Analyzing the Leakage Resistance of the NIST's Lightweight Crypto Standardization Process Finalists

Corentin Verhamme* Gaëtan Cassiers* François-Xavier Standaert*

April 8, 2022

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 9 out of the 10 candidates selected as finalists of the competition.

Our analysis follows two main steps:

First, we use a framework introduced by Bellizia et al. in order to evaluate the high-level leakage properties of the candidates' modes of operations [BBC+20].[1] This high-level analysis allows us to observe that 6 candidates can only/mostly rely on (expensive) implementation-level countermeasures. By contrast, 3 candidates (namely Ascon, ISAP and Romulus-T) have leakage-resistant features enabling so-called leveled implementations, where different parts of the implementations require different (more or less expensive) implementation-level countermeasures.

Second, we investigate the hardware performances of these 3 leakage-resistant modes of operation and evaluate their leveled implementation. For Ascon and Romulus-T, we protect the Key Derivation Function (KDF) and Tag Generation Function (TGF) against Differential Power Analysis (DPA) with Hardware Private Circuits (HPC), a state-of-the-art masking scheme that jointly provides resistance against physical defaults and composability [CGLS21, CS21]. For ISAP, the KDF and KGF are based on a leakage-resilient PRF that embeds a fresh re-keying mechanism such that they only require security against Simple Power Analysis (SPA). The latter is natively (and efficiently) obtained thanks to parallelism in hardware. For all 3 candidates, the bulk of the computation contains and internal re-keying mechanism. Hence SPA security (again achieved with hardware parallelism) guarantees confidentiality with leakage. This part of the implementation can even leak in an unbounded manner if only integrity with leakage is required.

We conclude that more than the quantitative comparison of the finalists, the main criteria that should guide the NIST in selecting a lightweight cryptography standard (if leakage is deemed important) are qualitative. The limited relevance of quantitative comparisons at this stage of the competition follows from two facts. For ciphers that rely on comparable countermeasures (like Ascon and Romulus-T), the performance gap is limited and predictable from simple proxies (and both are easier to protect than the AES). For ciphers that rely on different countermeasures (like ISAP), we currently lack (both theoretical and practical) tools that would allow a definitive comparison (e.g., with masking). By contrast, these three ciphers have different quantitative features, leading to a at least two clear questions that could (and we think, should) guide the final selection:

- *Is confidentiality with decryption leakage wanted?* Ascon, ISAP and Romulus-T all reach the top of the hiercachy in [GPPS19] for integrity with leakage (coined CIML2). The leveled

* Crypto Group, ICTEAM Institute, UCLouvain, Belgium.

[1] Excluding Grain-128AEAD, which cannot be captured with such a mode vs. primitive granularity.

implementation of Ascon only provides confidentiality with encryption leakages and misuse-resilience (coined CCAmL1). The leveled implementations of ISAP and Romulus-T can additionally provide confidentiality with decryption leakages and misuse-resilience (coined CCAmL2) at the cost of being two-pass (and can reach CCAmL1 in a single pass).

- *Flexibility or simplicity for the KDF and KGF?* Ascon and Romulus-T require DPA countermeasures like masking to protect their KDF and TGF. Implementing masking securely is a sensitive process that requires expertise. But it comes with a lot of flexibility: countermeasures do not always have to be deployed, different security vs. performance tradeoffs can be considered and one can have different security levels in encryption and decryption. ISAP relies on a re-keying mechanism so that only SPA security is needed for the whole implementation, which is easy to obtain in hardware. But it has no flexibility (the overheads of the leakage-resilient PRF have to be paid even if side-channel security is not a concern).[2]

A slightly longer-term question relates to the choice between permutations and Tweakable Block Ciphers (TBCs). While the same leakage-resistant features can be obtained at somewhat similar costs from permutations and sponges, these two building blocks come with some differences. On the one hand, TBC-based designs seem more amenable to security analyzes in the standard model [BGP+20, BGPS21], while permutations currently require idealized assumptions [DM19, GPPS20]. On the other hand, TBC-based schemes enable performing an inverse-based tag verification that can leak in full [BPPS17] while permutation-based schemes require masking [BMPS21] or additional computations [DM21] for securing this part of their design against leakage.

Acknowledgments. Gaëtan Cassiers and François-Xavier Standaert are respectively research fellow and senior research associate of the Belgian fund for scientific research (FNRS-F.R.S.). This work has been funded in parts by European Union via the ERC project 724725 (acronym SWORD).

References

[BBC+20] Davide Bellizia, Olivier Bronchain, Gaëtan Cassiers, Vincent Grosso, Chun Guo, Charles Momin, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Mode-level vs. implementation-level physical security in symmetric cryptography - A practical guide through the leakage-resistance jungle. In *CRYPTO (1)*, volume 12170 of *Lecture Notes in Computer Science*, pages 369–400. Springer, 2020.

[BGP+20] Francesco Berti, Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Tedt, a leakage-resist AEAD mode for high physical security applications. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(1):256–320, 2020.

[BGPS21] Francesco Berti, Chun Guo, Thomas Peters, and François-Xavier Standaert. Efficient leakage-resilient macs without idealized assumptions. In *ASIACRYPT (2)*, volume 13091 of *Lecture Notes in Computer Science*, pages 95–123. Springer, 2021.

[BMPS21] Olivier Bronchain, Charles Momin, Thomas Peters, and François-Xavier Standaert. Improved leakage-resistant authenticated encryption based on hardware AES coprocessors. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(3):641–676, 2021.

[2] Security in low-end embedded software implementations is unclear both for masking and re-keying, which can both be the target of strong attacks in low-noise contexts: see [BS21] for masking and [KPP20, BBC+20] for re-keying. We believe the understanding of low-noise leakages is not stable enough for being used as a guiding criteria.

[BPPS17] Francesco Berti, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. On leakage-resilient authenticated encryption with decryption leakages. *IACR Trans. Symmetric Cryptol.*, 2017(3):271–293, 2017.

[BS21] Olivier Bronchain and François-Xavier Standaert. Breaking masked implementations with many shares on 32-bit software platforms or when the security order does not matter. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(3):202–234, 2021.

[CGLS21] Gaëtan Cassiers, Benjamin Grégoire, Itamar Levi, and François-Xavier Standaert. Hardware private circuits: From trivial composition to full verification. *IEEE Trans. Computers*, 70(10):1677–1690, 2021.

[CS21] Gaëtan Cassiers and François-Xavier Standaert. Provably secure hardware masking in the transition- and glitch-robust probing model: Better safe than sorry. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2021(2):136–158, 2021.

[DM19] Christoph Dobraunig and Bart Mennink. Leakage resilience of the duplex construction. In *ASIACRYPT (3)*, volume 11923 of *Lecture Notes in Computer Science*, pages 225–255. Springer, 2019.

[DM21] Christoph Dobraunig and Bart Mennink. Leakage resilient value comparison with application to message authentication. In *EUROCRYPT (2)*, volume 12697 of *Lecture Notes in Computer Science*, pages 377–407. Springer, 2021.

[GPPS19] 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.

[GPPS20] Chun Guo, Olivier Pereira, Thomas Peters, and François-Xavier Standaert. Towards low-energy leakage-resistant authenticated encryption from the duplex sponge construction. *IACR Trans. Symmetric Cryptol.*, 2020(1):6–42, 2020.

[KPP20] Matthias J. Kannwischer, Peter Pessl, and Robert Primas. Single-trace attacks on keccak. *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, 2020(3):243–268, 2020.