Towards Tight Differential Bounds of Ascon

A Hybrid Usage of SMT and MILP

FSE 2023

Rusydi H. Makarim and Raghvendra Rohit

Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi

Cryptography Research Centre

Technology Innovation Institute

Ascon

Ascon

- Ascon is a family of of authenticated encryption and hashing algorithms designed by Dobraunig, Eichlseder, Mendel, and Schläffer (2014)
- Sponge-based mode of operation
- Ascon-permutation p^r with state size 320 bits and r rounds

Ascon

- Ascon is a family of of authenticated encryption and hashing algorithms designed by Dobraunig, Eichlseder, Mendel, and Schläffer (2014)
- Sponge-based mode of operation
- Ascon-permutation p^r with state size 320 bits and r rounds
- Selected as primary choice for lightweight authenticated encryption in the final portfolio of the CAESAR competition
- Selected as new standard for lightweight cryptography in the NIST lightweight cryptography cometition

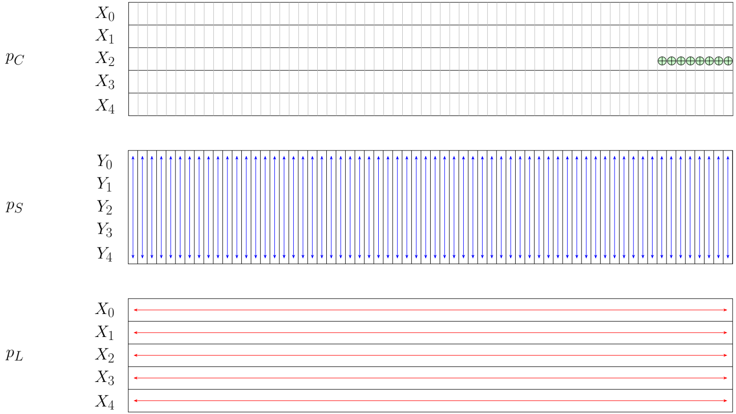
Ascon

- Ascon is a family of of authenticated encryption and hashing algorithms designed by Dobraunig, Eichlseder, Mendel, and Schläffer (2014)
- Sponge-based mode of operation
- Ascon-permutation p^r with state size 320 bits and r rounds
- Selected as primary choice for lightweight authenticated encryption in the final portfolio of the CAESAR competition
- Selected as new standard for lightweight cryptography in the NIST lightweight cryptography cometition

Our goal: Investigate the tight bounds for the differential and linear properties of p^r.

Ascon: Round function (p)

- $p := p_L \circ p_S \circ p_C$



Sbox and linear layer

- Sbox algebraic normal form

$$
\begin{aligned}
y_0 &= x_4x_1 + x_3 + x_2x_1 + x_2 + x_1x_0 + x_1 + x_0 \\
y_1 &= x_4 + x_3x_2 + x_3x_1 + x_3 + x_2x_1 + x_2 + x_1 + x_0 \\
y_2 &= x_4x_3 + x_4 + x_2 + x_1 + 1 \\
y_3 &= x_4x_0 + x_4 + x_3x_0 + x_3 + x_2 + x_1 + x_0 \\
y_4 &= x_4x_1 + x_4 + x_3 + x_1x_0 + x_1
\end{aligned}
$$

- Linear layer

$$
\begin{aligned}
X_0 &\leftarrow \Sigma_0(Y_0) = Y_0 + (Y_0 \ggg 19) + (Y_0 \ggg 28) \\
X_1 &\leftarrow \Sigma_1(Y_1) = Y_1 + (Y_1 \ggg 61) + (Y_1 \ggg 39) \\
X_2 &\leftarrow \Sigma_2(Y_2) = Y_2 + (Y_2 \ggg 1) + (Y_2 \ggg 6) \\
X_3 &\leftarrow \Sigma_3(Y_3) = Y_3 + (Y_3 \ggg 10) + (Y_3 \ggg 17) \\
X_4 &\leftarrow \Sigma_4(Y_4) = Y_4 + (Y_4 \ggg 7) + (Y_4 \ggg 41)
\end{aligned}
$$

- $+$: bitwise XOR; $\ggg$: right cyclic shift

Differential and linear properties of Sbox and linear layer

Sbox

- DDT has entries 2, 4 and 8 meaning the differential probabilities are 2^{-4}, 2^{-3} and 2^{-2}, respectively.
- LAT has entries 4, -4, 8, -8 meaning the bias are 2^{-3}, -2^{3}, 2^{-2} and -2^{-2}, respectively.

