Update on the Security Analysis of Ascon

Proposal for Presentation at NIST LWC Workshop 2022

Christoph Dobraunig[1], Maria Eichlseder[1], Johannes Erlacher[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 [DEMS21b] is one of the finalists in the NIST LWC project. Since it was published in 2014 and selected as the first choice for resource-constrained environments of the CAESAR portfolio in 2019 [DEMS16], there was already a substantial body of publications on Ascon's security before the beginning of the NIST LWC project.

In this talk, we provide an overview of recent third-party cryptanalysis results as well as our own work on new security bounds. We first focus on our efforts to improve the bounds for security against differential and linear cryptanalysis with new Boolean Satisfiability (SAT) models [EME22]. We find bounds for 4 and 6 rounds of the permutation which, while probably not tight, reinforce confidence in the security of Ascon, Ascon-Hash, and Ascon-Xof against differential and linear attacks with respect to the security claim. We also discuss the implications of these bounds for the recently proposed MAC variants based on the Ascon permutation [DEMS21a]. Additionally, we use a similar SAT model to provide differential bounds for the 1-round Ascon permutation with 1-bit rate as used in Isap, demonstrating the infeasibility of differentially-induced collisions in this construction.

We also provide a brief overview and discussion of recent third-party analysis results. Among others, Rohit et al. [RHSS21] slightly reduced the data complexity of previous 7-round attacks to stay below the limit of 2^{64} encrypted blocks. Rohit and Sarkar [RS21] investigated classes of "weak keys" which permit slightly better attacks for round-reduced Ascon. Gerault et al. [GPT21] investigated the applicability of differential distinguishers for forgeries on round-reduced Ascon. Civek and Tezcan [CT22] provided new experiments on differential-linear cryptanalysis. In summary, these results provide a more detailed understanding of Ascon's security margin, which essentially confirms and slightly refines the previously-known results on up to 7 out of 12 rounds of Ascon's permutation.

References

[CT22] Aslí Basak Civek and Cihangir Tezcan. "Differential-linear Attacks on Permutation Ciphers Revisited: Experiments on Ascon and DryGASCON". In: *Information Systems Security and Privacy – ICISSP 2022*. Ed. by Paolo Mori, Gabriele Lenzini, and Steven Furnell. SCITEPRESS, 2022, pp. 202–209. doi: 10.5220/0010982600003120.

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. *Ascon v1.2*. CAESAR Competition. 2016. url: https://competitions.cr.yp.to/caesar-submissions.html.

[DEMS21a] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. *Ascon PRF, MAC, and Short-Input MAC*. IACR Cryptology ePrint Archive, Report 2021/1574. 2021. URL: https://ia.cr/2021/1574.

[DEMS21b] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. "Ascon v1.2: Lightweight Authenticated Encryption and Hashing". In: *Journal of Cryptology* 34.3 (2021), p. 33. DOI: 10.1007/s00145-021-09398-9.

[EME22] Johannes Erlacher, Florian Mendel, and Maria Eichlseder. "Bounds for the Security of Ascon against Differential and Linear Cryptanalysis". In: *IACR Transactions on Symmetric Cryptology* 2022.1 (2022), pp. 64–87. DOI: 10.46586/tosc.v2022.i1.64-87.

[GPT21] David Gerault, Thomas Peyrin, and Quan Quan Tan. "Exploring Differential-Based Distinguishers and Forgeries for ASCON". In: *IACR Transactions on Symmetric Cryptology* 2021.3 (2021), pp. 102–136. DOI: 10.46586/tosc.v2021.i3.102-136.

[RHSS21] Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun. "Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon". In: *IACR Transactions on Symmetric Cryptology* 2021.1 (2021), pp. 130–155. DOI: 10.46586/tosc.v2021.i1.130-155.

[RS21] Raghvendra Rohit and Santanu Sarkar. "Diving Deep into the Weak Keys of Round Reduced Ascon". In: *IACR Transactions on Symmetric Cryptology* 2021.4 (2021), pp. 74–99. DOI: 10.46586/tosc.v2021.i4.74-99.