New Ascon Implementations

Proposal for Presentation at NIST LWC Workshop 2022

Christoph Dobraunig[1], Maria Eichlseder[1], Florian Mendel[2], Robert Primas[1] and Martin Schläffer[2]

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

https://ascon.iaik.tugraz.at

Ascon was published in 2014 and selected as the first choice for resource-constrained environments of the CAESAR portfolio in 2019 [DEMS16]. In the last 8 years, many results have been published that discuss and evaluate Ascon's security.

Ascon has been designed with side-channel resistance in mind. In this talk we present the latest results of protecting Ascon against side-channel attacks in software and hardware. We will focus on both, performance benchmarks and preliminary security evaluations. The S-box of Ascon can be efficiently masked with fewer instructions and no additional randomness using the Toffoli gate, as discussed in [Dae+20; SM21]. Additionally, shares can be stored and computed in a rotated form with limited performance impact on ARM platforms to reduce the side-channel leakage on real devices. Furthermore, Ascon allows for leveled implementations [AFM18; Bel+20] which allows to further improve the performance.

In addition, we present updated results on the performance and code size of Ascon AEAD, hashing and combined implementations. Finally, we conclude with new performance improvements for Ascon and the recently published Ascon PRF, MAC and (Short-Input) MAC [DEMS21]. All software implementations are published online[1] and evaluated in third-party benchmarking efforts.

Acknowledgments. Part of this work has been supported by the Austrian Science Fund (FWF): P26494-N15 and J 4277-N38.

References

[AFM18] Alexandre Adomnicai, Jacques J. A. Fournier, and Laurent Masson. "Masking the Lightweight Authenticated Ciphers ACORN and Ascon in Software". In: *IACR Cryptol. ePrint Arch.* (2018), p. 708. URL: https://eprint.iacr.org/2018/708.

[Bel+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: *Advances in Cryptology – CRYPTO 2020*. Ed. by Daniele Micciancio and Thomas Ristenpart. Vol. 12170. LNCS. Springer, 2020, pp. 369–400. URL: https://doi.org/10.1007/978-3-030-56784-2_13.

[1] https://github.com/ascon/ascon-c

[Dae+20] Joan Daemen, Christoph Dobraunig, Maria Eichlseder, Hannes Groß, Florian Mendel, and Robert Primas. "Protecting against Statistical Ineffective Fault Attacks". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* 2020.3 (2020), pp. 508–543. URL: https://doi.org/10.13154/tches.v2020.i3.508-543.

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. *Ascon v1.2*. CAESAR, first choice for lightweight applications (resource constrained environments), https://competitions.cr.yp.to/caesar-submissions.html. 2016.

[DEMS21] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. "Ascon PRF, MAC, and Short-Input MAC". In: *IACR Cryptol. ePrint Arch.* (2021), p. 1574. URL: https://eprint.iacr.org/2021/1574.

[SM21] Aein Rezaei Shahmirzadi and Amir Moradi. "Second-Order SCA Security with almost no Fresh Randomness". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.3 (2021), pp. 708–755. URL: https://doi.org/10.46586/tches.v2021.i3.708-755.