysis with a Leakage Model.* CHES 2004: 16-29. Julien Doget, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert: *Univariate side channel attacks and leakage modeling*. J. Cryptographic Engineering 1(2): 123-144 (2011). Lejla Batina, Benedikt Gierlichs, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert, Nicolas Veyrat-Charvillon: *Mutual Information Analysis: a Comprehensive Study*. J. Cryptology 24(2): 269-291 (2011)

Exploitation

- Profiled case: maximum likelihood
- Unprofiled case:
  - Difference-of-Means
  - Correlation (CPA)
  - « On-the-fly » regression
  - Mutual Information Analysis (MIA)
- Advanced topic: analytical (algebraic) attacks

Omar Choudary, Markus G. Kuhn: *Efficient Template Attacks.* CARDIS 2013: 253-270. Paul C. Kocher, Joshua Jaffe, Benjamin Jun: *Differential Power Analysis*. CRYPTO 1999: 388-397. Eric Brier, Christophe Clavier, Francis Olivier: *Correlation Power Analysis with a Leakage Model.* CHES 2004: 16-29. Julien Doget, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert: *Univariate side channel attacks and leakage modeling*. J. Cryptographic Engineering 1(2): 123-144 (2011). Lejla Batina, Benedikt Gierlichs, Emmanuel Prouff, Matthieu Rivain, François-Xavier Standaert, Nicolas Veyrat-Charvillon: *Mutual Information Analysis: a Comprehensive Study*. J. Cryptology 24(2): 269-291 (2011). Nicolas Veyrat-Charvillon, Benoît Gérard, François-Xavier Standaert*: Soft Analytical Side-Channel Attacks*. ASIACRYPT (1) 2014: 282-296

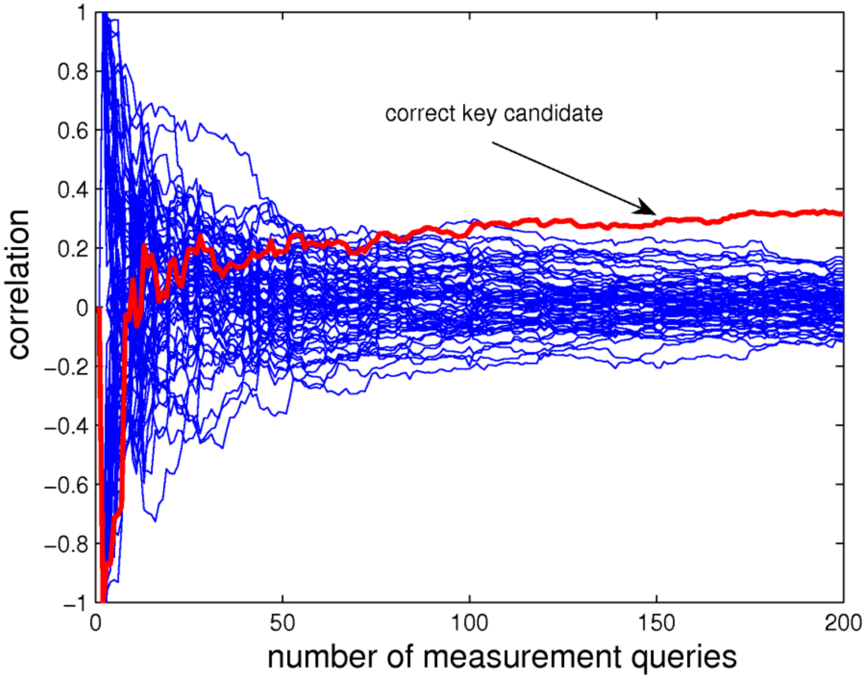
Gaussian templates



$$\tilde{k} = \underset{k^*}{\operatorname{argmax}} \prod_{i=1}^{q} \frac{1}{\sqrt{2 \cdot \pi} \cdot \sigma(L)} \cdot \exp\left(-\frac{1}{2} \cdot \left(\frac{l_i - m_i^{k^*}}{\sigma(L)}\right)^2\right)$$

- More efficient (why?)
- Outputs probabilities

CPA



$$\tilde{k} = \underset{k^*}{\operatorname{argmax}} \frac{\mathrm{E}(L \cdot M^{k^*}) - \mathrm{E}(L) \cdot \mathrm{E}(M^{k^*})}{\sigma(L) \cdot \sigma(M^{k^*})}$$

- Less efficient (why?)
- Outputs scores

CPA vs. Gaussian templates

- CPA: $$\tilde{k} = \operatorname*{argmax}_{k^*} \frac{\mathrm{E}\left(L \cdot M^{k^*}\right) - \mathrm{E}(L) \cdot \mathrm{E}(M^{k^*})}{\sigma(L) \cdot \sigma(M^{k^*})}$$

CPA vs. Gaussian templates

= 0 (normalization)

- CPA: $$\tilde{k} = \underset{k^*}{\operatorname{argmax}} \frac{\mathrm{E}\left(L \cdot M^{k^*}\right) - \mathrm{E}(L) \cdot \mathrm{E}(M^{k^*})}{\sigma(L) \cdot \sigma(M^{k^*})}$$

CPA vs. Gaussian templates

= 0 (normalization)

- CPA: $\tilde{k} = \underset{k^*}{\operatorname{argmax}} \frac{\mathrm{E}\left(L \cdot M^{k^*}\right) - \mathrm{E}(L) \cdot \mathrm{E}(M^{k^*})}{\sigma(L) \cdot \sigma(M^{k^*})}$

independent of *k**

CPA vs. Gaussian templates

= 0 (normalization)

- CPA: $$\tilde{k} = \underset{k^*}{\operatorname{argmax}} \frac{\mathrm{E}\left(L \cdot M^{k^*}\right) - \mathrm{E}(L) \cdot \mathrm{E}(M^{k^*})}{\sigma(L) \cdot \sigma(M^{k^*})}$$

independent of *k**

asymptotically independent of k*

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \, \mathrm{E}\left(L \cdot M^{k^*}\right)$

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \operatorname*{argmax}_{k^*} \mathrm{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates:

$$\tilde{k} = \operatorname*{argmax}_{k^*} \prod_{i=1}^{q} \frac{1}{\sqrt{2 \cdot \pi} \cdot \sigma(L)} \cdot \exp\left(-\frac{1}{2} \cdot \left(\frac{l_i - m_i^{k^*}}{\sigma(L)}\right)^2\right)$$

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}}\, \mathrm{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates:

$$\tilde{k} = \underset{k^*}{\operatorname{argmax}} \prod_{i=1}^{q} \frac{1}{\sqrt{2 \cdot \pi} \cdot \sigma(L)} \cdot \exp\left(-\frac{1}{2} \cdot \left(\frac{l_i - m_i^{k^*}}{\sigma(L)}\right)^2\right)$$

independent of k^*

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \operatorname{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates:

$$\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \prod_{i=1}^{q} \exp\left(-\frac{1}{2} \cdot \left(\frac{l_i - m_i^{k^*}}{\sigma(L)}\right)^2\right)$$

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \mathrm{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates:

$$\tilde{k} \propto \underset{k^*}{\operatorname{argmin}} \mathrm{E}(L^2) - 2 \cdot \mathrm{E}\left(L \cdot M^{k^*}\right) + \mathrm{E}(\left(M^{k^*}\right)^2)$$

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \mathrm{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates:

$$\tilde{k} \propto \underset{k^*}{\operatorname{argmin}} \mathrm{E}(L^2) - 2 \cdot \mathrm{E}\left(L \cdot M^{k^*}\right) + \mathrm{E}(\left(M^{k^*}\right)^2)$$

independent of *k**

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \, \mathrm{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates:

$$\tilde{k} \propto \underset{k^*}{\operatorname{argmin}} \, \mathrm{E}(L^2) - 2 \cdot \mathrm{E}\left(L \cdot M^{k^*}\right) + \mathrm{E}\left(\left(M^{k^*}\right)^2\right)$$

independent of *k**

asymptotivally independent of k*

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \operatorname*{argmax}_{k^*} \mathrm{E}\left(L \cdot M^{k^*}\right)$
- Gaussian templates: $\tilde{k} \propto \operatorname*{argmax}_{k^*} \mathrm{E}\left(L \cdot M^{k^*}\right)$

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \operatorname{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates: $\tilde{k} \propto \underset{k^*}{\operatorname{argmax}} \operatorname{E}\left(L \cdot M^{k^*}\right)$

$\Rightarrow$ Both attacks are asymtotically equivalent

- For 1st-order leakages
  - i.e., unprotected implementations
- Given they exploit the same model

CPA vs. Gaussian templates

- CPA: $\tilde{k} \propto \underset{k^*}{\mathrm{argmax}}\, \mathrm{E}\left(L \cdot M^{k^*}\right)$

- Gaussian templates: $\tilde{k} \propto \underset{k^*}{\mathrm{argmax}}\, \mathrm{E}\left(L \cdot M^{k^*}\right)$

$\Rightarrow$ Both attacks are asymtotically equivalent
- For 1st-order leakages
  - i.e., unprotected implementations
- Given they exploit the same model

$\Rightarrow$ Gaussian templates outperforms CPA because it (usually) exploits a better (profiled) **model**

Stefan Mangard, Elisabeth Oswald, François-Xavier Standaert: *One for all - all for one: unifying standard differential power analysis attacks*. IET Information Security 5(2): 100-110 (2011)

Outline

- Preliminary questions / definitions
- Side-channel basics (attack steps)
- **Noise (aka hardware) is not enough**
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- Mitigating hardware defaults (is hard)
- Transparency is needed (open source)
- Summary and conclusions

First-order CPA (I)

- **Lemma 1.** The mutual information between two normally distributed random variables X, Y with means μ_X, μ_Y and variances σ_X^2, σ_Y^2 equals:

$$\mathrm{MI}(X;Y) = -\frac{1}{2}\log_2(1-\rho(X,Y)^2)$$

Stefan Mangard, Elisabeth Oswald, François-Xavier Standaert: *One for all - all for one: unifying standard differential power analysis attacks*

First-order CPA (I)

- **Lemma 1.** The mutual information between two normally distributed random variables X, Y with means μ_X, μ_Y and variances σ_X^2, σ_Y^2 equals:

$$\mathrm{MI}(X;Y) = -\frac{1}{2}\log_2(1 - \rho(X,Y)^2)$$

- **Lemma 2.** In a CPA, the number of samples required to distinguish the corrrect key with model M_k from the other key candidates with models M_{k*} is $\propto \frac{c}{\rho(M_k,L)^2}$ (*with c a small constant depending on the SR & # of key candidates*)

Stefan Mangard, Elisabeth Oswald, François-Xavier Standaert: *One for all - all for one: unifying standard differential power analysis attacks*. IET Information Security 5(2): 100-110 (2011). Stefan Mangard: Hardware Countermeasures against DPA ? A Statistical Analysis of Their Effectiveness. CT-RSA 2004: 222-235

First-order CPA (II)

- **Lemma 3.** Let X, Y and L be three random variables s.t. $Y = X + N_1$ and $L = Y + N_2$ with N_1 and N_2 two additive noise variables. Then:

$$\rho(X, L) = \rho(X, Y) \cdot \rho(Y, L)$$

François-Xavier Standaert, Eric Peeters, Gaël Rouvroy, Jean-Jacques Quisquater, *An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays*, Proceedings of the IEEE, vol. 94, num. 2, pp 383-394, 2006

First-order CPA (II)

- **Lemma 3.** Let X, Y and L be three random variables s.t. $Y = X + N_1$and $L = Y + N_2$ with N_1 and N_2 two additive noise variables. Then:

$$\rho(X, L) = \rho(X, Y) \cdot \rho(Y, L)$$

- **Lemma 4.** The correlation coefficient between the sum of n independent and identically distributed random variables and the sum of the first $m < n$ of these equals $\sqrt{m/n}$

François-Xavier Standaert, Eric Peeters, Gaël Rouvroy, Jean-Jacques Quisquater, *An Overview of Power Analysis Attacks Against Field Programmable Gate Arrays*, Proceedings of the IEEE, vol. 94, num. 2, pp 383-394, 2006

