A MEMORY HIERARCHY PROTECTED AGAINST SIDE-CHANNEL ATTACKS

CONTACT

E. Bertrand Talaki ; Olivier Savry ; David Hely ; Mathieu Bouvier Des Noes
Univ. Grenoble Alpes, CEA, Leti, F-38000 Grenoble
Firstname.lastname@cea.fr

Introduction

Many first order power side-channel attacks have been reported on all the components of the memory hierarchy of System on Chips from the main memory to the CPU registers. In this context, memory hierarchy encryption is widely used to ensure confidentiality of data. However, this solution suffers from memory and area overhead especially for cache memories that already occupy a large part of the spatial footprint of a processor. Lightening the encryption with a Boolean masking approach in cache memories is a promising solution in order to cope with security and architectural constraints.

Objectives

1) Investigate and assess conditions on mask values for an optimal security
2) Define and implement a lightweight mask generator (LightMaG) to comply with security and architectural constraints

Materials & Methods

Simulated traces

$$L(v) = \varphi(v) + Noise$$

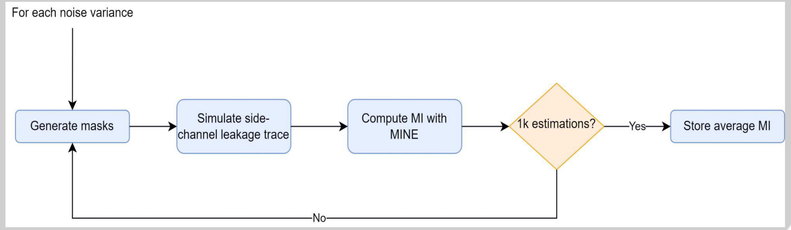
v: 8-bit variable
φ = HW (Hamming weight)
Noise: Gaussian noise of mean 0 and variance σ^2

- Generate random data *d*, random masks *m* and compute $d_m = d \oplus m$
- The final leakage trace is the tuple $(\boldsymbol{L(d_m)}, \boldsymbol{L(m)})$

MI estimation with MINE [1]

Estimate Mutual Information:

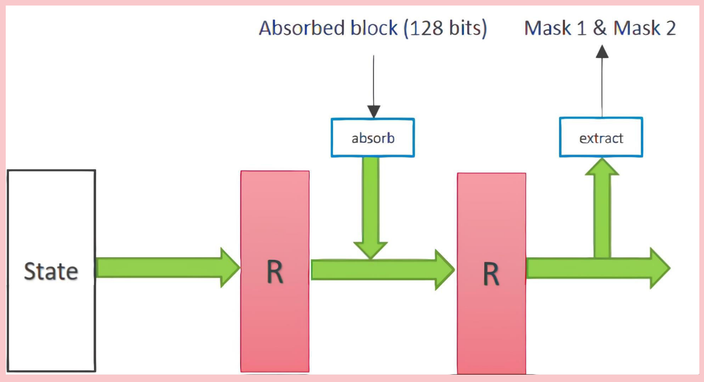
$$MI(HW(d), (L(d_m), L(m)))$$



Characterization of masks distributions

Security requirement: generated masks must enable the protection of the masking scheme against an attacker with up to 10,000 attack traces

Mask generation (LightMaG)



R: Subterranean 2.0 round function [2]

