Analyzing the Leakage-Resistance of some Round-2 Candidates of the NIST's Lightweight Crypto Standardization Process

—Lightweight Cryptography Workshop 2019—

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. In this talk, we will analyze the leakage-resistance of some of the candidates selected for the second round of the competition, including Ascon, ISAP, PHOTON-Beetle, Pyjamask and Spook (by elaborating on the results in [3]).

Our starting point for this purpose is the definitional framework introduced in [2] and discussed in [5]. Based on it, we observe that the aforelisted submissions to the NIST competition follow quite different approaches to prevent side-channel attacks. Some use "mode-level" mechanisms to mitigate the leakage (with more or less formal guarantees), others opt for algorithmic optimizations that enable efficient "implementation-level" countermeasures such as masking [1, 4] – a few submissions mix both.

Concretely, we will start by simplifying the types of mode-level leakage-resistant guarantees in four categories (typically reflected by the selected ciphers), and describing the design tweaks that are instrumental in proving integrity and confidentiality guarantees with leakage in these four cases.

Next, we will discuss the interaction between these formal guarantees of leakage-resistance and concrete side-channel security. This discussion allows us to cast the different authenticated encryption schemes under investigation as a tradeoff between the constraints on the modes in order to deal with certain types of (sometimes liberal) leakages and the pressure on implementers to limit the leakage.

Since more mode-level leakage-resistance usually implies some overheads in the unprotected setting, there is no generally better authenticated encryption scheme and the selection of an algorithm with the required implementation-level countermeasures creates a wide design space that is quite dependent on application constraints. In general, we conclude that as the required security against side-channel attacks increases, more mode-level leakage-resistance helps to limit the performance overheads.

References

1. Suresh Chari, Charanjit S. Jutla, Josyula R. Rao, and Pankaj Rohatgi. Towards Sound Approaches to Counteract Power-Analysis Attacks. In *CRYPTO*, volume 1666 of *Lecture Notes in Computer Science*, pages 398–412. Springer, 1999.
2. Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Authenticated encryption with nonce misuse and physical leakage: Definitions, separation results and first construction - (extended abstract). In *LATINCRYPT*, volume 11774 of *Lecture Notes in Computer Science*, pages 150–172. Springer, 2019.
3. Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Towards Low-Energy Leakage-Resistant Authenticated Encryption from the Duplex Sponge Construction. *IACR Cryptology ePrint Archive*, 2019:193, 2019.
4. Yuval Ishai, Amit Sahai, and David A. Wagner. Private circuits: Securing hardware against probing attacks. In *CRYPTO*, volume 2729 of *Lecture Notes in Computer Science*, pages 463–481. Springer, 2003.
5. François-Xavier Standaert. Towards and Open Approach to Secure Cryptographic Implementations (Invited Talk). In *EUROCRYPT (1)*, volume 11476 of *Lecture Notes in Computer Science*, page xv. Springer, 2019, https://www.youtube.com/watch?v=KdhrsuJT1sE.