Paper & pencil estimations (I)

- FPGA implementation of the AES
- Adversary targeting the 1st byte of key
- Hamming weight leakage function/model
- 8-bit loop architecture broken in 10 traces

Paper & pencil estimations (I)

- FPGA implementation of the AES
- Adversary targeting the 1st byte of key
- Hamming weight leakage function/model
- 8-bit loop architecture broken in 10 traces

- How does the attack data complexity scale
  - For a 32-bit architecture?
    - i.e., with 24 bits of « algorithmic noise »
  - For a 128-bit architecture?
    - i.e., with 120 bits of « algorithmic noise »

Paper & pencil estimations (II)

- Hint: $L = \mathrm{M} + \mathrm{N} = (M_P + M_U) + N$

Paper & pencil estimations (II)

- Hint: $L = \mathrm{M} + \mathrm{N} = (M_P + M_U) + N$
- Lemma 3: $\rho(M_P, L) =$

Paper & pencil estimations (II)

- Hint: $L = \mathrm{M} + \mathrm{N} = (M_P + M_U) + N$
- Lemma 3: $\rho(M_P, L) = \rho(M_P, M) \cdot \rho(M, L)$
- Lemma 4: $\rho(M_P, M) = ?$
  - For the 8-bit architecture:
  - For the 32-bit architecture:
  - For the 128-bit architecture:

Paper & pencil estimations (II)

- Hint: $L = \mathrm{M} + \mathrm{N} = (M_P + M_U) + N$
- Lemma 3: $\rho(M_P, L) = \rho(M_P, M) \cdot \rho(M, L)$
- Lemma 4: $\rho(M_P, M) = ?$
  - For the 8-bit architecture: $\sqrt{8/8}$
  - For the 32-bit architecture:
  - For the 128-bit architecture:

Paper & pencil estimations (II)

- Hint: $L = \mathrm{M} + \mathrm{N} = (M_P + M_U) + N$
- Lemma 3: $\rho(M_P, L) = \rho(M_P, M) \cdot \rho(M, L)$
- Lemma 4: $\rho(M_P, M) = ?$
  - For the 8-bit architecture: $\sqrt{8/8}$
  - For the 32-bit architecture: $\sqrt{8/32}$
  - For the 128-bit architecture: $\sqrt{8/128}$

Paper & pencil estimations (II)

- Hint: $L = \mathrm{M} + \mathrm{N} = (M_P + M_U) + N$
- Lemma 3: $\rho(M_P, L) = \rho(M_P, M) \cdot \rho(M, L)$
- Lemma 4: $\rho(M_P, M) = ?$
  - For the 8-bit architecture: $\sqrt{8/8}$
  - For the 32-bit architecture: $\sqrt{8/32}$
  - For the 128-bit architecture: $\sqrt{8/128}$
- Lemma 2: $\frac{c}{(\sqrt{8/8} \cdot \rho(M,L))^2} = 10$

Paper & pencil estimations (III)

- Data complexity for the 32-bit case:
- Data complexity for the 128-bit case:

Paper & pencil estimations (III)

- Data complexity for the 32-bit case: 40
- Data complexity for the 128-bit case: 160

- Is noise an efficient countermeasure?

Paper & pencil estimations (III)

- Data complexity for the 32-bit case: 40
- Data complexity for the 128-bit case: 160

- Is noise an efficient countermeasure?
  - 32-bit case: security $\times 4$, cost $\times ?$

Paper & pencil estimations (III)

- Data complexity for the 32-bit case: 40
- Data complexity for the 128-bit case: 160

- Is noise an efficient countermeasure?
  - 32-bit case: security $\times 4$, cost $\times 4$

- How to trade data for time?

Paper & pencil estimations (III)

- Data complexity for the 32-bit case: 40
- Data complexity for the 128-bit case: 160

- Is noise an efficient countermeasure?
  - 32-bit case: security $\times 4$, cost $\times 4$

- How to trade data for time?
  - Target more than 8 bits at once
  - Cancels (a part of) the « algorithmic noise »
  - e.g., 32-bit architecture: $\rho(M_P, M) =$

Paper & pencil estimations (III)

- Data complexity for the 32-bit case: 40
- Data complexity for the 128-bit case: 160

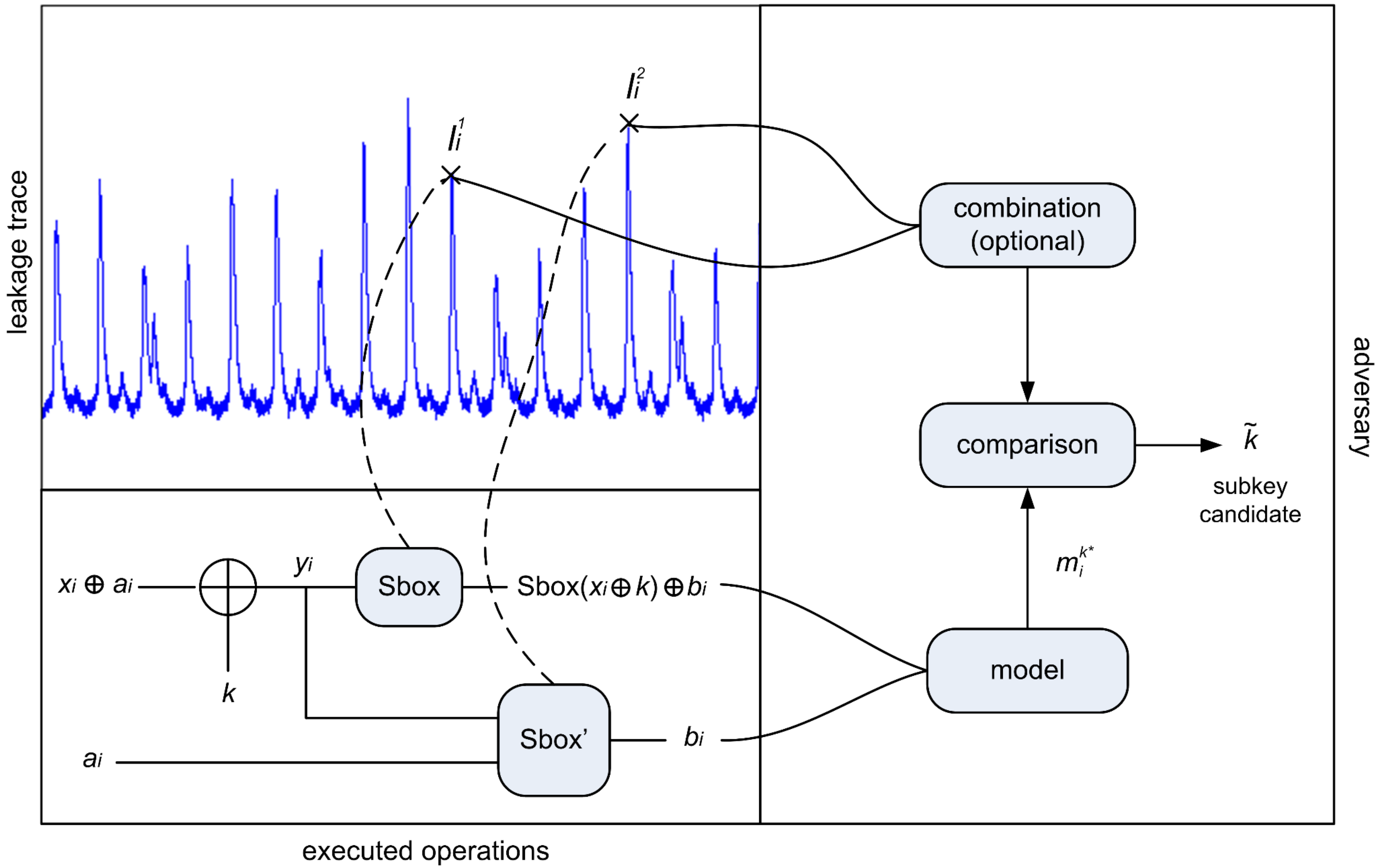
- Is noise an efficient countermeasure?
  - 32-bit case: security $\times 4$, cost $\times 4$

- How to trade data for time?
  - Target more than 8 bits at once
  - Cancels (a part of) the « algorithmic noise »
  - e.g., 32-bit architecture: $\rho(M_P, M) = \sqrt{32/32}$
  - (10 < data complexity < 40 because of *c*)

Outline

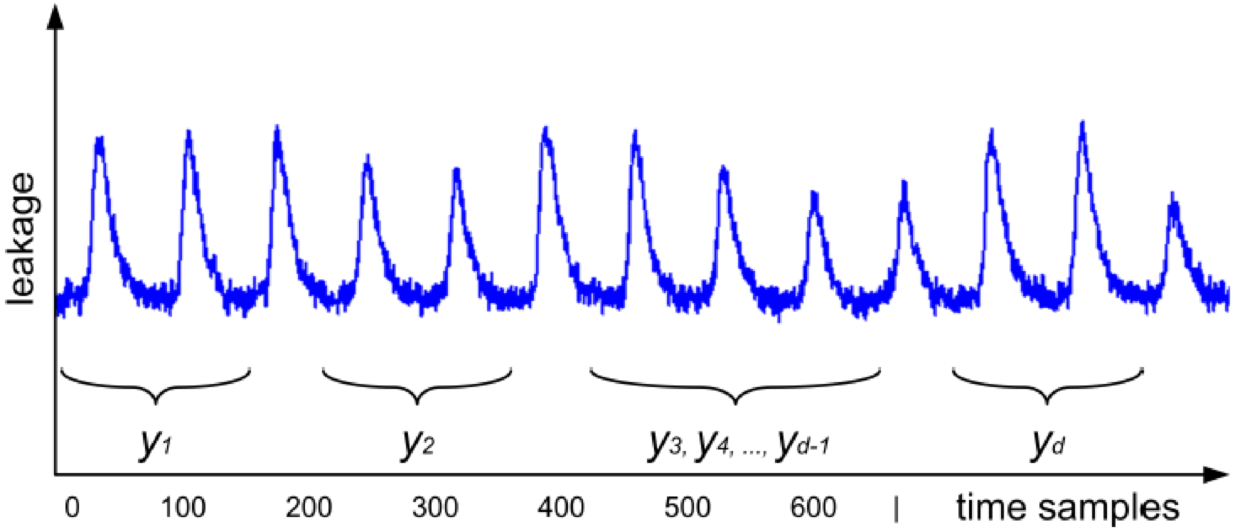
- Preliminary questions / definitions
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- **Noise amplification (aka masking)**
- Reductions help (aka leakage resilience)
- Mitigating hardware defaults (is hard)
- Transparency is needed (open source)
- Summary and conclusions

Masking & 2nd-order DPA



More generally (I)

- Let $z = S(x \oplus k) = S(y)$ be a leaking S-box
- Let $y = y_1 \oplus y_2 \oplus \cdots \oplus y_d$ be a sharing of y



- Perform computations on "shared" variables

More generally (II)

- Linear operations: $\mathrm{f(a)} = \mathrm{f}(a_1) \oplus \mathrm{f}(a_2) \oplus \cdots \oplus \mathrm{f}(a_d)$

More generally (II)

- Linear operations: $\mathrm{f(a)} = \mathrm{f}(a_1) \oplus \mathrm{f}(a_2) \oplus \cdots \oplus \mathrm{f}(a_d)$
- Multiplications: $\mathrm{c} = a \times b$ in three steps

Yuval Ishai, Amit Sahai, David Wagner: *Private Circuits: Securing Hardware against Probing Attacks*. CRYPTO 2003: 463-481. Matthieu Rivain, Emmanuel Prouff*: Provably Secure Higher-Order Masking of AES*. CHES 2010: 413-427

More generally (II)

- Linear operations: $\mathrm{f(a)} = \mathrm{f}(a_1) \oplus \mathrm{f}(a_2) \oplus \cdots \oplus \mathrm{f}(a_d)$
- Multiplications: $\mathrm{c} = a \times b$ in three steps

$$\begin{bmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{bmatrix}$$

partial products

Yuval Ishai, Amit Sahai, David Wagner: *Private Circuits: Securing Hardware against Probing Attacks*. CRYPTO 2003: 463-481. Matthieu Rivain, Emmanuel Prouff: *Provably Secure Higher-Order Masking of AES*. CHES 2010: 413-427