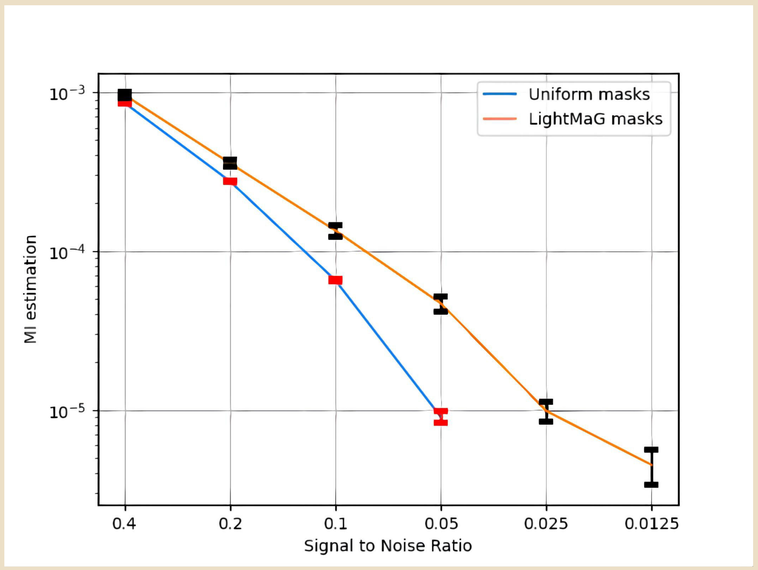
Resource utilization on Digilent Genesys 2 FPGA: 400 LUTs ➔ 0.6% overhead on CVA6 SoC
Max frequency: 150 MHz

$$State \leftarrow \mathrm{K}||\mathrm{ASID}||\mathrm{IV}||\mathrm{Ptr\_id}||@||0^{16}||1^{16}$$

$$Masked\_data||Masked\_tag \leftarrow data \oplus Mask_1||Integrity\_tag(data) \oplus Mask_2$$

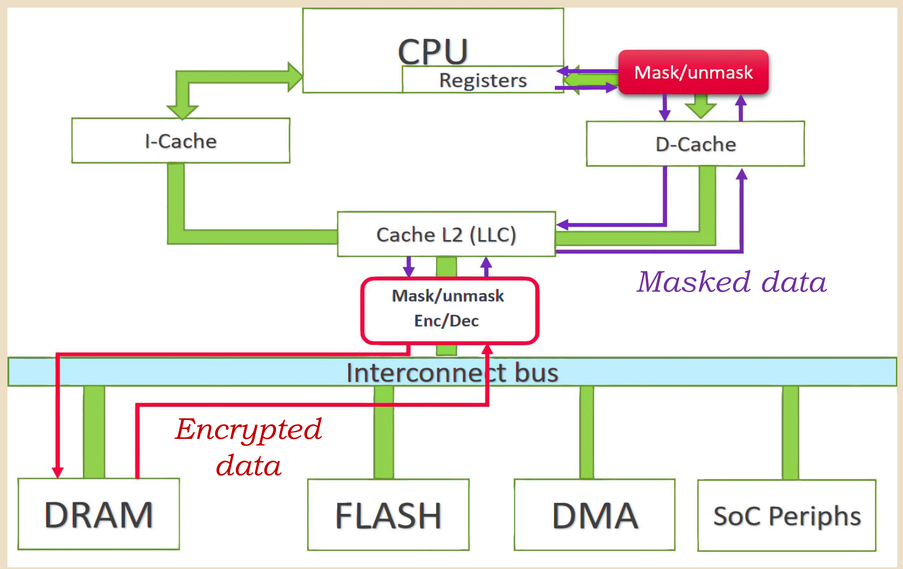
Results

Security evaluation of LightMaG masks



MI of 10^{-5} for SNR=0.02 ➔ *~500k attack traces for success rate of 99%*

Protected memory hierarchy



Conclusion

- Security of the masks: MI of 10^{-5} for SNR of 0.02
- Mask generation done in one clock cycle
- Spatial footprint of 400 LUTs; only 0.6% overhead & max freq of 150 MHz
- Only an 8-bit IV is stored instead of the whole mask
- Lightening of the memory hierarchy encryption
- Enabling masked computation in execute stage in pipeline

References

[1] V. Cristiani et al. , « Leakage assessment through neural estimation of the mutual information », in *International Conference on Applied Cryptography and Network Security*, 2020, p. 144–162.
[2] J. Daemen et al. , « The Subterranean 2.0 cipher suite », *IACR Transactions on Symmetric Cryptology*, p. 262–294, 2020.