Update on the Performance and Mode-level Properties of ISAP

Proposal for Presentation

Christoph Dobraunig[1], Maria Eichlseder[1], Stefan Mangard[1], Florian Mendel[2], Bart Mennink[3], Robert Primas[1] and Thomas Unterluggauer[1]

[1] Graz University of Technology, Austria
[2] Infineon Technologies AG, Germany
[3] Radboud University, Netherlands

Isap v2.0 [Dob+20] is a family of lightweight authenticated encryption algorithms designed with a focus on robustness against implementation attacks. Isap v2.0 is of particular interest for applications like firmware updates where robustness against power analysis and fault attacks is crucial and code size and a small footprint in hardware matters. In this talk, we summarize the mode-level features of Isap v2.0, how they affect concrete implementation attacks, and what performance one can expect from Isap v2.0 in different use cases.

In the first part, we revisit the mode-level properties of Isap v2.0. We consider the conventional security guarantees achieved by Isap v2.0 mode, as well as its strength in the context of other settings, such as nonce-misuse, release of unverified plaintext, and others. We extend our observations towards the security of the Isap v2.0 mode in a leaky environment. In this context, we discuss two novel leakage resilience results and their relation to Isap v2.0: (i) leakage resilient value comparison, particularly the "PVP" function, and the combined SuKS-then-PVP (StP) construction as it would appear in Isap v2.0 [DM21], and (ii) a proposal for a more meaningful leakage resilience model, introduced alongside the "asakey" encryption mode that resembles the encryption mode of Isap v2.0 [DMP20].

In the second part, we give an overview of how the ISAP mode affects concrete power analysis and fault attacks, with a particular focus on critical scenarios like firmware updates. We comment amongst others on DPA-based key/plaintext/tag recovery attacks and discuss the concrete instantiation of the StP construction in current hardware/software implementations of Isap v2.0. Finally, we present general performance metrics of Isap v2.0 in different use cases, including use cases that are not within the primary scope of the NIST LWC standardization project.

References

[Dob+20] Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, Florian Mendel, Bart Mennink, Robert Primas, and Thomas Unterluggauer. "Isap v2.0". In: *IACR Transactions on Symmetric Cryptology* 2020.S1 (2020), pp. 390–416. URL: https://doi.org/10.13154/tosc.v2020.iS1.390-416.

[DM21] Christoph Dobraunig and Bart Mennink. "Leakage Resilient Value Comparison with Application to Message Authentication". In: *EUROCRYPT (2)*. Vol. 12697. Lecture Notes in Computer Science. Springer, 2021, pp. 377–407.

[DMP20] Christoph Dobraunig, Bart Mennink, and Robert Primas. “Leakage and Tamper Resilient Permutation-Based Cryptography”. In: *IACR Cryptol. ePrint Arch.* (2020), p. 200. URL: https://eprint.iacr.org/2020/200.