More generally (II)

- Linear operations: $f(a) = f(a_1) \oplus f(a_2) \oplus \cdots \oplus f(a_d)$
- Multiplications: $c = a \times b$ in three steps

$$\begin{bmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{bmatrix} + \begin{bmatrix} 0 & r_1 & r_2 \\ -r_1 & 0 & r_3 \\ -r_2 & r_3 & 0 \end{bmatrix}$$

partial products refreshing

Yuval Ishai, Amit Sahai, David Wagner: *Private Circuits: Securing Hardware against Probing Attacks*. CRYPTO 2003: 463-481. Matthieu Rivain, Emmanuel Prouff: *Provably Secure Higher-Order Masking of AES*. CHES 2010: 413-427

More generally (II)

- Linear operations: $\mathrm{f(a)} = \mathrm{f}(a_1) \oplus \mathrm{f}(a_2) \oplus \cdots \oplus \mathrm{f}(a_d)$

- Multiplications: $\mathrm{c} = a \times b$ in three steps

$$\begin{bmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{bmatrix} + \begin{bmatrix} 0 & r_1 & r_2 \\ -r_1 & 0 & r_3 \\ -r_2 & r_3 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

partial products refreshing compression

Yuval Ishai, Amit Sahai, David Wagner: *Private Circuits: Securing Hardware against Probing Attacks*. CRYPTO 2003: 463-481. Matthieu Rivain, Emmanuel Prouff: *Provably Secure Higher-Order Masking of AES*. CHES 2010: 413-427

More generally (II)

- Linear operations: $\mathrm{f}(\mathrm{a}) = \mathrm{f}(a_1) \oplus \mathrm{f}(a_2) \oplus \cdots \oplus \mathrm{f}(a_d)$
- Multiplications: $\mathrm{c} = a \times b$ in three steps

$$\begin{bmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{bmatrix} + \begin{bmatrix} 0 & r_1 & r_2 \\ -r_1 & 0 & r_3 \\ -r_2 & r_3 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

partial products — refreshing — compression

$\Rightarrow$ Quadratic overheads & randomness

Yuval Ishai, Amit Sahai, David Wagner: *Private Circuits: Securing Hardware against Probing Attacks*. CRYPTO 2003: 463-481. Matthieu Rivain, Emmanuel Prouff: *Provably Secure Higher-Order Masking of AES*. CHES 2010: 413-427

More generally (II)

- Linear operations: $f(a) = f(a_1) \oplus f(a_2) \oplus \cdots \oplus f(a_d)$
- Multiplications: $c = a \times b$ in three steps

$$\begin{bmatrix} a_1 b_1 & a_1 b_2 & a_1 b_3 \\ a_2 b_1 & a_2 b_2 & a_2 b_3 \\ a_3 b_1 & a_3 b_2 & a_3 b_3 \end{bmatrix} + \begin{bmatrix} 0 & r_1 & r_2 \\ -r_1 & 0 & r_3 \\ -r_2 & r_3 & 0 \end{bmatrix} \Rightarrow \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}$$

partial products refreshing compression

$\Rightarrow$ Quadratic overheads & randomness

$\Rightarrow$ Composable (from gadgets to circuits)

Yuval Ishai, Amit Sahai, David Wagner: *Private Circuits: Securing Hardware against Probing Attacks*. CRYPTO 2003: 463-481. Matthieu Rivain, Emmanuel Prouff: *Provably Secure Higher-Order Masking of AES*. CHES 2010: 413-427. Gilles Barthe, Sonia Belaïd, François Dupressoir, Pierre-Alain Fouque, Benjamin Grégoire, Pierre-Yves Strub, Rébecca Zucchini: *Strong Non-Interference and Type-Directed Higher-Order Masking*. ACM Conference on Computer and Communications Security 2016: 116-129

Main theorem (informal)

- Assume leakage variables $L_{Z_i} = \delta(Z_i) + N$ s.t.
  - $\mathrm{MI}(Z_i; L_{Z_i}) \leq \frac{c}{d}$ (why d? – or d^2 in proofs)
  - The leakages of the shares are independent
- For a masking scheme with *d* shares
- And an adversary using *m* measurements
- Then: $\mathrm{SR} \leq 1 - \left(1 - \mathrm{MI}(Z_i; L_{Z_i})^d\right)^m$

Alexandre Duc, Sebastian Faust, François-Xavier Standaert: Making Masking Security Proofs Concrete - Or How to Evaluate the Security of Any Leaking Device. EUROCRYPT (1) 2015: 401-429

Main theorem (informal)

- Assume leakage variables $L_{Z_i} = \delta(Z_i) + N$ s.t.
  - $\mathrm{MI}(Z_i; L_{Z_i}) \leq \frac{c}{d}$ (multiplications)
  - The leakages of the shares are independent
- For a masking scheme with *d* shares
- And an adversary using *m* measurements

- Then: $\mathrm{SR} \leq 1 - \left(1 - \mathrm{MI}(Z_i; L_{Z_i})^d\right)^m$

Alexandre Duc, Sebastian Faust, François-Xavier Standaert: *Making Masking Security Proofs Concrete - Or How to Evaluate the Security of Any Leaking Device*. EUROCRYPT (1) 2015: 401-429

Main theorem (informal)

- Assume leakage variables $L_{Z_i} = \delta(Z_i) + N$ s.t.
  - $\mathrm{MI}(Z_i; L_{Z_i}) \leq \frac{c}{d}$ (multiplications)
  - The leakages of the shares are independent
- For a masking scheme with *d* shares
- And an adversary using *m* measurements

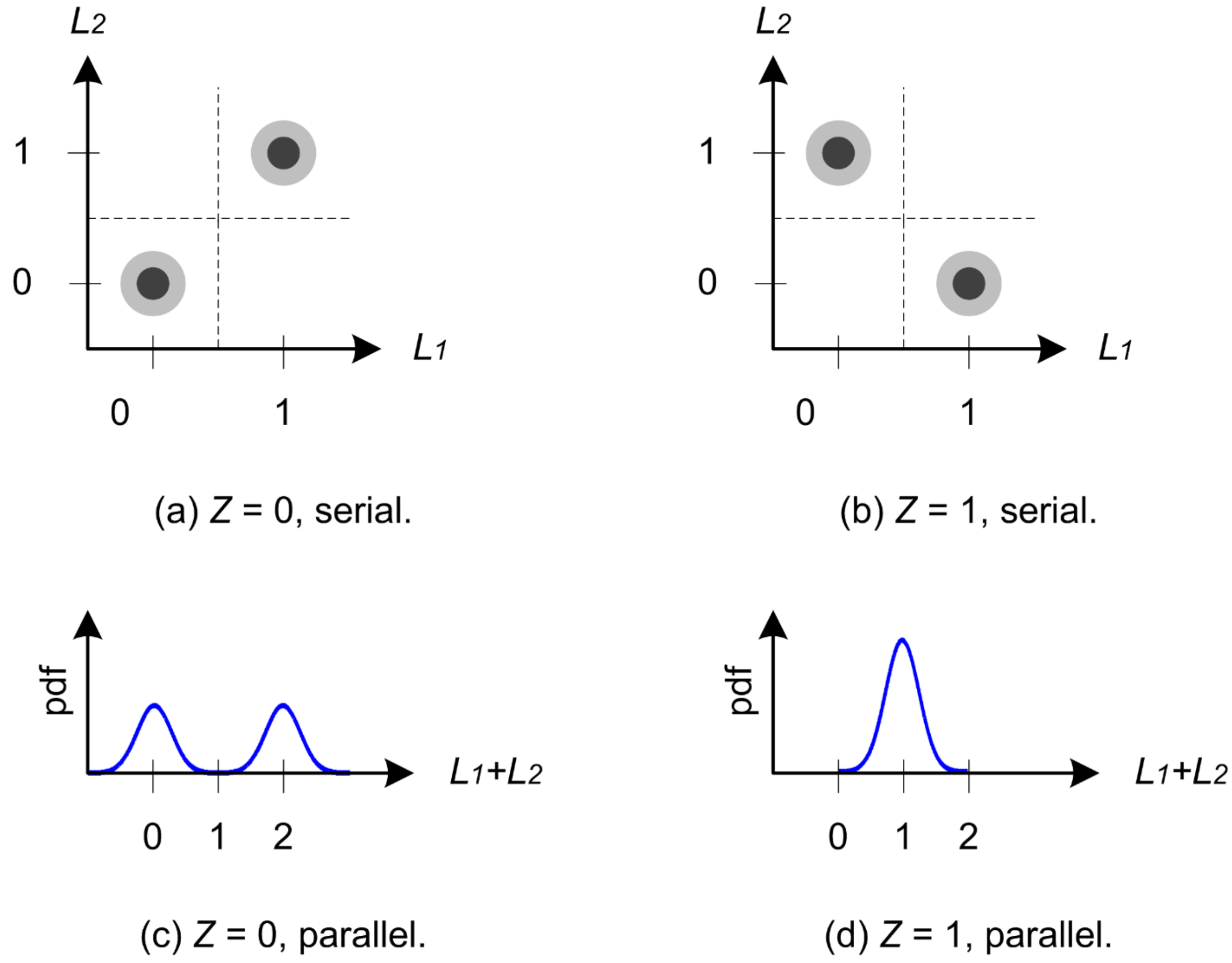
- Then: $\mathrm{SR} \leq 1 - \left(1 - \mathrm{MI}(Z_i; L_{Z_i})^d\right)^m$

- For $m = 1$, $\mathrm{SR} \leq \mathrm{MI}(Z_i; L_{Z_i})^d \propto (\sigma_N^2)^d$
- (Intuitively ≈ "noisy" piling up lemma)

Alexandre Duc, Sebastian Faust, François-Xavier Standaert: Making Masking Security Proofs Concrete - Or How to Evaluate the Security of Any Leaking Device. EUROCRYPT (1) 2015: 401-429

