Cube-like attack against Ascon

Jules Baudrin, Anne Canteaut & Léo Perrin

Inria Paris

In April 2019, the American National Institute of Standards and Technology (NIST) started a standardization process in the field of lightweight symmetric cryptography [NIS17]. Their intention is to identify algorithms which can provide authenticity, integrity and/or confidentiality at "smaller costs" in order to be used on constrained devices. Many of these devices, especially in the context of the "Internet of Things", do not primarily aim at protecting data. There is thus an incontestable need to guide the usages and to identify algorithms which can provide security, at the cost of a size/speed/security trade-off.

Ascon [DEMS19] is a finalist of the NIST standardization process and was also part of the final "lightweight applications" portfolio of CAESAR (a previous standardization process, [CAE14]). In front of many different definitions of lightweightness [BP17], the authors of Ascon chose to provide a versatile algorithm and claim a "very low memory footprint in hardware and software, while still being fast, robust and secure".

To do so, they based their work on the already-analyzed Sponge Duplex mode of operation [BDPA11, BDPV12] and thus mainly focused on the design of their permutation. This permutation is based on successive alternations between linear and non-linear layers. The non-linear layer is of primary matter for security and relies on several parallel calls to a Substitution-box (S-box). In order to facilitate masking (in the context of easily-accessible devices) but also to minimize the costs, this S-box has a low algebraic degree: it is quadratic. This choice in the design is not without consequences and might lead to some attacks.

In this work, we analyze the reliability of Ascon against cube-attacks [DS09] taking an article of Rohit *et al.* [RHSS21] as starting point. In their original form, cube-attacks aimed at recovering information about secret data by first building a linear system (whose unknowns are secret-key bits), and then recovering the value of the linear combinations involved. Through a linear-system solving, an adversary can thus recover (some of) the secret-key bits. However, finding such linear combinations, *i.e.* whose values are accessible in the genuine conditions of use, is usually difficult.

Here, by a careful analysis of the Algebraic Normal Form (ANF) of the permutation, we define a new way to obtain such linear combinations. Our method leads to some attacks against round-reduced versions of Ascon, but it might be adaptable to other algorithms as it does not rely (much) on the specificities of Ascon. Rather, it is based on a lack of diffusion that we study with a new approach. Through the analysis of the polynomial representation of the permutation (the ANF), diffusion can be apprehended by looking at the "shuffling and mixing" of public and secret variables. In general, the situation is quite intricate after a few rounds, especially because the more the degree increases, the more combinatorial possibilities there are to obtain a chosen monomial by successive multiplications. However, due to internal properties of Ascon, it may happen that only a single combinatorial possibility leads to a chosen monomial. This property is a key point of our method.

[BDPA11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Cryptographic sponge functions, 2011. https://keccak.team/sponge_duplex.html.

[BDPV12] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Duplexing the sponge: Single-pass authenticated encryption and other applications. In Ali Miri and Serge Vaudenay, editors, SAC 2011, volume 7118 of LNCS, pages 320–337, Toronto, Ontario, Canada, August 11–12, 2012. Springer, Heidelberg, Germany.

[BP17] Alex Biryukov and Leo Perrin. State of the art in lightweight symmetric cryptography. Cryptology ePrint Archive, Report 2017/511, 2017. https://eprint.iacr.org/2017/511.

[CAE14] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, March 2014. https://competitions.cr.yp.to/caesar.html.

[DEMS19] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. Technical report, National Institute of Standards and Technology, 2019. https://csrc.nist.gov/Projects/lightweight-cryptography/finalists.

[DS09] Itai Dinur and Adi Shamir. Cube attacks on tweakable black box polynomials. In Antoine Joux, editor, EUROCRYPT 2009, volume 5479 of LNCS, pages 278–299, Cologne, Germany, April 26–30, 2009. Springer, Heidelberg, Germany.

[NIS17] NIST Lightweight Cryptography competition, January 2017. https://csrc.nist.gov/Projects/lightweight-cryptography.

[RHSS21] Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun. Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon. IACR Transactions on Symmetric Cryptology, 2021(1):130–155, March 2021.