Preliminary Analysis of Ascon-Xof and Ascon-Hash

Christoph Dobraunig Maria Eichlseder Florian Mendel
Martin Schläffer

Version 0.1

1 Introduction

In this note, we present additional preliminary analysis dedicated to Ascon-Xof and Ascon-Hash [DEMS19]. Throughout this note, we will use $S^C_{x,y,z}$, $S^N_{x,y,z}$, $S^L_{x,y,z}$ to refer to bit z in word y in round x at the input of the constant addition (S^C), non-linear layer (S^N), and linear layer (S^L), respectively.

2 Preimage Attacks

2.1 Pre-Image on Round-Reduced Ascon-Xof

We consider pre-image attacks on a version of Ascon-Xof where the number of rounds in p^a has been reduced to 2 and the length of the hash value H is truncated to 64 bits. Hence, it is expected to hit this value with a probability of 2^{-64} and thus, the expected workload to find a pre-image is around 2^{64}. For simplicity, we consider the round-reduced variant of Ascon-Xof without round constants and with an all-zero equivalent IV.

If we then take a look at the output of the S-box of the first round, we see that the 3 bits $S^L_{0,0,i}$, $S^L_{0,1,i}$, and $S^L_{0,3,i}$ of the S-box output depend on the input bit $S^N_{0,0,i}$, while the bits $S^L_{0,2,i} = 1$ and $S^L_{0,4,i} = 0$. Hence, after the application of the linear layer, bit i of the first word $S^N_{1,0,i} = \Sigma_{0,i}(S^N_{0,0})$, bit i of the second word $S^N_{1,1,i} = \Sigma_{1,i}(S^N_{0,0})$, bit i of the third word $S^N_{1,2,i} = 1$, bit i of the fourth word $S^N_{1,3,i} = \Sigma_{3,i}(S^N_{0,0})$, and bit i of the fifth word $S^N_{1,4,i} = 0$.

Due to the word-wise structure of Ascon's linear layer, we only have to obey the first bit of the ANF of the S-box and get:

$$\Sigma_0^{-1}(H_i) = S^N_{1,4}S^N_{1,1} + S^N_{1,3} + S^N_{1,2}S^N_{1,1} + S^N_{1,2} + S^N_{1,1}S^N_{1,0} + S^N_{1,1} + S^N_{1,0}$$
$$\Sigma_0^{-1}(H_i) = \Sigma_{0,i}(S^N_{0,0}) \cdot \Sigma_{1,i}(S^N_{0,0}) + \Sigma_{3,i}(S^N_{0,0}) + \Sigma_{0,i}(S^N_{0,0})$$

We see that the only non-linear term is $\Sigma_{0,i}(S^N_{0,0}) \cdot \Sigma_{1,i}(S^N_{0,0})$, which can be linearized by guessing 3 bits of $S^N_{0,0}$. Hence, if we do not take independencies into account, we can get 1 additional linear equation in $S^N_{0,0,i}$ per 3 guessed $S^N_{0,0,i}$. Thus, after 48 guesses, we get 16 linear equations and can attempt to solve the system and get a candidate solution for H. However, this can be improved taking dependencies into account, for instance if 39 consecutive bits in $S^N_{0,0}$ are guessed, already 25 linear equations can be derived. Taking the padding bit into account, we have 63 degrees of freedom, hence, it is likely that a one block solution for a pre-image, which can be found with 2^{39} guesses.

2.2 Pre-Image on Round-Reduced Ascon-Xof with Increased Rate

In this section we will show an attack on Ascon-Xof, where the rate is increased to the first 3 words, the number of rounds for p^a is redued to 3 and the equivalent IV is set to 0. As in the previous section, the hash value H is truncated to 64 bits, hence, a random input value matches a preimage with a probability of 2^{-64}. However, compared to the previous section, we can benefit from the additional degrees of freedom gotten by the increased rate.