Linear layer

- The differential and linear branch number is 4.

Ascon Permutation Differential and Linear Bounds

Differential bounds of Ascon

- Bounds on the number of active Sboxes

#Rounds	Lower bound	Upper bound	Source
4	-	47	[DEMS14]

Differential bounds of Ascon

- Bounds on the number of active Sboxes

#Rounds	Lower bound	Upper bound	Source
4	-	47	[DEMS14]
4	-	44	[DEMS15]

Differential bounds of Ascon

- Bounds on the number of active Sboxes

#Rounds	Lower bound	Upper bound	Source
4	-	47	[DEMS14]
4	-	44	[DEMS15]
4	36 (not tight)	-	[EME22]

Differential bounds of Ascon

- Bounds on the number of active Sboxes

#Rounds	Lower bound	Upper bound	Source
4	-	47	[DEMS14]
4	-	44	[DEMS15]
4	36 (not tight)	-	[EME22]
4	-	43	Ours

Differential bounds of Ascon

- Bounds on the number of active Sboxes

#Rounds	Lower bound	Upper bound	Source
4	-	47	[DEMS14]
4	-	44	[DEMS15]
4	36 (not tight)	-	[EME22]
4	-	43	Ours
5	-	78	[DEMS15]

Differential bounds of Ascon

- Bounds on the number of active Sboxes

#Rounds	Lower bound	Upper bound	Source
4	-	47	[DEMS14]
4	-	44	[DEMS15]
4	36 (not tight)	-	[EME22]
4	-	43	Ours
5	-	78	[DEMS15]
5	-	72	Ours

Differential bounds of Ascon

Cryptography Research Centre

- Bounds on the number of active Sboxes

#Rounds	Lower bound	Upper bound	Source
4	-	47	[DEMS14]
4	-	44	[DEMS15]
4	36 (not tight)	-	[EME22]
4	-	43	Ours
5	-	78	[DEMS15]
5	-	72	Ours

- We found many differential trails with 44 active Sboxes for 4 rounds.
- We did not find a trail with weight better than 107 and 190 for 4 and 5 rounds.
- We proved that the weight of any 3 round differential trail is at least 40 (with MILP + SMT). This was also proved independently in [EME22].

Linear bounds of Ascon

- Bounds on the squared correlation

#Rounds	Lower bound	Upper bound	Source
4	-	2^{-98}	[DEMS15]

Linear bounds of Ascon

- Bounds on the squared correlation

#Rounds	Lower bound	Upper bound	Source
4	-	2^{-98}	[DEMS15]
4	2^{-72} (not tight)	2^{-98}	[EME22]

Linear bounds of Ascon

- Bounds on the squared correlation

#Rounds	Lower bound	Upper bound	Source
4	-	2^{-98}	[DEMS15]
4	2^{-72} (not tight)	2^{-98}	[EME22]
5	-	2^{-186}	[DEMS15]

Linear bounds of Ascon

- Bounds on the squared correlation

#Rounds	Lower bound	Upper bound	Source
4	-	2^{-98}	[DEMS15]
4	2^{-72} (not tight)	2^{-98}	[EME22]
5	-	2^{-186}	[DEMS15]
5	2^{-74} (not tight)	2^{-186}	[EME22]

Linear bounds of Ascon

- Bounds on the squared correlation

#Rounds	Lower bound	Upper bound	Source
4	-	2^{-98}	[DEMS15]
4	2^{-72} (not tight)	2^{-98}	[EME22]
5	-	2^{-186}	[DEMS15]
5	2^{-74} (not tight)	2^{-186}	[EME22]
5	-	2^{-184}	Ours

Linear bounds of Ascon

- Bounds on the squared correlation

#Rounds	Lower bound	Upper bound	Source
4	-	2^{-98}	[DEMS15]
4	2^{-72} (not tight)	2^{-98}	[EME22]
5	-	2^{-186}	[DEMS15]
5	2^{-74} (not tight)	2^{-186}	[EME22]
5	-	2^{-184}	Ours

- The trail for 5 rounds we found has 78 active Sboxes and squared correlation 2^{-184} while the previous best one has 67 active Sboxes and squared correlation 2^{-186}.
- We found multiple linear trails with 43 active Sboxes for 4 rounds but could not improve the squared correlation. We also proved that there is no 3-round linear trail with 14 active Sboxes.

