A New Conditional Cube Attack on Reduced-Round Ascon-128a in a Nonce-misuse Setting

Donghoon Chang[1,2], Jinkeon Kang[1] and Meltem Sönmez Turan[1]

[1] National Institute of Standards and Technology, Gaithersburg, Maryland, USA,
donghoon.chang@nist.gov, jinkeon.kang@nist.gov, meltem.turan@nist.gov
[2] Strativia, Largo, Maryland, USA

Extended Abstract

Ascon [DEMS21] is one of the finalists of the National Institute of Standards and Technology (NIST) lightweight cryptography standardization process. The Ascon family is a permutation-based design that uses monkeyDuplex construction [BDPA12] with extra key additions during initialization and finalization to prevent key-recovery and forgery attacks even after the internal state is recovered by an attacker during the encryption. The family includes three AEAD variants; Ascon-128 (primary), Ascon-128a, and Ascon-80pq. The Ascon family received a significant amount of third party analysis (e.g., [LDW17, LZWW17, RHSS21, RAD19, JM19, ZDW19, DEMS15, Tez16].

The secondary version Ascon-128a claims to provide 128-bit security of privacy and authenticity when unique nonce values are used for the encryption under the same key. The maximum available data to the attacker is limited to 2^{64} 64-bit blocks per key. In a nonce-misuse setting, the designers claimed that Ascon-128a provides 128-bit security of privacy and authenticity if nonces are reused a few times by accident as long as the combination of nonce and associated data stays unique. A key recovery attacks for Ascon-128a with complexity significantly below 2^{96} even after a secret state is recovered by an implementation attack is not expected, due to the extra key additions during the initialization and the finalization.

In 2009, Dinur and Shamir introduced the *cube attacks* to algebraically analyze symmetric-key ciphers. Cube attacks aim to recover secret key bits from the polynomial called *superpoly* by summing the output values over a subset of public variables (e.g., initialization vector or tweak) called the *cube*. Cube attacks were applied to a number of primitives (e.g., [DMP+15, LDB+19, DS11]) The main idea can be considered as a generalization of earlier attacks using higher-order differentials (e.g., include examples). Later, additional variants of the attacks were developed (e.g., dynamic cube attacks [DS11], conditional cube attacks [HWX+17], correlation cube attacks [LYWL18], deterministic cube attacks [YT18], and IV-representation based cube attack [FWDM18] division property-based cube attacks [TIHM17]). The developments in cube attacks is summarized in [COOP22].

In this study, we analyse the security of Ascon-128a in a nonce-misuse setting using conditional cube attacks. Table 1 summarizes the existing cube attacks on Ascon-128a. We present new state and key recovery attacks on a reduced-round Ascon-128a in which the internal permutation for associated data and message processing is reduced from 8 to 7 rounds (the number of rounds for initialization and finalization remain unchanged)[1].

[1]The number of rounds is represented as a 3-tuple representing the number of rounds during initialization,

The state-recovery attack requires 2^{117} data and 2^{118} time with negligible memory. After recovering the state, again in a nonce-misuse scenario, secret key can be recovered with additional 2^{32} data, $2^{97.6}$ time and 2^{32} memory complexities.

Table 1: Summary of cube attacks on Ascon-128a

Attack type	Method	Rounds [1] (12, 8, 12)	Data	Time	Memory	Nonce misuse	Ref.
Key recovery	Conditional cube	6,⋆,⋆	2^{40}	2^{40}	-	No	[LDW17]
	Cube	7,⋆,⋆	$2^{77.2}$	$2^{103.92}$	-	No	[LDW17]
	Cube	7,⋆,⋆	2^{64}	2^{123}	-	No	[RHSS21]
	Cube	7,5,⋆	2^{33}	2^{97}	-	Yes	[LZWW17]
	Conditional cube	⋆,7,⋆	2^{117}	2^{118}	2^{32}	Yes	this study
Forgery	Cube	⋆,⋆,5	2^{17}	2^{17}	-	Yes	[LZWW17]
	Cube	⋆,⋆,6	2^{33}	2^{33}	-	Yes	[LZWW17]
State-recovery	Conditional cube	⋆,7,⋆	2^{117}	2^{118}	-	Yes	this study

Although the presented attacks do not violate the security claims of the designers, they are helpful to understand the security margin of Ascon-128a in nonce-misuse setting.