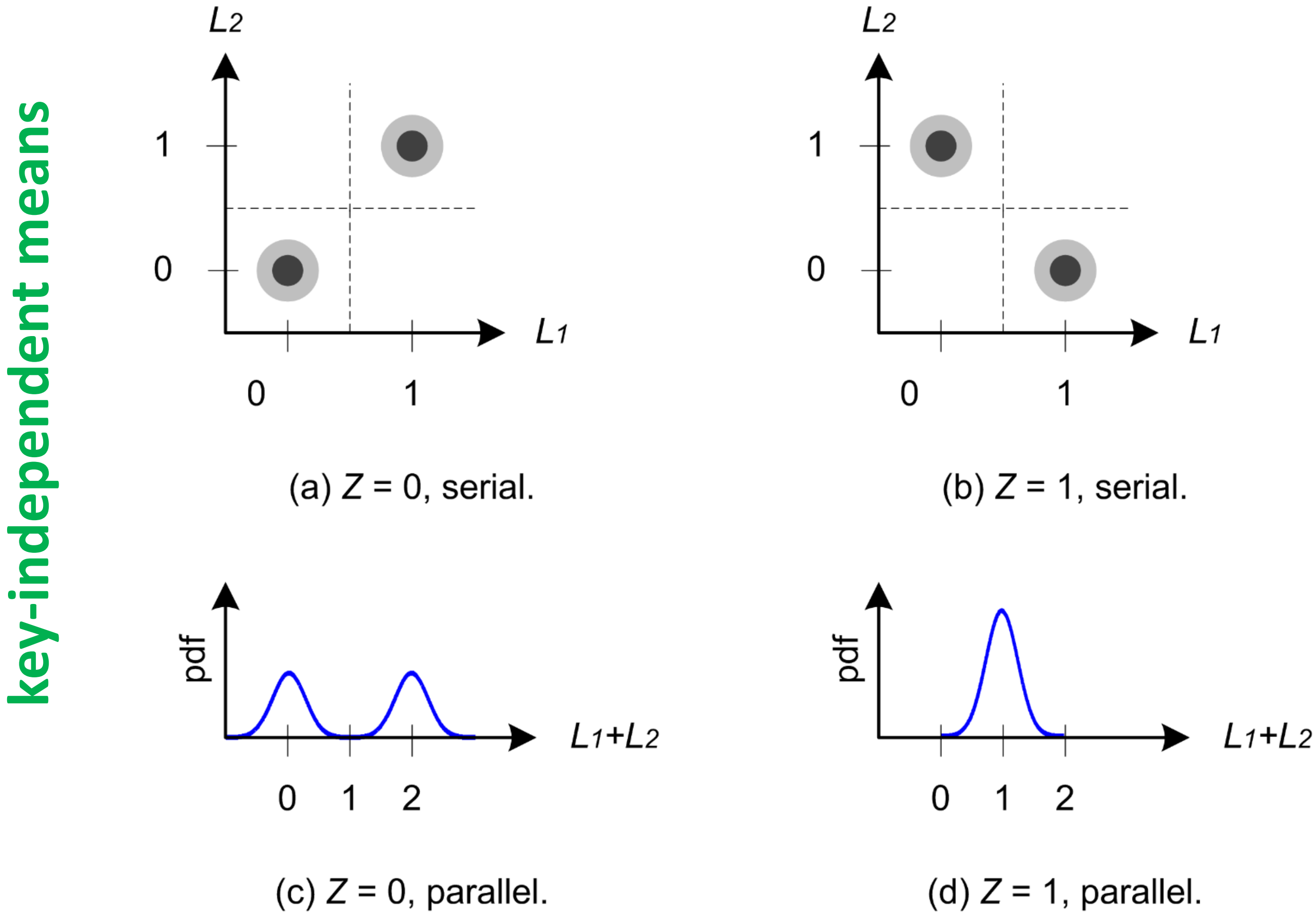
Statistical intuition

- 1-bit, 2-shares example



Statistical intuition

- 1-bit, 2-shares example



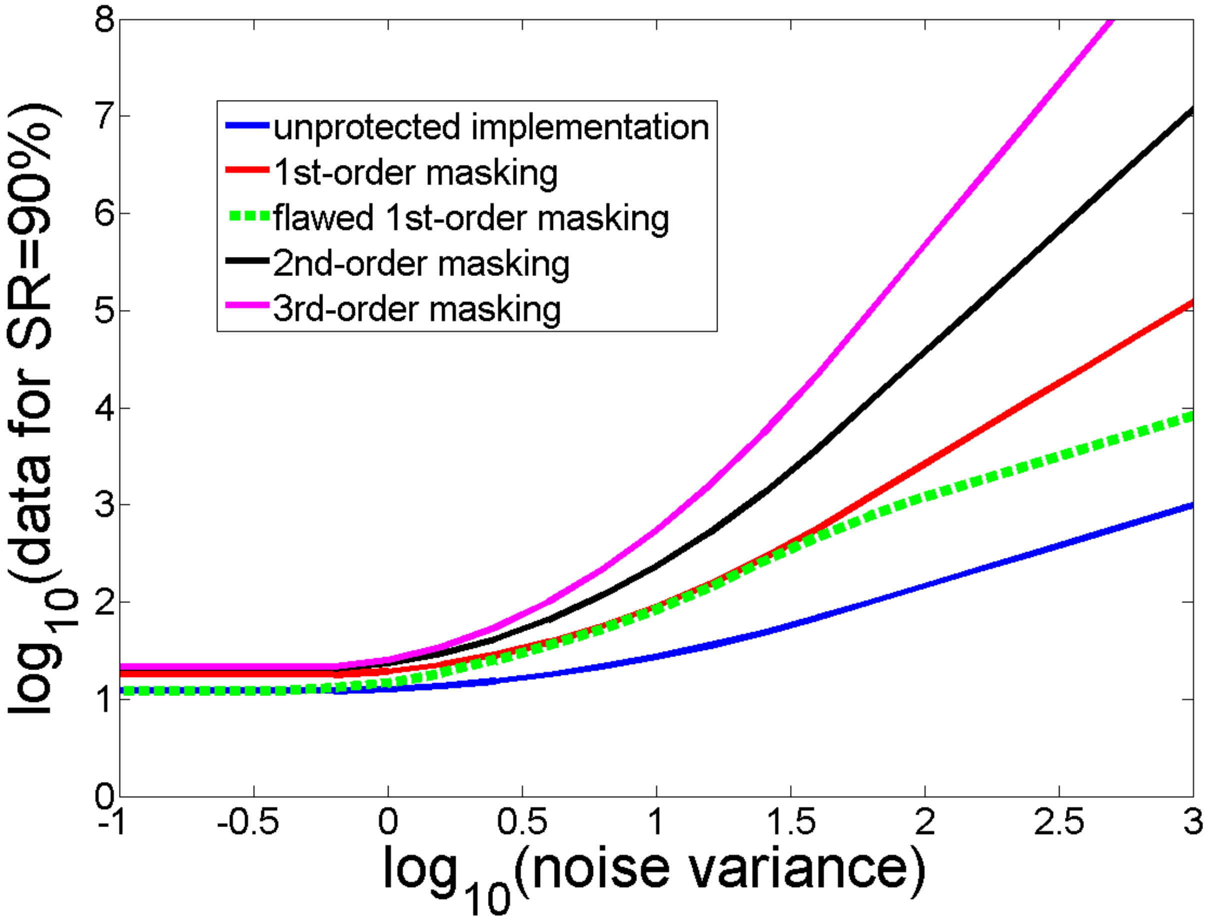
(a) Z = 0, serial.

(b) Z = 1, serial.

(c) Z = 0, parallel.

(d) Z = 1, parallel.

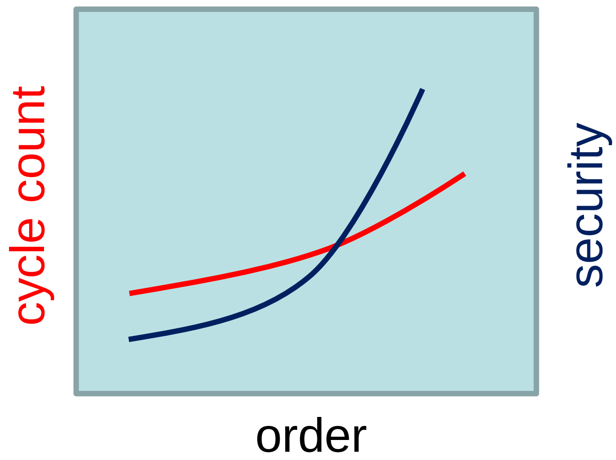
- Slope of the IT curves = d (*if independent leaks*)



Wrapping up

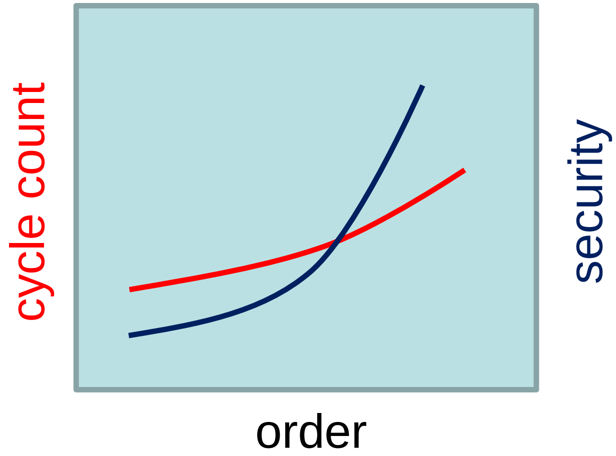
- Is masking an efficient countermeasure?
  - Security (data) is exponential in d
  - Cost is [...]

- Is masking an efficient countermeasure?
  - Security (data) is exponential in d
  - Cost is […] quadratic in d



Wrapping up

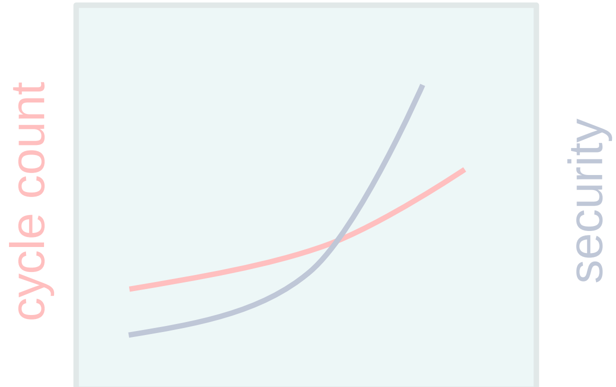
- Is masking an efficient countermeasure?
  - Security (data) is exponential in d
  - Cost is [...] quadratic in d



- If the leakages are noisy and independent (!)

Wrapping up

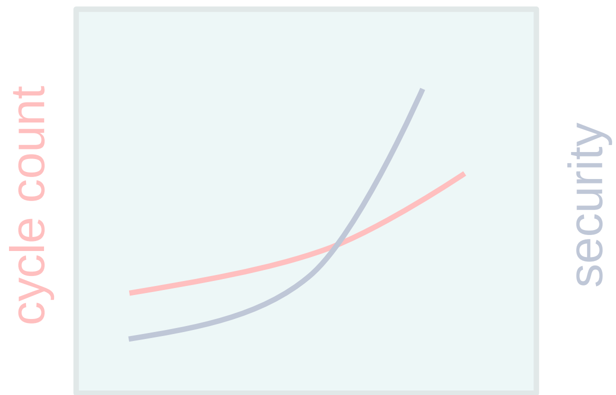
- Is masking an efficient countermeasure?
  - Security (data) is exponential in d
  - Cost is [...] quadratic in d



- If the leakages are noisy and independent (!)
- How does the time complexity scale in d?

Wrapping up

- Is masking an efficient countermeasure?
  - Security (data) is exponential in d
  - Cost is [...] quadratic in d

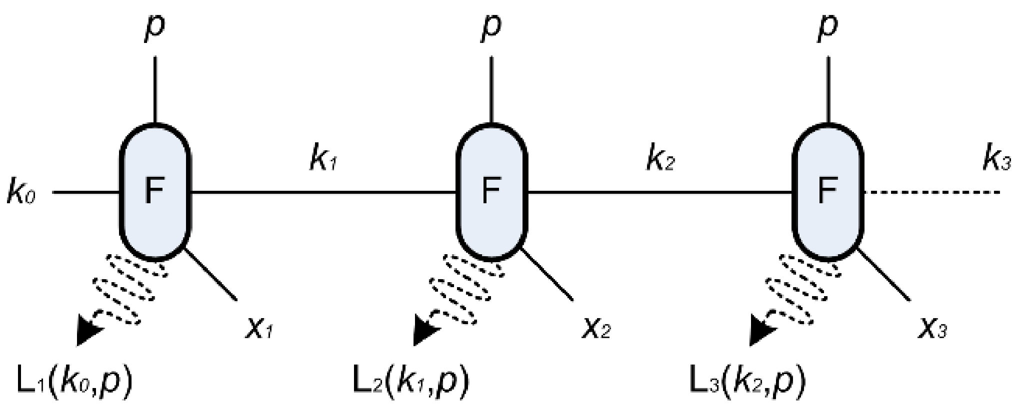


- If the leakages are noisy and independent (!)
- How does the time complexity scale in d?
  - Depends on the implem. (e.g., serial or //)

Outline

- Preliminary questions / definitions
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- **Reductions help (aka leakage resilience)**
- Mitigating hardware defaults (is hard)
- Transparency is needed (open source)
- Summary and conclusions