For simplicity, we make our considerations without padding. Hence, we have at the input for the first round $S^N_{0,3} = S^N_{0,4} = 0$ due to the IV. Furthermore, we choose an input structure, where $S^N_{0,2} = S^N_{0,0} + 1 = x + 1$ and $S^N_{0,1} = 0$. Thus, after the first round of the permutation, we get the following structure:

$$S^C_{1,0} = 1, S^C_{1,1} = 1, S^C_{1,2} = \Sigma_2(x), S^C_{1,3} = 1, S^C_{1,4} = 0.$$

The constant addition adds at some position a one to $S^C_{1,2,i}$, hence we capture this by introducing linear functions $f_{2,i}$, which correspond to either $f_{2,i} = \Sigma_{2,i}(x)$, or $f_{2,i} = \Sigma_{2,i}(x) + 1$, dependent whether a constant addition happens at position i or not. So, after the second round, we get:

$$S^C_{2,0,i} = 0, S^C_{2,1,i} = \Sigma_{1,i}(f_{2,i}(x)), S^C_{2,2,i} = \Sigma_{2,i}(f_{2,i}(x)), S^C_{2,3,i} = \Sigma_{3,i}(f_{2,i}(x)), S^C_{2,4,i} = 1.$$

Again, we have a constant addition to $S^C_{2,2,i}$, so we get $S^N_{2,2,i} = f'_{2,i}(\Sigma_{2,i}(x))$, where $f'_{2,i} = \Sigma_{2,i}(x)$, or $f'_{2,i} = \Sigma_{2,i}(x) + 1$. Then, we finally end up with:

$$\Sigma_0^{-1}(H_i) = S^L_{2,0} = f'_{2,i}(\Sigma_{2,i}(x)) \cdot \Sigma_{1,i}(f_{2,i}(x)) + \Sigma_{3,i}(f_{2,i}(x)) + f'_{2,i}(\Sigma_{2,i}(x))$$

So we end up with $f'_{2,i}(\Sigma_2(x)) \cdot \Sigma_1(f_{2,i}(x))$ being the only non-linear term. So we focus on it to make it linear by guesses. If we have a look at $\Sigma_{2,i}(\Sigma_{2,i}(x))$, we get:

$$\begin{aligned}\Sigma_{2,i}(\Sigma_{2,i}(x)) &= x_i + x_{i+1} + x_{i+6} + x_{i+1} + x_{i+2} + x_{i+7} + x_{i+6} + x_{i+7} + x_{i+12} \\ &= x_i + x_{i+2} + x_{i+12}\end{aligned}$$

Hence, we can get 16 linear equations for 48 guesses. Hence, if we do not consider padding, we can likely get a solution after the 2^{48} tries since we have 64 degrees of freedom in total.

2.3 Pre-Image on Round-Reduced Ascon-Xof Utilizing the Degree

In this section we again consider round-reduced variants of Ascon-Xof, where the output value H has been truncated to 64 bits. Furthermore, we do not consider the padding. Bernstein [Ber10] gives the general observation that the search for pre-images can be sped-up for low degree functions, since the evaluation of the polynomial in some output bits might use less bit-operations than computing the whole function (in our case the permutation of Ascon). He also states the following formula for the bit operations needed by the attack:

$$T \cdot \sum_{j=0}^{d} \binom{n}{j} + b \cdot \sum_{j=0}^{d} j \binom{n}{j} + b \cdot n \cdot 2^{n-1} + T \cdot 2^{n-b}$$

Where T is the number of bit operations of the function to compute that seperates the input from the hash value, d is the degree of this function, b is the number of bits of the output computed by a polynomial of degree d and n is the number of inputs bits involved in the calculation of the polynomial.

If we consider 5 rounds of Ascon permutation, the output bits have a maximal degree $d = 16$ in the input bits, since for a rate of 64, always one input bit goes to one S-box in the first round. The computation of the output involves $n = 64$ bits. If we now choose $b = 8$, we can find a pre-image in $297 \cdot 2^{64}$ bit-operations instead of $10280 \cdot 2^{64}$ performed in a brute force search. If we consider 6 rounds of Ascon, the improvement by this attack is to use $7213 \cdot 2^{64}$ instead of $12336 \cdot 2^{64}$ when choosing $b = 8$.