Our Approach

Motivation and basic idea

- SMT or MILP or CP has its own advantage in solving a specific problem, for e.g., SMTs are highly efficient for (un)satisfiability problems while MILP performs well for optimization problems.
- The prior works on automated tools have analyzed ciphers independently with CP, MILP and SMT.
- The run-time becomes difficult to predict for large instances.

Motivation and basic idea

- SMT or MILP or CP has its own advantage in solving a specific problem, for e.g., SMTs are highly efficient for (un)satisfiability problems while MILP performs well for optimization problems.
- The prior works on automated tools have analyzed ciphers independently with CP, MILP and SMT.
- The run-time becomes difficult to predict for large instances.

Our approach: Use SMT and MILP in a hybrid manner.

SMT and MILP models for Ascon

Please see our paper for the model details.

Step 1: Valid configurations of active Sboxes for 2 rounds

Cryptography Research Centre

- Using SMT model, find all valid pairs (d_0, d_1) which results in a differential trail with d_0 and d_1 active Sboxes at round 0 and 1, respectively.
- Example of valid pairs: (1, 3), (1, 11), (2, 4), $\cdots$
- Example of invalid pairs: (3, 4), (10, 3), (16, 3), (18, 3)
- Time: It took seconds for Step 1.

Step 2: Valid configurations of active Sboxes for 3 rounds

Cryptography Research Centre

- Pre-filter some candidates using Step 1.
- Using SMT model, find all valid pairs (d_0, d_1, d_2) which results in a differential trail with d_0, d_1 and d_2 active Sboxes at round 0, 1 and 2, respectively.

15	{(1, 3, 11)}
16	{(1, 3, 12), (2, 4, 10)}
17	{(1, 3, 13), (2, 4, 11)}
18	{(1, 3, 14), (2, 4, 12), (4, 4, 10)}
19	{(1, 3, 15), (2, 4, 13), (3, 3, 13), (4, 4, 11)}
22	{(1, 3, 18), (1, 5, 16), (2, 4, 16), (2, 5, 15), (2, 6, 14), (3, 3, 16), (3, 5, 14), (3, 6, 13), (4, 4, 14), (4, 5, 13), (4, 6, 12), (5, 4, 13), (5, 5, 12), (5, 6, 11), (6, 4, 12), (6, 5, 11), (6, 6, 10), (7, 4, 11), (7, 5, 10), (8, 4, 10), (8, 5, 9), (10, 2, 10)}

Total configurations

- Comparison of number of configurations for 3-round trails. Here $\mathcal{U}$ denotes the number of remaining cases left to solve for completing the search space for a given n.

n	$\lvert\mathcal{I}_n^3\rvert$	$\lvert\mathcal{S}_n^3\rvert$	$\mathcal{U}$	n	$\lvert\mathcal{I}_n^3\rvert$	$\lvert\mathcal{S}_n^3\rvert$	$\mathcal{U}$
15	37	1	0	24	156	≥ 43	35
16	47	2	0	25	174	≥ 55	38
17	56	2	0	26	195	≥ 62	47
18	66	3	0	27	215	≥ 73	67
19	77	4	0	28	236	≥ 85	77
20	90	8	0	29	257	≥ 88	98
21	104	21	0	30	279	≥ 95	114
22	121	22	0	31	303	≥ 118	111
23	137	≥ 35	21	32	328	≥ 136	117

- The average time to solve a single instance was around 15-20 minutes. Some instances could be solved in seconds while others took more than an hour.

Proof: Minimum weight of 3-round differential trail

- We take all configurations up to 20 active Sboxes and find their weight using MILP.

(d_0, d_1, d_2)	Minimum weight	(d_0, d_1, d_2)	Minimum weight
(1, 3, 11)	40	(1, 3, 12)	46
(2, 4, 10)	43	(1, 3, 13)	44
(2, 4, 11)	46	(1, 3, 14)	44
(2, 4, 12)	46	(4, 4, 10)	≥ 43 [not tight]
(1, 3, 15)	49	(2, 4, 13)	49
(3, 3, 13)	45	(4, 4, 11)	≥ 41 [not tight]
(1, 3, 16)	49	(1, 5, 14)	55
(2, 4, 14)	50	(2, 5, 13)	55
(3, 3, 14)	49		

Step 3: Valid configurations of active Sboxes for 4 rounds

- Pre-filter some candidates using invalid pairs from Step 1 and Step 2. (# candidates ≈ 72000)

Step 3: Valid configurations of active Sboxes for 4 rounds

- Pre-filter some candidates using invalid pairs from Step 1 and Step 2. (# candidates ≈ 72000)
- Using SMT and MILP, pre-filter more candidates by extending 3-round valid configurations in forward and backward directions. See Lemmas 1-4 in our paper. We found a differential trail with 43 active Sboxes at this stage. (# candidates ≈ 11496). It took around 8 CPU days for this reduction.