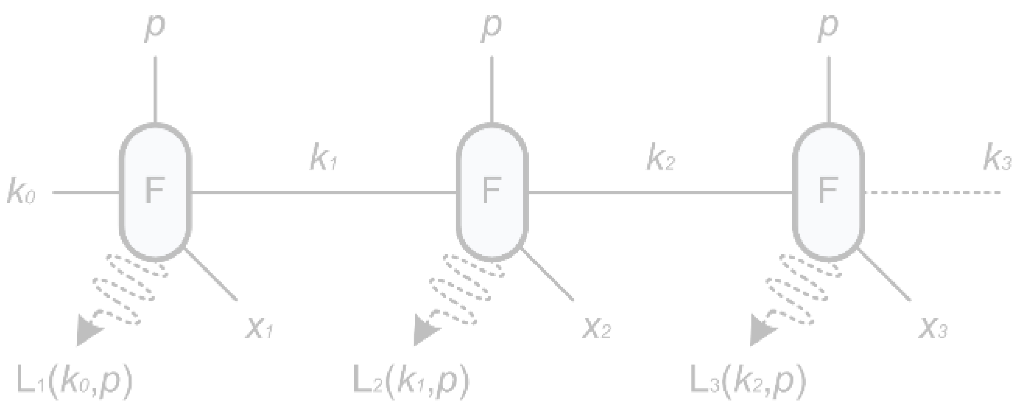
- Most natural construction: forward-secure PRG



Mihir Bellare, Bennet S. Yee: *Forward-Security in Private-Key Cryptography*. CT-RSA 2003: 1-18

Stateful PRGs

- Most natural construction: forward-secure PRG

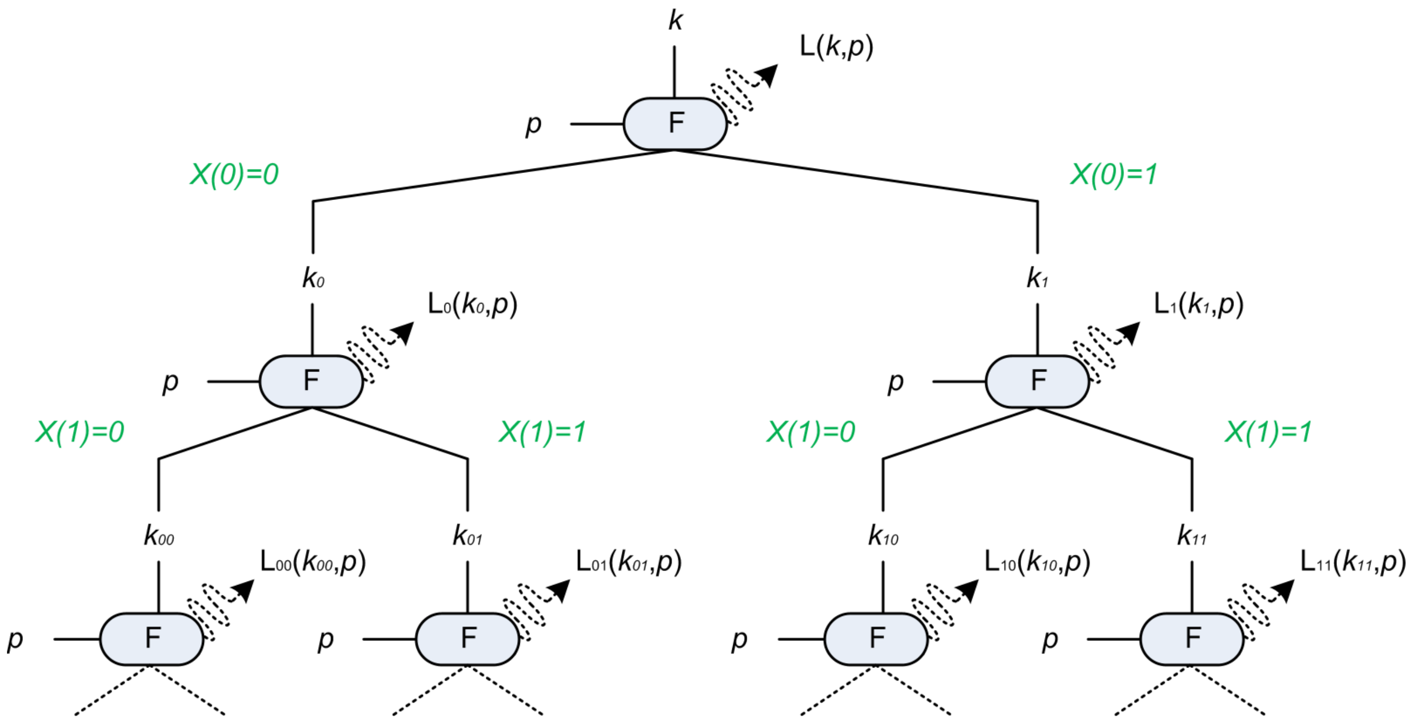


- Re-keying impact: bounds the number of (noisy) measurements per key (*prevents averaging*)

Mihir Bellare, Bennet S. Yee: *Forward-Security in Private-Key Cryptography*. CT-RSA 2003: 1-18

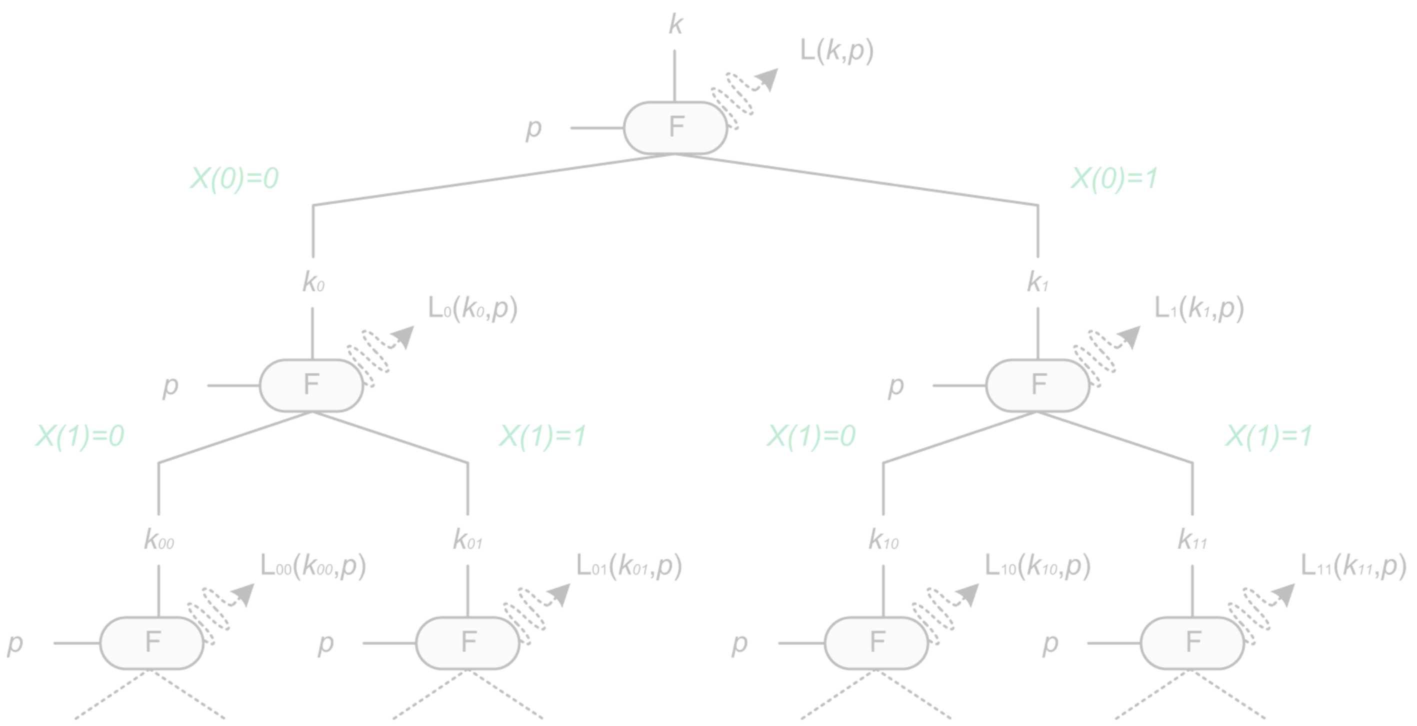
Stateless PRFs (or PRPs)

- Most natural construction: GGM tree



Oded Goldreich, Shafi Goldwasser, Silvio Micali: *How to Construct Random Functions*. FOCS 1984: 464-479

- Most natural construction: GGM tree



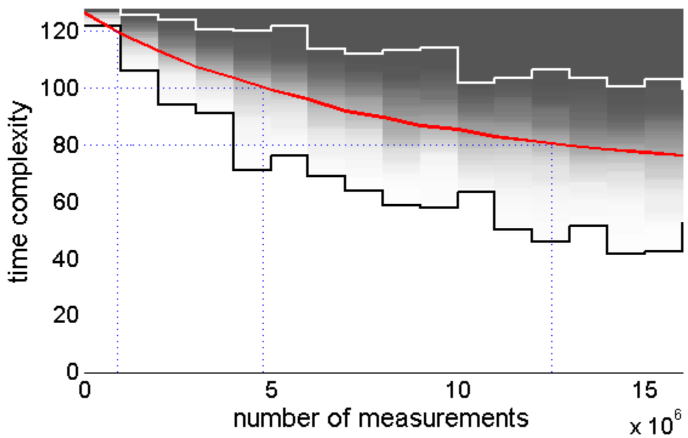
- Re-keying impact: bounds the number of noise-free observations per key (*allows averaging*)

Oded Goldreich, Shafi Goldwasser, Silvio Micali: *How to Construct Random Functions*. FOCS 1984: 464-479

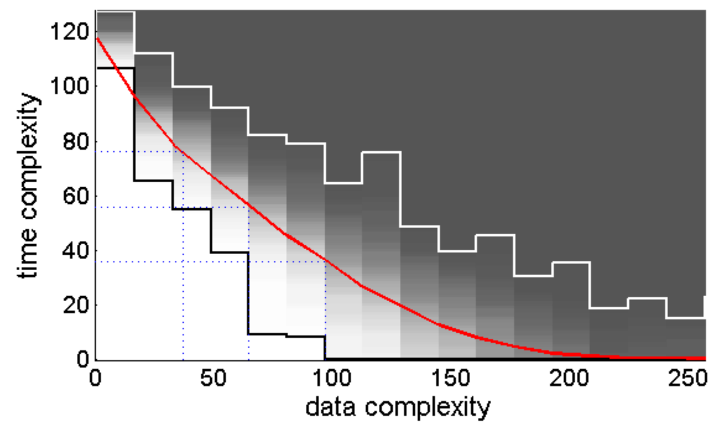
The stateful / stateless separation

- Key recovery security (standard DPA):

PRG



PRF



- « Bounded security » for the PRG only
  - (Analytical/algebraic attacks not considered)

Sonia Belaïd, Vincent Grosso, François-Xavier Standaert: *Masking and leakage-resilient primitives: One, the other(s) or both?* Cryptography and Communications 7(1): 163-184 (2015)

Pragmatic view

- A call to a stateless primitive is always needed
  - For initialization / randomization
  - For authentication and encryption

Olivier Pereira, François-Xavier Standaert, Srinivas Vivek: *Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives*. ACM Conference on Computer and Communications Security 2015: 96-108

Pragmatic view

- A call to a stateless primitive is always needed
  - For initialization / randomization
  - For authentication and encryption

- But we can try to encrypt large messages with a single call to this (more expensive) primitive

Olivier Pereira, François-Xavier Standaert, Srinivas Vivek: *Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives*. ACM Conference on Computer and Communications Security 2015: 96-108

Pragmatic view

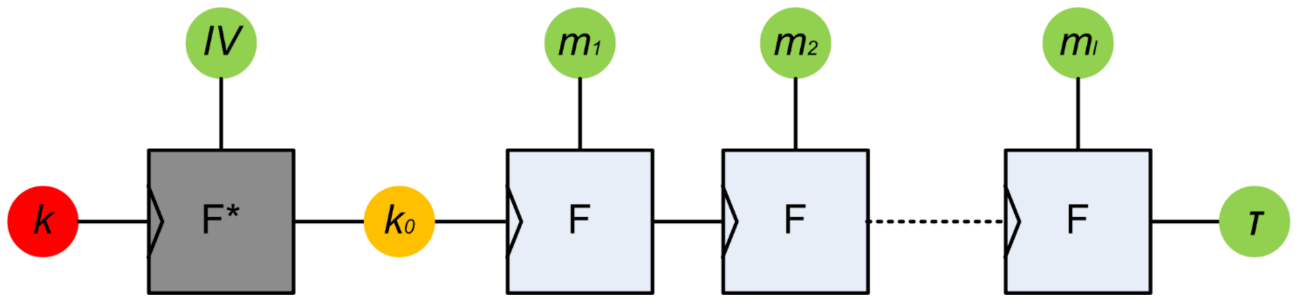
- A call to a stateless primitive is always needed
  - For initialization / randomization
  - For authentication and encryption

