Updates on the Implementation Security 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

https://isap.iaik.tugraz.at

Isap v2.0 [Dob+20] is a family of lightweight authenticated encryption algorithms designed with a focus on robustness against implementation attacks. Its instances are based either on Ascon's permutation [DEMS16] or Keccak-p[400] [BDPV11; Nat15]. Isap v2.0 is of particular interest for applications like firmware updates where robustness against power analysis and fault attacks is crucial and codesize and a small footprint in hardware matters.

In this talk, we focus on the implementation security aspects of Isap v2.0. First, we revisit Isap v2.0's mode-level features such as increased resistance against implementation attacks including DPA [KJJ99], DFA [BS97], SFA [FJLT13], and SIFA [Dob+18].

We then outline the results of the recent CHES paper "Single-Trace Attacks on Keccak", which is co-authored by one of Isap v2.0's designers, and studies the applicability of SPA/Template attacks on cryptographic constructions that are used within Isap v2.0 [KPP20].

Finally, we discuss a newly released compact co-processor implementing Ascon's permutation [SP20], which is to appear at CARDIS 2020. This co-processor can be used to significantly speed up Ascon/Isap v2.0 computations, while providing increased protection against SPA/Template attacks at the same time.

References

[BDPV11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. *The Keccak reference, Version 3.0.* 2011. URL: https://keccak.team/files/Keccak-reference-3.0.pdf.

[BS97] Eli Biham and Adi Shamir. "Differential Fault Analysis of Secret Key Cryptosystems". In: *Advances in Cryptology – CRYPTO '97.* Ed. by Burton S. Kaliski Jr. Vol. 1294. LNCS. Springer, 1997, pp. 513–525. URL: https://doi.org/10.1007/BFb0052259.

[Dob+18] Christoph Dobraunig, Maria Eichlseder, Thomas Korak, Stefan Mangard, Florian Mendel, and Robert Primas. "SIFA: Exploiting Ineffective Fault Inductions on Symmetric Cryptography". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2018.3 (2018), pp. 547–572. URL: https://doi.org/10.13154/tches.v2018.i3.547-572.

[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.

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. *Ascon v1.2 (Submission to the CAESAR Competition)*. Final Portfolio of CAESAR: http://competitions.cr.yp.to/caesar-submissions.html. 2016.

[FJLT13] Thomas Fuhr, Éliane Jaulmes, Victor Lomné, and Adrian Thillard. "Fault Attacks on AES with Faulty Ciphertexts Only". In: *Workshop on Fault Diagnosis and Tolerance in Cryptography – FDTC 2013*. Ed. by Wieland Fischer and Jörn-Marc Schmidt. IEEE Computer Society, 2013, pp. 108–118. URL: https://doi.org/10.1109/FDTC.2013.18.

[KPP20] Matthias J. Kannwischer, Peter Pessl, and Robert Primas. "Single-Trace Attacks on Keccak". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020.3 (2020), pp. 243–268. URL: https://doi.org/10.13154/tches.v2020.i3.243-268.

[KJJ99] Paul C. Kocher, Joshua Jaffe, and Benjamin Jun. "Differential Power Analysis". In: *Advances in Cryptology – CRYPTO '99*. Ed. by Michael J. Wiener. Vol. 1666. LNCS. Springer, 1999, pp. 388–397. URL: https://doi.org/10.1007/3-540-48405-1_25.

[Nat15] National Institute of Standards and Technology. *FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions*. Federal Information Processing Standards Publication 202, U.S. Department of Commerce. Aug. 2015.

[SP20] Stefan Steinegger and Robert Primas. *A Fast and Compact Accelerator for Ascon and Friends*. Cryptology ePrint Archive, Report 2020/1083. https://eprint.iacr.org/2020/1083. To appear at CARDIS. 2020.