TU Graz

Leakage Bounds for Gaussian Side Channels

Thomas Unterluggauer[1], Thomas Korak[1], Stefan Mangard[1], Robert Schilling[1], Luca Benini[2], Frank K. Gürkaynak[2], and Michael Muehlberghuber[2],

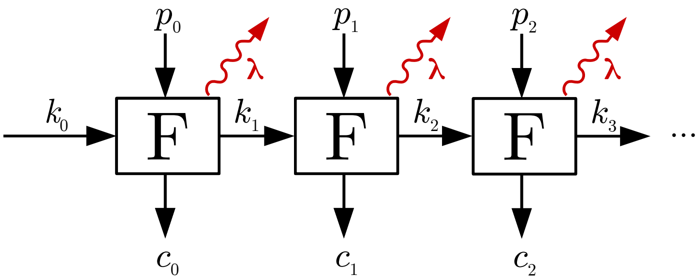
[1] IAIK, Graz University of Technology
[2] Integrated Systems Laboratory, ETH Zürich

14. November 2017

Content

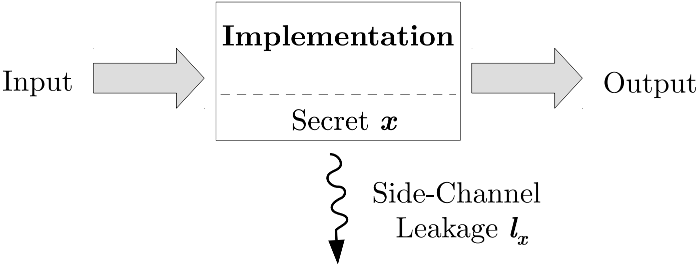
- Side-channel attacks threaten embedded devices
- Leakage-resilient schemes offer bounded leakage
- Challenge: specify leakage of underlying primitive
- This work: new approach to quantify leakage under a single data input
  - Mutual information in multivariate leakages: capacity of n-to-m communication channels
  - Channel capacity: (multivariate) SNR in m POIs
  - Averaging N traces: SNR increases $\sim N^m$
  - Practical verification: KECCAK-f[400] on ASIC

Motivation



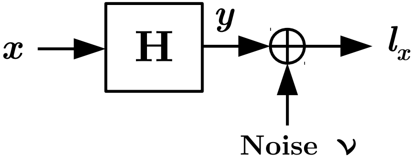
- Key update inherently prevents DPA
- Total leakage is bounded given λ-bit leakage of F
- Practical question: what is the value of λ?

Leakage Quantification



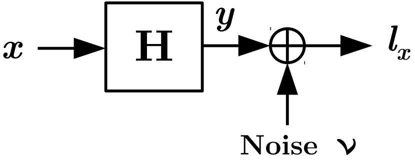
- Attacker tries to learn x from l_x
- Quantify information about x in l_x
  - Mutual information
  - $MI(X, L_x) = H[X] - H[X|L_x]$

Channel Model



- Channel $\mathbf{H}$: leakage behavior of implementation
- Linear $m \times n$ channel matrix $\mathbf{H}$:
  - $\mathbf{l}_x = \mathbf{Hx} + \nu$
- Secret state $\mathbf{x}$: $n \times 1$ vector (for n-bit state)
- Leakage trace $\mathbf{l}_x$: $m \times 1$ vector (for m POIs)
- Noise ν: $m \times 1$ vector

Channel Capacity



- Maximize mutual information between $\mathbf{x}$ and $\mathbf{l}_x$
  - Channel capacity $C = \max_{p(X)} \; MI(X, L_x)$
- Similar to Multi-Input Multi-Output (MIMO) channels
  - Wireless communication: n senders, m receivers

Capacity of MIMO Channels

- Capacity of MIMO channel (fixed $\mathbf{H}$):

$$C = \max_{\Sigma_{\mathbf{x}}:tr(\Sigma_{\mathbf{x}})=P} \log_2 \left|\mathbf{I}_m + \mathbf{H}\Sigma_{\mathbf{x}}\mathbf{H}^H\right|$$

- $n \times n$ signal covariance matrix $\Sigma_{\mathbf{x}}$
- Gaussian white noise with $\sigma_\nu^2 = 1$
- Side channels:
  - No power constraint P
  - Real values, e.g., power, no complex numbers
  - Noise correlations and different variances

Capacity of Gaussian Side Channels (1)

- Capacity of Gaussian Side Channels

$$C = \max_{p(X)} MI(X, L_x) = \frac{1}{2} \log_2 |\mathbf{I}_m + \Sigma_\nu^{-1} \mathbf{H} \Sigma_{\mathbf{x}} \mathbf{H}^H|.$$