- But we can try to encrypt large messages with a single call to this (more expensive) primitive

- And to use leakage-resilient PRGs otherwise

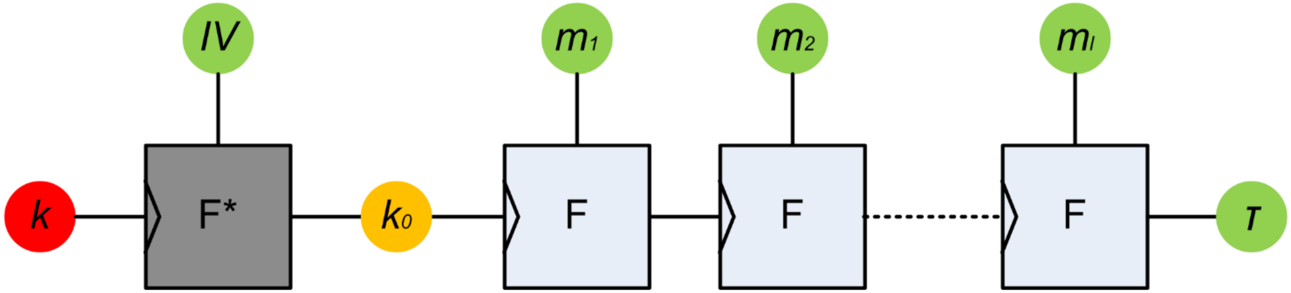
Olivier Pereira, François-Xavier Standaert, Srinivas Vivek: *Leakage-Resilient Authentication and Encryption from Symmetric Cryptographic Primitives*. ACM Conference on Computer and Communications Security 2015: 96-108

Example I: authentication



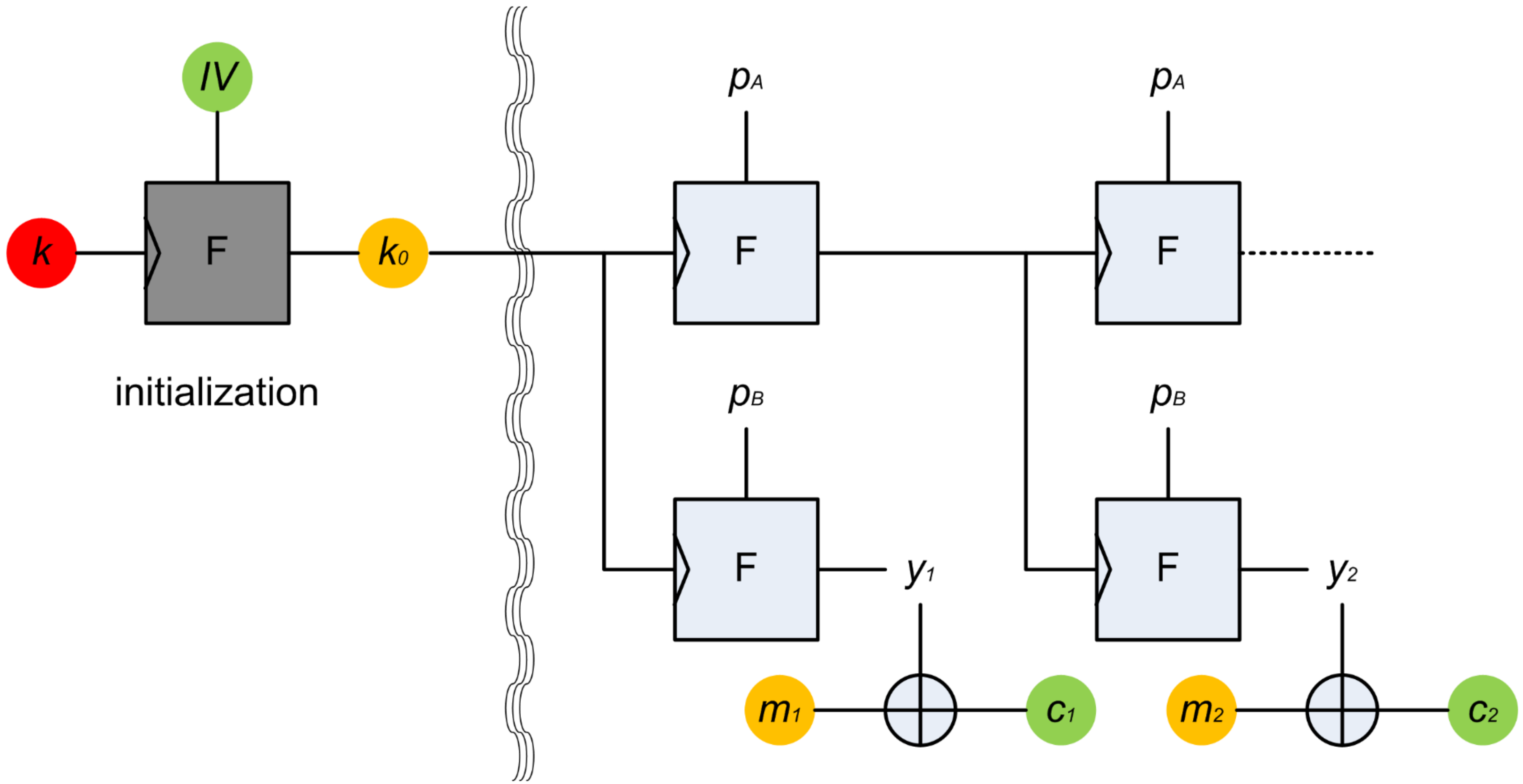
- Green: public value, orange: ephemeral secret, red: long-term secret (protected with leak-free F*)

Example I: authentication



- Green: public value, orange: ephemeral secret, red: long-term secret (protected with leak-free F*)
- τ unforgeable even with leakage (during enc.)
- Security of 1-block ≈ security of *l*-blocks
- & high-security levels expected
  - Because it is an unpredictability game!

Example II: encryption



- Similar reduction but lower security levels
  - Because it is an indistinguishability game!

Additional remarks (I)

- In theory, the proof challenge remains open

François-Xavier Standaert, Olivier Pereira, Yu Yu: *Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions.* CRYPTO (1) 2013: 335-352. Jake Longo, Daniel P. Martin, Elisabeth Oswald, Daniel Page, Martijn Stam, Michael Tunstall: *Simulatable Leakage: Analysis, Pitfalls, and New Constructions*. ASIACRYPT (1) 2014: 223-242

  - Yet, the pragmatic model seems sound

Additional remarks (I)

- In theory, the proof challenge remains open

François-Xavier Standaert, Olivier Pereira, Yu Yu: *Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions.* CRYPTO (1) 2013: 335-352. Jake Longo, Daniel P. Martin, Elisabeth Oswald, Daniel Page, Martijn Stam, Michael Tunstall: *Simulatable Leakage: Analysis, Pitfalls, and New Constructions*. ASIACRYPT (1) 2014: 223-242

  - Yet, the pragmatic model seems sound

- In practice, how to design F* is open too

Additional remarks (I)

- In theory, the proof challenge remains open

François-Xavier Standaert, Olivier Pereira, Yu Yu: *Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions.* CRYPTO (1) 2013: 335-352. Jake Longo, Daniel P. Martin, Elisabeth Oswald, Daniel Page, Martijn Stam, Michael Tunstall: *Simulatable Leakage: Analysis, Pitfalls, and New Constructions*. ASIACRYPT (1) 2014: 223-242

  - Yet, the pragmatic model seems sound

- In practice, how to design F* is open too, e.g.,
  - Masking (⇒ bitslice ciphers)

Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici: *LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations*. FSE 2014: 18-37

Additional remarks (I)

- In theory, the proof challenge remains open

François-Xavier Standaert, Olivier Pereira, Yu Yu: *Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions.* CRYPTO (1) 2013: 335-352. Jake Longo, Daniel P. Martin, Elisabeth Oswald, Daniel Page, Martijn Stam, Michael Tunstall: *Simulatable Leakage: Analysis, Pitfalls, and New Constructions*. ASIACRYPT (1) 2014: 223-242

  - Yet, the pragmatic model seems sound

- In practice, how to design F* is open too, e.g.,
  - Masking (⇒ bitslice ciphers)

    Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici: *LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations*. FSE 2014: 18-37

  - PRFs with non-standard assumptions

    Marcel Medwed, François-Xavier Standaert, Antoine Joux: *Towards Super-Exponential Side-Channel Security with Efficient Leakage-Resilient PRFs*. CHES 2012: 193-212. Marcel Medwed, François-Xavier Standaert, Ventzi Nikov, Martin Feldhofer, *Unknown-Input Attacks in the Parallel Setting: Improving the Security and Performances of the CHES 2012 Leakage-Resilient PRF*, ASIACRYPT 2016 (to appear)

Additional remarks (I)

- In theory, the proof challenge remains open

François-Xavier Standaert, Olivier Pereira, Yu Yu: *Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions.* CRYPTO (1) 2013: 335-352. Jake Longo, Daniel P. Martin, Elisabeth Oswald, Daniel Page, Martijn Stam, Michael Tunstall: *Simulatable Leakage: Analysis, Pitfalls, and New Constructions*. ASIACRYPT (1) 2014: 223-242

  - Yet, the pragmatic model seems sound

- In practice, how to design F* is open too, e.g.,
  - Masking (⇒ bitslice ciphers)

Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, Kerem Varici: *LS-Designs: Bitslice Encryption for Efficient Masked Software Implementations*. FSE 2014: 18-37

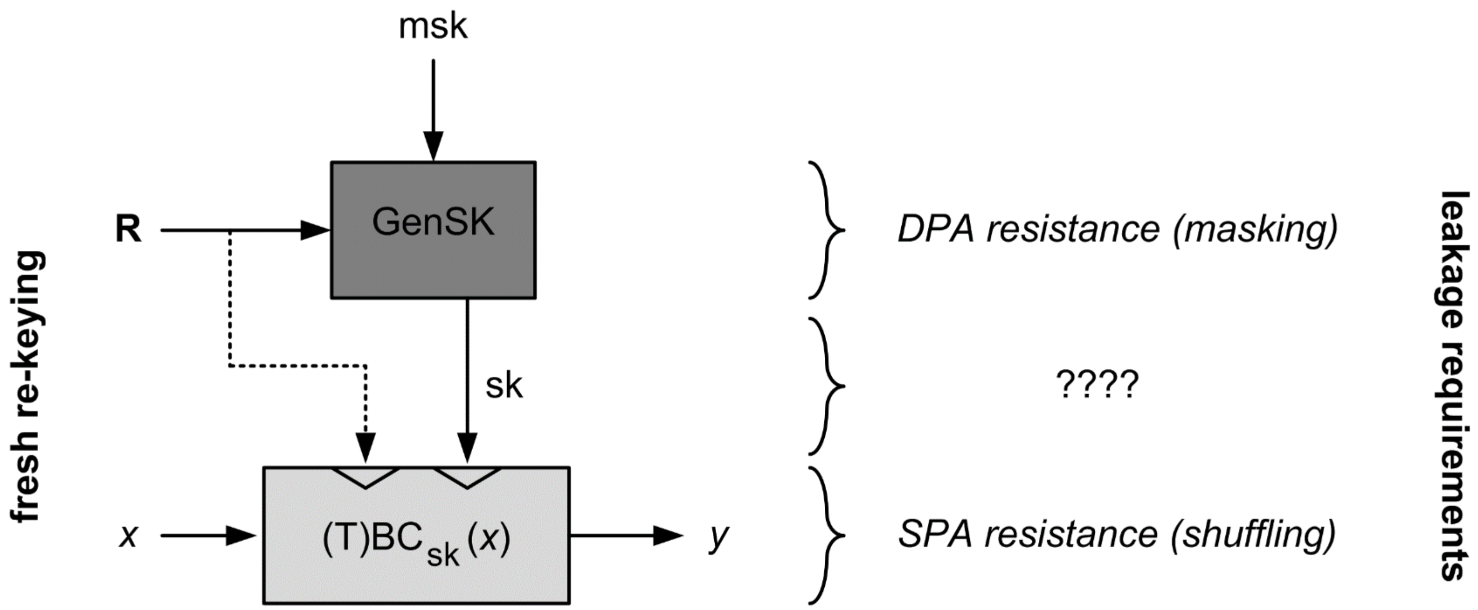
  - PRFs with non-standard assumptions

Marcel Medwed, François-Xavier Standaert, Antoine Joux: *Towards Super-Exponential Side-Channel Security with Efficient Leakage-Resilient PRFs*. CHES 2012: 193-212. Marcel Medwed, François-Xavier Standaert, Ventzi Nikov, Martin Feldhofer, *Unknown-Input Attacks in the Parallel Setting: Improving the Security and Performances of the CHES 2012 Leakage-Resilient PRF*, ASIACRYPT 2016 (to appear)

