Update on Ascon Implementations
Proposal for Presentation

Christoph Dobraniig\textsuperscript{1}, Maria Eichlseder\textsuperscript{1}, Florian Mendel\textsuperscript{2} and Martin Schläffer\textsuperscript{2}

\textsuperscript{1} Graz University of Technology, Austria
\textsuperscript{2} Infineon Technologies AG, Germany

https://ascon.iak.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\textsuperscript{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


\textsuperscript{1}https://github.com/ascon/ascon-c