Secure and Efficient Masking of Lightweight Ciphers in Software and Hardware
(with Application to the Spook AEAD)
—Lightweight Cryptography Workshop 2020—

Olivier Brochain, Gaëtan Cassiers, François-Xavier Standaert
ICTEAM/ELEN/Crypto Group, UCL, Louvain-la-Neuve, Belgium

Security against side-channel attacks has been explicitly mentioned by the NIST as a target in the ongoing standardization process for lightweight cryptography. Many candidates to the competition took this criteria into account by minimizing the number of non-linear operations (e.g., AND gates) in their algorithms, which is in general beneficial to the masking countermeasure.

In this talk, we will discuss:

– The gains that lightweight ciphers can offer over the AES for masking,
– The various challenges that the secure implementation of masking raises in software and in hardware, and tracks to solve them efficiently.

For this purpose, we will leverage state-of-the-art results from the masking literature [1, 2] and illustrate them thanks to the side-channel cryptanalysis challenge against masked Spook implementations that is (resp., was) running for CHES 2021 (resp., 2020). See https://ctf.spook.dev/ for the details.

We will conclude by discussing the extent to which similar conclusions hold for other lightweight ciphers with similar non-linear complexity, and suggesting directions for a fair evaluation and comparison of masked implementations.

References