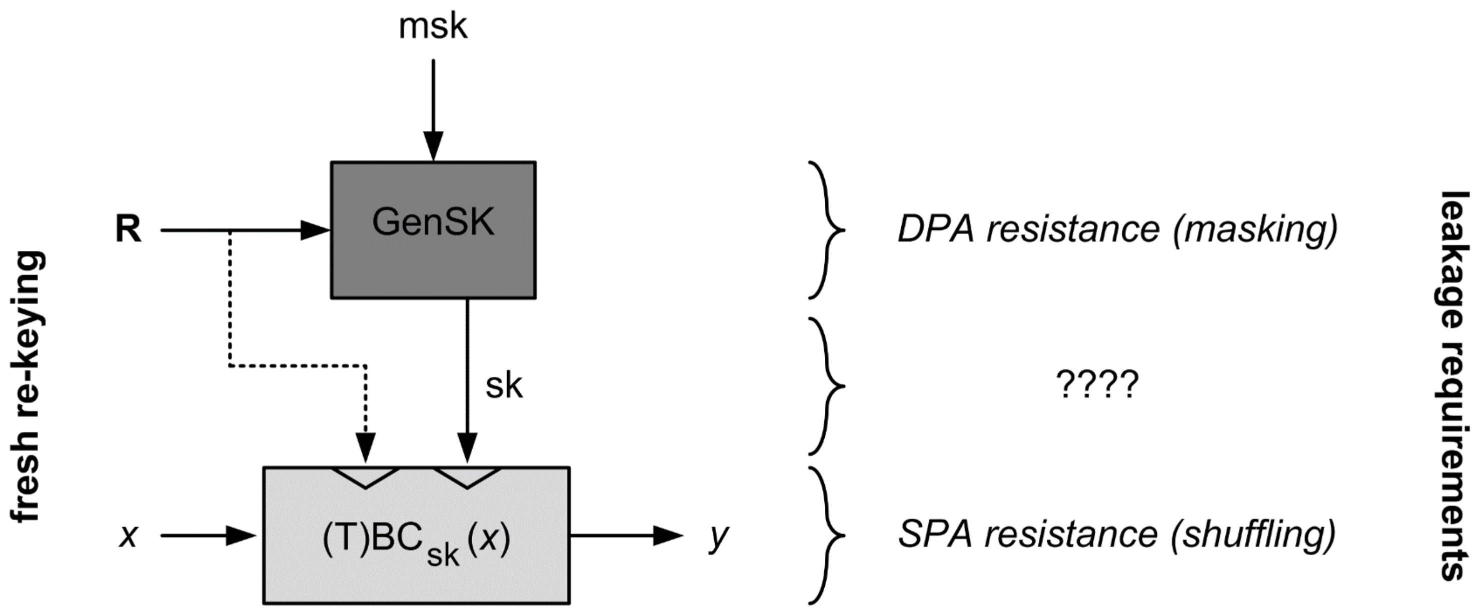
  - Key homomorphism & fresh re-keying

Christoph Dobraunig, François Koeune, Stefan Mangard, Florian Mendel, François-Xavier Standaert: *Towards Fresh and Hybrid Re-Keying Schemes with Beyond Birthday Security*. CARDIS 2015: 225-241

A recent proposal (Crypto 2016)



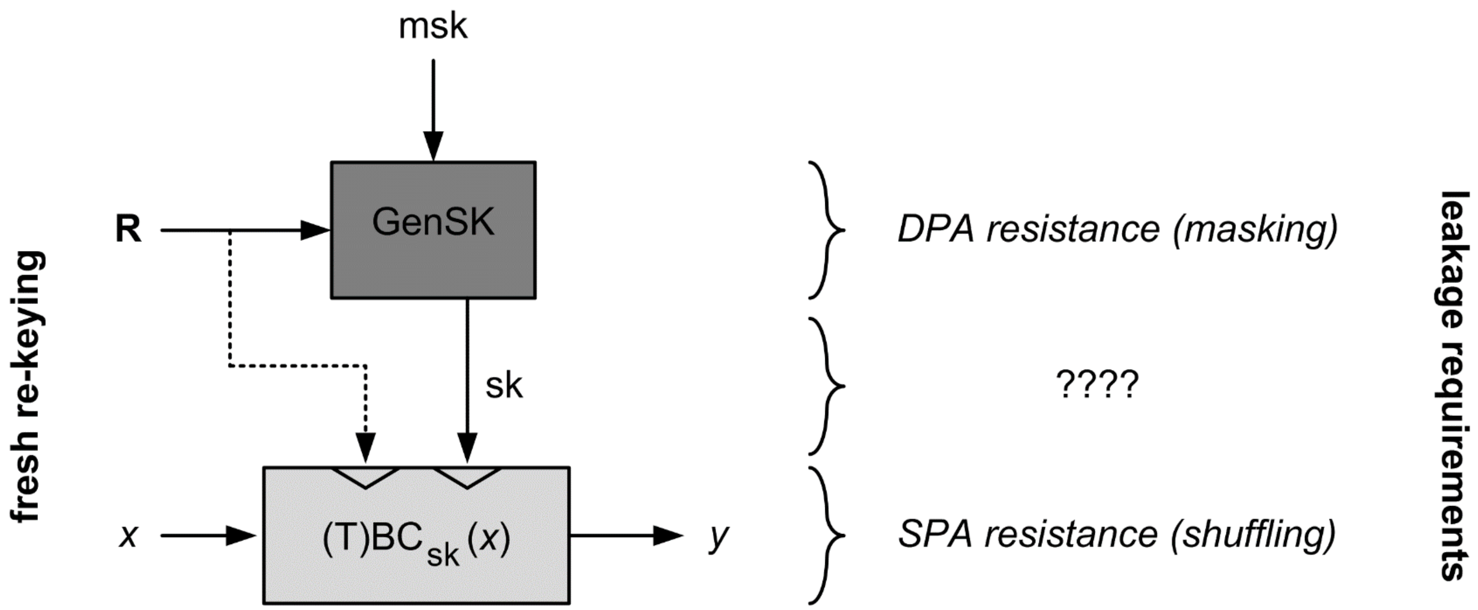
A recent proposal (Crypto 2016)



- Cryptographically strong re-keying function
  - $\mathrm{sk} = <\mathbf{R}, \mathrm{msk}> = \sum(<\mathbf{R}, \mathrm{msk}_i>)$

Stefan Dziembowski, Sebastian Faust, Gottfried Herold, Anthony Journault, Daniel Masny, François-Xavier Standaert: *Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems*. CRYPTO (2) 2016: 272-301

A recent proposal (Crypto 2016)



- Cryptographically strong re-keying function
  - $\text{sk} = <\mathbf{R}, \text{msk}> = \sum(<\mathbf{R}, \text{msk}_i>)$
- Security based on hard lattice problems
- Simple & efficient: all computations in Z_{2^m}

Stefan Dziembowski, Sebastian Faust, Gottfried Herold, Anthony Journault, Daniel Masny, François-Xavier Standaert: *Towards Sound Fresh Re-keying with Hard (Physical) Learning Problems*. CRYPTO (2) 2016: 272-301

Additional remarks (II)

- Authenticated encryption is also possible
  - But combination with IV misuse is tricky
  - Because controlling the IV transforms ephemeral secrets into long-term ones
  - Same reason makes LR-decryption tricky

- Authenticated encryption is also possible
  - But combination with IV misuse is tricky
  - Because controlling the IV transforms ephemeral secrets into long-term ones
  - Same reason makes LR-decryption tricky

- Full misuse resistance does not seem possible
  - (In the symmetric crypto setting)

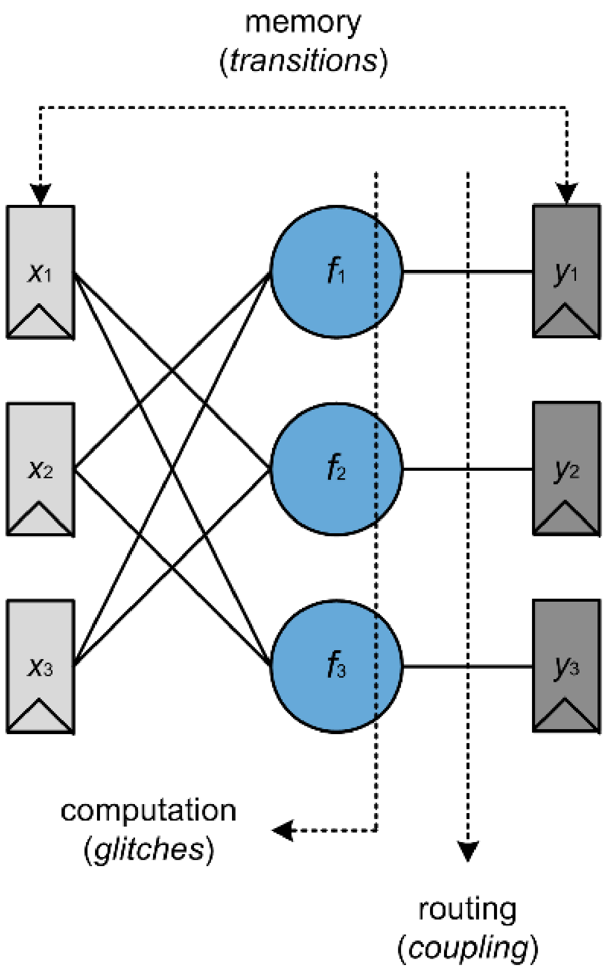
⇒ Current answer: ciphertext integrity with misuse (possible because unpredictability-based)

Francesco Berti and François Koeune and Olivier Pereira and Thomas Peters and François-Xavier Standaert: *Leakage-Resilient and Misuse-Resistant Authenticated Encryption*. IACR ePrint, 2016

Outline

- Preliminary questions / definitions
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- **Mitigating hardware defaults (is hard)**
- Transparency is needed (open source)
- Summary and conclusions