References

[BDPA12] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. Permutation-based Encryption, Authentication and Authenticated Encryption. DIAC – Directions in Authenticated Ciphers, 2012. https://keccak.team/files/KeccakDIAC2012.pdf.

[COOP22] Marco Cianfriglia, Elia Onofri, Silvia Onofri, and Marco Pedicini. Ten years of cube attacks. Cryptology ePrint Archive, Report 2022/137, 2022. https://ia.cr/2022/137.

[DEMS15] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Cryptanalysis of Ascon. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2015.

[DEMS21] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer. Ascon. Submission to the NIST Lightweight Cryptography Standardization Process, 2021. https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/ascon-spec-final.pdf.

[DMP+15] Itai Dinur, Pawel Morawiecki, Josef Pieprzyk, Marian Srebrny, and Michal Straus. Cube attacks and cube-attack-like cryptanalysis on the round-reduced keccak sponge function. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 733–761. Springer, 2015.

[DS11] Itai Dinur and Adi Shamir. Breaking grain-128 with dynamic cube attacks. In Antoine Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 167–187. Springer, 2011.

[1] the number of rounds during associated data or message processing, and the number of rounds during finalization, respectively. The number represented as ⋆ can be arbitrary.

[FWDM18] Ximing Fu, Xiaoyun Wang, Xiaoyang Dong, and Willi Meier. A key-recovery attack on 855-round trivium. *IACR Cryptol. ePrint Arch.*, page 198, 2018.

[HWX+17] Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang, and Jingyuan Zhao. Conditional cube attack on reduced-round keccak sponge function. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part II*, volume 10211 of *Lecture Notes in Computer Science*, pages 259–288, 2017.

[JM19] Priyanka Joshi and Bodhisatwa Mazumdar. A Subset Fault Analysis of ASCON. Cryptology ePrint Archive, Report 2019/1370, 2019. https://eprint.iacr.org/2019/1370.

[LDB+19] Zheng Li, Xiaoyang Dong, Wenquan Bi, Keting Jia, Xiaoyun Wang, and Willi Meier. New conditional cube attack on keccak keyed modes. *IACR Trans. Symmetric Cryptol.*, 2019(2):94–124, 2019.

[LDW17] Zheng Li, Xiaoyang Dong, and Xiaoyun Wang. Conditional Cube Attack on Round-Reduced ASCON. *IACR Transactions on Symmetric Cryptology*, 2017(1):175–202, Mar. 2017.

[LYWL18] Meicheng Liu, Jingchun Yang, Wenhao Wang, and Dongdai Lin. Correlation cube attacks: From weak-key distinguisher to key recovery. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part II*, volume 10821 of *Lecture Notes in Computer Science*, pages 715–744. Springer, 2018.

[LZWW17] Yanbin Li, Guoyan Zhang, Wei Wang, and Meiqin Wang. Cryptanalysis of round-reduced ASCON. *Sci. China Inf. Sci.*, 60(3):38102, 2017.

[RAD19] K. Ramezanpour, P. Ampadu, and W. Diehl. A Statistical Fault Analysis Methodology for the ASCON Authenticated Cipher. In *2019 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, pages 41–50, 2019.

[RHSS21] Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun. Misuse-free key-recovery and distinguishing attacks on 7-round ascon. *IACR Trans. Symmetric Cryptol.*, 2021(1):130–155, 2021.

[Tez16] Cihangir Tezcan. Truncated, Impossible, and Improbable Differential Analysis of ASCON. In Olivier Camp, Steven Furnell, and Paolo Mori, editors, *Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016, Rome, Italy, February 19-21,2016*, pages 325–332. SciTePress, 2016.

[TIHM17] Yosuke Todo, Takanori Isobe, Yonglin Hao, and Willi Meier. Cube attacks on non-blackbox polynomials based on division property. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 250–279. Springer, 2017.

[YT18] Chen-Dong Ye and Tian Tian. An algebraic method to recover superpolies in cube attacks. Cryptology ePrint Archive, Report 2018/1082, 2018. https://ia.cr/2018/1082.

[ZDW19] Rui Zong, Xiaoyang Dong, and Xiaoyun Wang. Collision Attacks on Round-Reduced Gimli-Hash/Ascon-Xof/Ascon-Hash. Cryptology ePrint Archive, Report 2019/1115, 2019. https://eprint.iacr.org/2019/1115.