3 Collision Attack

In this section, we discuss collision attacks on round-reduced Ascon-Hash and Ascon-Xof. Since we focus in the analysis on collisions during the message absorbing phase of the schemes, our results are applicable to both the hash and eXtendable output function. Collision producing differentials of this form have already be given for 6 rounds of the Ascon permutation in [DEMS16]. Unfortunately, this trail is quite dense as it has 117 active S-boxes. Thus, it is not suited for a collisions attack. Even if we leverage all available degrees of freedom by allowing an attacker to choose the initial value, we are not able to find a collision for 6 (out of 12) rounds. Therefore, we restricted our search to collision producing differentials for 4 and 5 rounds using the same tool as in [DEMS16] that has in the past successfully been used in the analysis of SHA-256 [MNS11; MNS13]. Using this tool, we could find a practical semi-free-start collision for 4 (out of 12) rounds of Ascon-Hash and Ascon-Xof given in Figure 1.

round	state	difference
	177537760b6a7b4b	9000000000040000
	6e7a0bba2ed9e736	0000000000000000
	9aff10e403752f21	0000000000000000
	7ac1d330cf9ee9c2	0000000000000000
	88fc524dd1092975	0000000000000000
	8e2919a34aa78b4f	1040120900040000
	f8ec50f5193e17ff	1000080001040004
1	f8c88d0910726467	0000000000000000
	5c7453f66c0f3efd	0000000000000000
	03f613581bb25cb9	0000000000000000
	14e7b8acbbf085f1	904088490145a084
	6a25ac7c557f0f4e	10428a4101248000
2	9984d786381625f7	08400c2001821006
	1e230875a0079fa9	114602278c44c186
	e0c29f3a0dff9d81	10e0902102082008
	5e994e62eba7e010	c1824ac20aa400cb
	c502f6422ec4b3d7	14831e8a81a4814e
3	c96362c46ea40408	14831e0281a48183
	bf0c9307b5efe0b1	e30040611a1b4881
	2afe991b302b65a3	320000ab913b484c
	ccaa3e2b2adb8f9b	b5463ce488575401
	2648f9ab9dc8f4e0	0000000000000000
4	8d17e35ce6ae9626	0000000000000000
	f92955837cd0e419	0000000000000000
	b78b0c1137cdc72d	0000000000000000

Figure 1: Semi-free-start collision for 4 rounds.

Although we could also find a suitable trail for 5 rounds that is rather sparse over the first 3 rounds, we were not able to find an actual message pair with practical complexity using basic message modification techniques. However, we think that this might be achieved by using more sophisticated message modification techniques, which are particular crafted for the design of Ascon. However, going beyond 5 rounds seems to be infeasible at the moment due to the fact that all collision producing trails for Ascon are very dense. This shows that Ascon-Hash and Ascon-Xof with 12 rounds provide a rather large security margin against collision attacks. Even if using all 320 bits of additional degrees of freedom in a semi-free-start collision, it is currently only possible to attak 4 out of the 12 rounds.

Acknowledgments

Part of this work has been supported by the Austrian Science Fund (FWF): J 4277-N38.

Bibliography

[Ber10] Daniel J. Bernstein. *Second preimages for 6 (7 (8??)) rounds of Keccak?* http://ehash.iaik.tugraz.at/uploads/6/65/NIST-mailing-list_Bernstein-Daemen.txt. (Posted on the NIST mailing list). 2010 (p. 2).

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. *Ascon v1.2*. Submission to Round 3 of the CAESAR competition. 2016. URL: https://ascon.iaik.tugraz.at (p. 3).

[DEMS19] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. *Ascon v1.2*. Submission to NIST. 2019. URL: https://ascon.iaik.tugraz.at (p. 1).

[MNS11] Florian Mendel, Tomislav Nad, and Martin Schläffer. "Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions". In: *ASIACRYPT 2011*. Ed. by Dong Hoon Lee and Xiaoyun Wang. Vol. 7073. LNCS. Springer, 2011, pp. 288–307. DOI: 10.1007/978-3-642-25385-0_16. URL: https://doi.org/10.1007/978-3-642-25385-0%5C_16 (p. 3).

[MNS13] Florian Mendel, Tomislav Nad, and Martin Schläffer. "Improving Local Collisions: New Attacks on Reduced SHA-256". In: *EUROCRYPT 2013*. Ed. by Thomas Johansson and Phong Q. Nguyen. Vol. 7881. LNCS. Springer, 2013, pp. 262–278. DOI: 10.1007/978-3-642-38348-9_16. URL: https://doi.org/10.1007/978-3-642-38348-9%5C_16 (p. 3).