- $m \times m$ noise covariance matrix Σ_ν

Capacity of Gaussian Side Channels (2)

$$C = \frac{1}{2} \log_2 |\mathbf{I}_m + \Sigma_\nu^{-1} \mathbf{H} \Sigma_\mathbf{x} \mathbf{H}^H|$$

- Channel matrix $\mathbf{H}$ is typically unknown...
- Profile side channel: multivar. Gaussian distribution
  - Templates: $(\mu_i, \Sigma_{\nu,i})$ for all possible states $\mathbf{x}_i$
- Independent noise: estimate Σ_ν from $\Sigma_{\nu,i}$
- Means μ_i give $\Sigma_\mathbf{y}$ (corresponding to $\mathbf{y} = \mathbf{H}\mathbf{x}$)
  - $\Sigma_\mathbf{y} = \mathbf{H} \Sigma_\mathbf{x} \mathbf{H}^H$

Leakage from Gaussian Side Channels

- Channel capacity: $C = \frac{1}{2}\log_2 \left|\mathbf{I}_m + \Sigma_\nu^{-1}\Sigma_\mathbf{y}\right|$
- Multivariate SNR: $\Sigma_\nu^{-1}\Sigma_\mathbf{y}$
  - Reflects correlations in signal and noise
  - Device- and measurement-specific
- Univariate leakage:
  - $C = \frac{1}{2}\log_2\left(1 + \frac{\sigma_y^2}{\sigma_\nu^2}\right) = \frac{1}{2}\log_2\left(1 + SNR\right)$

Averaging Attacker

Averaging Attacker

- Attackers observe the same operation multiple times
  - E.g., decryption of an FPGA bitfile
- Average N leakage traces $\mathbf{l_x}$ to remove noise
  - Noise covariance changes: $\overline{\Sigma}_\nu = \frac{1}{N}\Sigma_\nu$
  - Channel capacity increases:

$$C = \frac{1}{2}\log_2\left|\mathbf{I}_m + N \cdot \Sigma_\nu^{-1}\Sigma_\mathbf{y}\right|$$

Estimated Attack Complexity

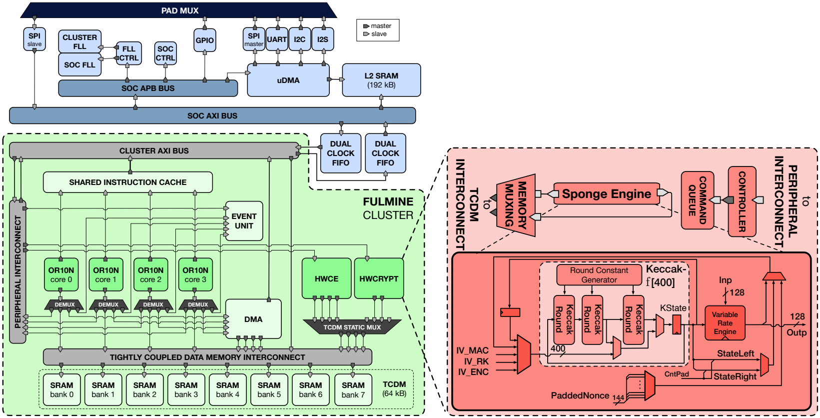
- Averaging a large number of traces
  - $C \approx \frac{1}{2} \log_2 \left(1 + N^m \left|\Sigma_\nu^{-1}\Sigma_{\mathbf{y}}\right|\right)$
- Scalar, single-trace $SNR_m = \left|\Sigma_\nu^{-1}\Sigma_{\mathbf{y}}\right|$
- Leakage proportional to N^m
- Number of averaged traces N reflects attack complexity
  - Tool for both attackers and designers

Experimental Evaluations

Experimental Evaluations

- Implementation of KECCAK-f[400]-based ISAP
  - Leakage-resilient authenticated encryption
  - Specifies leakage bounds for 128-bit security
- Two kind of evaluations:
  - Verify soundness of leakage bounds
    - Evaluate MI and channel capacity on hardware
  - Estimate security of ISAP implementation

