Differential-Linear Cryptanalysis of ASCON: Theory vs. Practice

Cihangir Tezcan

Department of Cyber Security, Graduate School of Informatics, Middle East Technical University, Ankara, Turkey
cihangir@metu.edu.tr

Abstract. Experimental results on the differential-linear distinguishers of Ascon show that these distinguishers have better bias in practice compared to the theoretical calculations. This difference suggests that in practice a distinguisher with a worse theoretical bias might be better than the best distinguisher. By using the parallel computing power of GPUs, we observed that better distinguishers can be obtained experimentally in practice which cannot be obtained theoretically by known methods. We obtained the best known 5-round differential-linear distinguishers for the permutation of Ascon experimentally, some of which can be turned into related-key attacks.

1 Introduction

Many differential-linear distinguishers obtained for Ascon work better in practice. For instance, [4] observed that their 4-round differential-linear distinguisher with bias 2^{-20} can be as high as 2^{-2} in practice when checked experimentally. Such a huge difference allows the attacker to perform the attack with a very small amount of data. Differential-linear connectivity table was introduced in [1] to explain this gap by trying to remove the independence assumption between the differential and the linear characteristics and obtained the bias as 2^{-5}. Although it is better than the theoretical bias of 2^{-20}, it is still far from the practical bias of 2^{-2}. Therefore, it is assumed that this gap comes from the large 320-bit state of Ascon and the slow diffusion and confusion provided by the round function. Thus, experiments provide better results compared to the theoretical methods. The best 5-round differential-linear attacks on Ascon was provided in [5] where the biases are $2^{-8.03}$, $2^{-15.05}$, $2^{-14.87}$, and $2^{-11.91}$ when the two key bits for the activated S-box are (0, 0), (0, 1), (1, 0) and (1, 1), respectively. These biases were also obtained experimentally and they are significantly higher than the theoretically obtained values.

Differential-linear attacks combine a differential with a linear approximation. In order to construct such a distinguisher, masked bits in the input of the linear approximation must correspond to the output bits of the differential that have fixed differences. We relaxed this constraint in our experiments and checked the bias of 5-round distinguishers where the input has a difference only at a single

S-box and for the part of the linear approximation we used the one that is used in [5]. We optimized Ascon for GPUs to perform our experiments with more data. This way, we obtained the best 5-round differential-linear distinguishers some of which can also be used as a related-key attack on 5-round Ascon. These new results are obtained in our book chapter that is currently under review [3], which is the expanded version of our conference paper [2].

Checking a 5-round differential-linear Ascon distinguisher with 2^{35} data takes less than a second on an Nvidia RTX 4090 GPU with our optimized implementation. Note that we perform 5-round permutation on a pair. Thus, our optimizations also allow us to try 2^{35} keys in a second when we perform an exhaustive key search attack on the initialization part of Ascon which performs 12-round permutation.

Acknowledgment

The work of Cihangir Tezcan has been supported by TUBITAK 1001 Project under the grant number 121E228 and by Middle East Technical University Scientific Research Projects Coordination Unit under grant number AGEP-704-2023-11294.

References

1. Bar-On, A., Dunkelman, O., Keller, N., Weizman, A.: Dlct: A new tool for differential-linear cryptanalysis. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. pp. 313–342. Springer (2019)
2. Civek, A.B., Tezcan, C.: Experimentally obtained differential-linear distinguishers for permutations of ASCON and DryGASCON (to appear). In: Furnell, S., Mori, P., Weippl, E., Camp, O. (eds.) Information Systems Security and Privacy. Springer International Publishing, Cham (2023)
3. Civek, A.B., Tezcan, C.: Differential-linear attacks on permutation ciphers revisited: Experiments on Ascon and DryGASCON. In: Mori, P., Lenzini, G., Furnell, S. (eds.) Proceedings of the 8th International Conference on Information Systems Security and Privacy, ICISSP 2022, Online Streaming, February 9-11, 2022. pp. 202–209. SCITEPRESS (2022). https://doi.org/10.5220/0010982600003120, https://doi.org/10.5220/0010982600003120
4. Dobraunig, C., Eichlseder, M., Mendel, F.: Heuristic tool for linear cryptanalysis with applications to caesar candidates. In: International Conference on the Theory and Application of Cryptology and Information Security. pp. 490–509. Springer (2015)
5. Tezcan, C.: Analysis of ascon, drygascon, and shamash permutations. International Journal of Information Security Science **9**(3), 172–187 (2020)