Step 3: Valid configurations of active Sboxes for 4 rounds

- Pre-filter some candidates using invalid pairs from Step 1 and Step 2. (# candidates ≈ 72000)
- Using SMT and MILP, pre-filter more candidates by extending 3-round valid configurations in forward and backward directions. See Lemmas 1-4 in our paper. We found a differential trail with 43 active Sboxes at this stage. (# candidates ≈ 11496). It took around 8 CPU days for this reduction.
- There are at least 36 active Sboxes for 4 rounds (result from [EME22]). This reduces the number of cases to 9793.

Notes on time complexity and reducing cases further

- There are easy configurations which returns False within $2 - 20$ minutes while there are some which require even 2 hours or more.

Notes on time complexity and reducing cases further

Cryptography Research Centre

- There are easy configurations which returns False within $2 - 20$ minutes while there are some which require even 2 hours or more.
- Out of the 9793 cases, there are 954 cases where $d_0 = 5$. We find that a necklace with weight 5 at round 0 on average require 2.5 minutes to return True or False (checked with around 105 necklaces).

Notes on time complexity and reducing cases further

- There are easy configurations which returns False within $2 - 20$ minutes while there are some which require even 2 hours or more.
- Out of the 9793 cases, there are 954 cases where $d_0 = 5$. We find that a necklace with weight 5 at round 0 on average require 2.5 minutes to return True or False (checked with around 105 necklaces).
- Out of the 9793 cases, there are 504 cases where $d_1 = 5$. We solved all 119133 necklaces in 5 days and could not find any 4-round trail of the form $(d_0, 5, d_2, d_3)$ such that $d_0 + 5 + d_2 + d_3 \leq 42$.

Notes on time complexity and reducing cases further

- There are easy configurations which returns False within $2-20$ minutes while there are some which require even 2 hours or more.
- Out of the 9793 cases, there are 954 cases where $d_0 = 5$. We find that a necklace with weight 5 at round 0 on average require 2.5 minutes to return True or False (checked with around 105 necklaces).
- Out of the 9793 cases, there are 504 cases where $d_1 = 5$. We solved all 119133 necklaces in 5 days and could not find any 4-round trail of the form $(d_0, 5, d_2, d_3)$ such that $d_0 + 5 + d_2 + d_3 \leq 42$.
- #remaining cases: 9289

Notes on time complexity and reducing cases further

- There are easy configurations which returns False within $2 - 20$ minutes while there are some which require even 2 hours or more.
- Out of the 9793 cases, there are 954 cases where $d_0 = 5$. We find that a necklace with weight 5 at round 0 on average require 2.5 minutes to return True or False (checked with around 105 necklaces).
- Out of the 9793 cases, there are 504 cases where $d_1 = 5$. We solved all 119133 necklaces in 5 days and could not find any 4-round trail of the form $(d_0, 5, d_2, d_3)$ such that $d_0 + 5 + d_2 + d_3 \leq 42$.
- #remaining cases: 9289
- Difficult to predict time to find the exact bound. However, some other techniques may filter these cases in an efficient way.

Extension to 5 rounds and linear trails

- We used a similar approach to find the 5-round differential trail with 72 active Sboxes. The configuration is (5, 9, 10, 23, 25).
- Again, we use the same approach to find the new 5-round linear trail with 78 [21, 5, 9, 11, 30] active Sboxes and correlation 92 [21, 5, 18, 18, 30].

Concluding Remarks

Concluding remarks

- We improved the differential and linear bounds of Ascon using MILP and SMT in a hybrid manner.
- Finding exact differential and linear bounds for 4 rounds Ascon is still challenging.
- Finding all 3-round valid/invalid choices up to 30 active Sboxes will reduce the number of cases significantly.
- The hybrid approach could be utilized for other ciphers as well.

Thank you!

Cryptography Research Centre

`https://github.com/Crypto-TII/ascon_hybrid_milp_smt`
`https://tosc.iacr.org/index.php/ToSC/article/view/9859/9358`

Technology Innovation Institute

Cryptography Research Centre

tii.ae