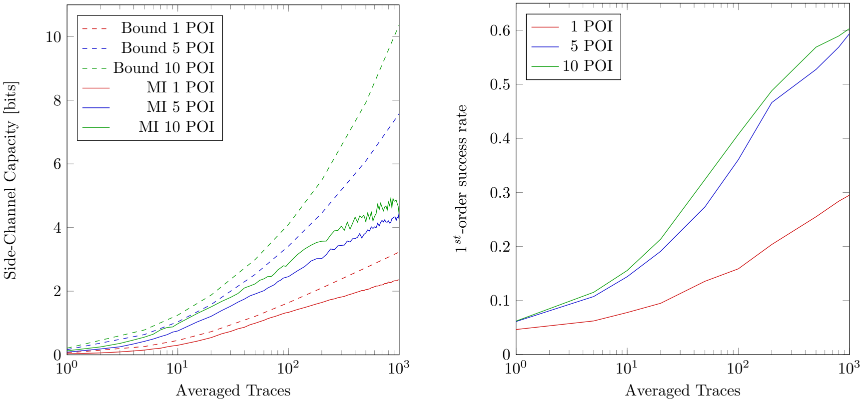
Evaluation Hardware: FULMINE



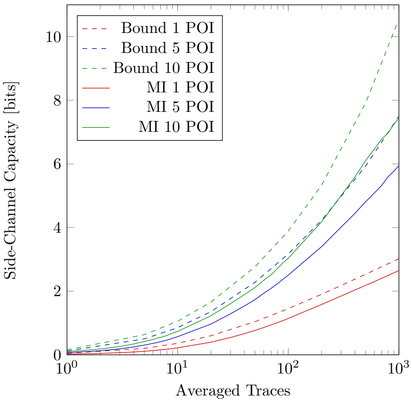
Methodology

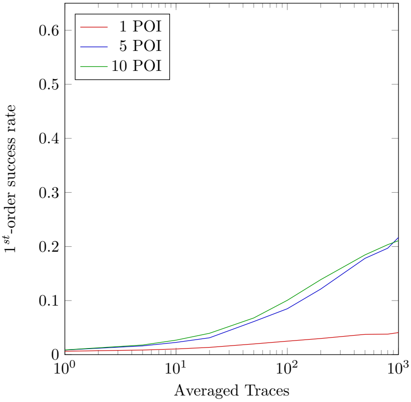
- Creation of multivariate Gaussian power templates
  - 5- and 8-bit parts of 400-bit KECCAK-f[400] state
  - Remaining state held constant
- Training phase: 1400 measurements per class
- Choice of POIs:
  - Points of highest variance
  - Maintain a certain minimum distance
  - Register and combinatorial activity

Capacity and Mutual Information (32 classes)



Capacity and Mutual Information (256 classes)



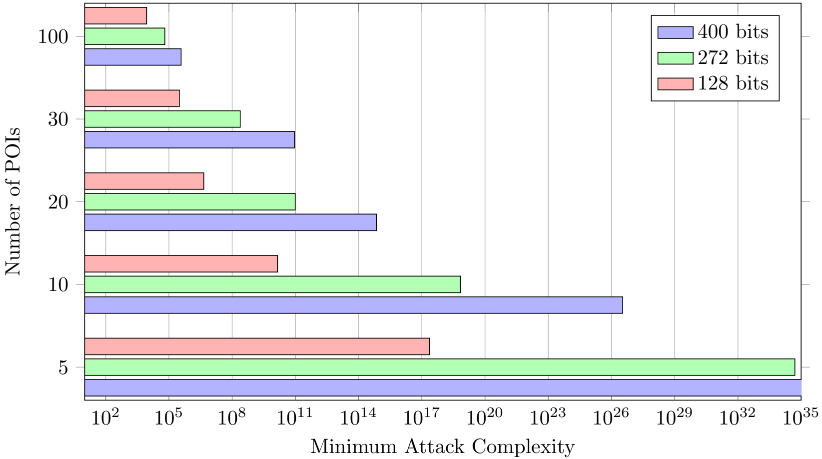


Security Estimation of ISAP

- Large state size
  - 400-bit KECCAK-f[400] state
  - Template building infeasible
- $SNR_m = |\Sigma_\nu^{-1}\Sigma_\mathbf{y}|$ is relevant for leakage quantification
  - SNR_m determined for 5- and 8-bit templates
  - Estimation for larger state: security margin γ

$$N = \left(\frac{2^{2S} - 1}{\gamma \cdot SNR_m}\right)^{1/m}$$

Security of ISAP on FULMINE ($\gamma = 100$)



Conclusion

- Leakage quantification is of ongoing interest
- Method to quantify the leakage from Gaussian side channels
  - Capacity of n-to-m communication channels
- Leakage bounded by physical property: SNR
- Averaging N traces: SNR increases $\sim N^m$
  - Tool to estimate the attack complexity
- Practical verification on ASIC: KECCAK-f[400]

Leakage Bounds for Gaussian Side Channels

Thomas Unterluggauer[1], Thomas Korak[1], Stefan Mangard[1], Robert Schilling[1], Luca Benini[2], Frank K. Gürkaynak[2], and Michael Muehlberghuber[2],

[1] IAIK, Graz University of Technology
[2] Integrated Systems Laboratory, ETH Zürich

14. November 2017