Update on Ascon Implementations

Proposal for Presentation

Christoph Dobraunig[1], Maria Eichlseder[1], Florian Mendel[2] 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 six years, many results have been published that discuss and evaluate Ascon's security.

In this talk, we focus on some lesser-known implementation characteristics of Ascon. While Ascon is designed primarily for high performance and efficiency on resource-constrained devices, it also performs very well on 64-bit machines. For 32-bit platforms, the primary implementation technique is bit interleaving [BDPVV12], which provides several benefits in implementing Ascon. Additionally, Ascon can be implemented at a very low code size with a minimum impact on performance. All software implementations are published online[1] and have been evaluated in third-party benchmarking efforts.

Finally, Ascon has been designed with side-channel resistance in mind. We discuss several software options to protect Ascon against side-channel attacks. This includes the ability to efficiently mask the S-box with fewer instructions and less randomness using the Toffoli gate, as discussed in [Dae+20]. Additionally, shares can be stored and computed in a rotated form with limited performance impact to reduce the side-channel leakage on real devices. Furthermore, Ascon allows for leveled implementations, as outlined by Bellizia et al. [Bel+20].

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

References

[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.

[BDPVV12] Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, and Ronny Van Keer. *Keccak implementation overview version 3.2*. 2012. URL: https://keccak.team.

[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.