- Can break leakage independence requirements

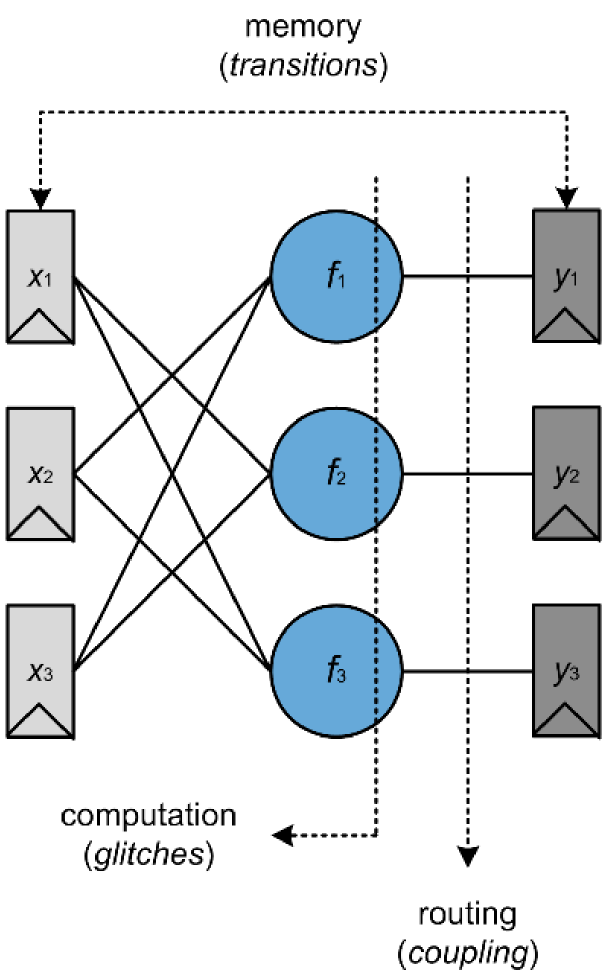


- e.g., recombine the shares of a masking scheme

⇒ Makes secure masked implementation hard to obtain

Stefan Mangard, Thomas Popp, Berndt M. Gammel: *Side-Channel Leakage of Masked CMOS Gates*. CT-RSA 2005: 351-365. Josep Balasch, Benedikt Gierlichs, Vincent Grosso, Oscar Reparaz, François-Xavier Standaert: *On the Cost of Lazy Engineering for Masked Software Implementations*. CARDIS 2014: 64-81. Svetla Nikova, Vincent Rijmen, Martin Schläffer: *Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches*. J. Cryptology 24(2): 292-321 (2011)

- Can break leakage independence requirements



- e.g., recombine the shares of a masking scheme

⇒ Makes secure masked implementation hard to obtain

- Default-tolerant protections would be (very) handy

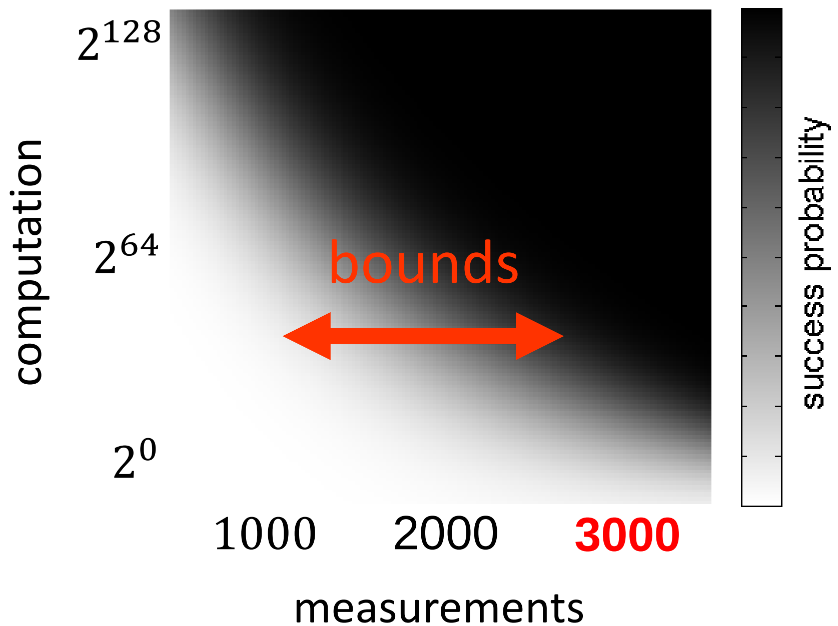
Stefan Mangard, Thomas Popp, Berndt M. Gammel: *Side-Channel Leakage of Masked CMOS Gates*. CT-RSA 2005: 351-365. Josep Balasch, Benedikt Gierlichs, Vincent Grosso, Oscar Reparaz, François-Xavier Standaert: *On the Cost of Lazy Engineering for Masked Software Implementations*. CARDIS 2014: 64-81. Svetla Nikova, Vincent Rijmen, Martin Schläffer: *Secure Hardware Implementation of Nonlinear Functions in the Presence of Glitches*. J. Cryptology 24(2): 292-321 (2011)

Outline

- Preliminary questions / definitions
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- Mitigating hardware defaults (is hard)
- **Transparency is needed (open source)**
- Summary and conclusions

standard practice

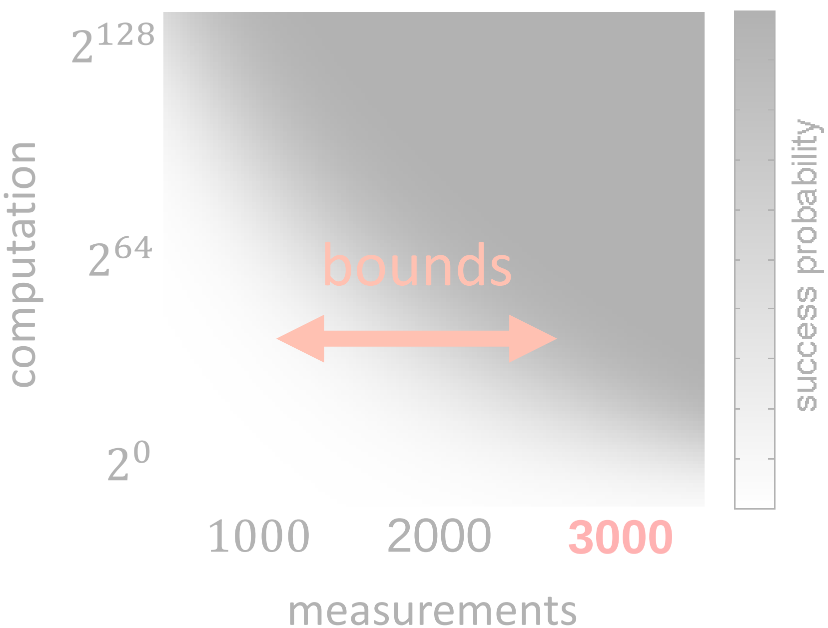
attack-based evaluations



Security evaluation tools

standard practice

attack-based evaluations



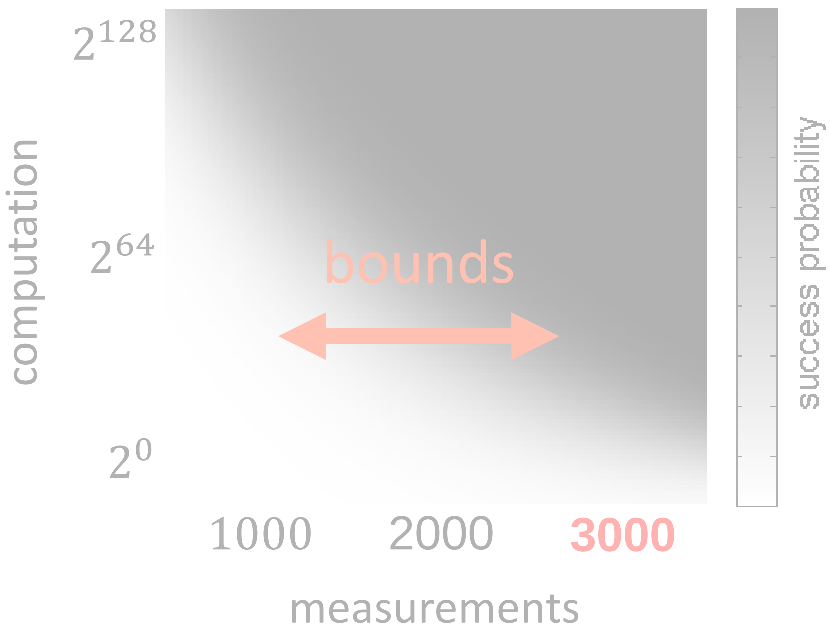
Security evaluation tools

standard practice

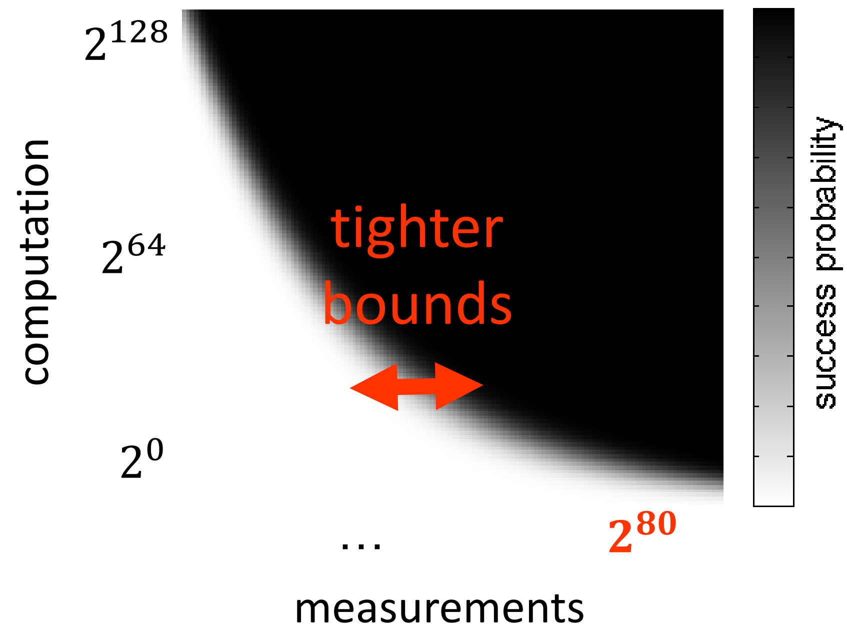
transparency

helps evaluations

attack-based evaluations



proof-based evaluations



Impact for design

- As masking order increases, the # of d-tuples of informative samples increases (say by d)

$\Rightarrow$ the gap between "simple" attacks targeting one d-tuple and d ones increase by a factor d

Impact for design

- As masking order increases, the # of d-tuples of informative samples increases (say by d)

⇒ the gap between "simple" attacks targeting one d-tuple and d ones increase by a factor d

- If shares are re-used (allowing averaging before combination) this factor becomes d^d

Impact for design

- As masking order increases, the # of d-tuples of informative samples increases (say by d)

⇒ the gap between "simple" attacks targeting one d-tuple and d ones increase by a factor d

- If shares are re-used (allowing averaging before combination) this factor becomes d^d

⇒ It means security depends on efficiency (in cycles), e.g., parallelism reduces # of leaking tuples

Outline

- Preliminary questions / definitions
- Side-channel basics (attack steps)
- Noise (aka hardware) is not enough
- Noise amplification (aka masking)
- Reductions help (aka leakage resilience)
- Transparency is needed (open source)
- Mitigating hardware defaults (is hard)
- **Summary and conclusions**

Conclusions (I)

- Effective countermeasures against side-channel attacks always combine sound hardware assumptions & mathematical amplification

Conclusions (I)

- Effective countermeasures against side-channel attacks always combine sound hardware assumptions & mathematical amplification

- High physical security is not mission impossible but has a cost! (e.g., time $\times$>10, area $\times$>2)
  - Yet, good designs can mitigate this cost

Conclusions (I)

- Effective countermeasures against side-channel attacks always combine sound hardware assumptions & mathematical amplification
- High physical security is not mission impossible but has a cost! (e.g., time $\times$>10, area $\times$>2)
  - Yet, good designs can mitigate this cost
- Metric I: # of operations per sensitive variable
  - Physical security $\propto$ efficiency
- Metric II: non-linearity (because hard to mask)

Conclusions (II)

- Systematic ways to deal with hardware defaults also has a price (e.g., doubling the # of shares)
  - But is probably worth it (to reduce risk)

Conclusions (II)

- Systematic ways to deal with hardware defaults also has a price (e.g., doubling the # of shares)
  - But is probably worth it (to reduce risk)

- Security should not depend on adversaries
  - Beware of too specific evaluations (T-tests)
  - Especially for protected implementations

Conclusions (II)

- Systematic ways to deal with hardware defaults also has a price (e.g., doubling the # of shares)
  - But is probably worth it (to reduce risk)
- Security should not depend on adversaries
  - Beware of too specific evaluations (T-tests)
  - Especially for protected implementations
- Long-term: open source codes/chips that can be used by any (non SCA expert) engineer

THANKS

http://perso.uclouvain.be/fstandae/