Misuse-Free Key-Recovery and Distinguishing Attacks on 7-Round Ascon

NIST LWC 2022

Raghvendra Rohit, Kai Hu, Sumanta Sarkar & Siwei Sun

Motivation

Cryptography Research Centre

- Ascon is one of the winners of the CAESAR competition in lightweight applications category
- Finalist (out of 10) of the ongoing NIST lightweight cryptography standardization competition

Motivation

Cryptography Research Centre

- Ascon is one of the winners of the CAESAR competition in lightweight applications category
- Finalist (out of 10) of the ongoing NIST lightweight cryptography standardization competition
- Considering (1) nonce-respecting setting and (2) data limit of 2^{64} blocks (associated data + plaintext) per key

Best known attacks cover up to 6 out of 12 rounds

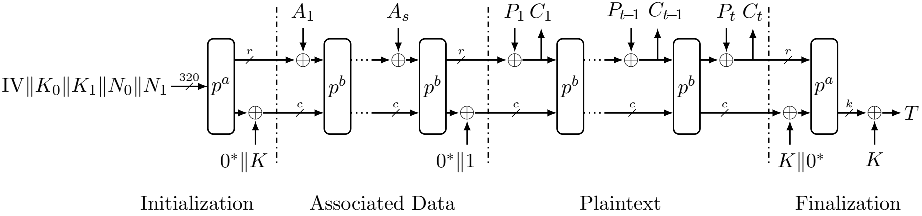
Motivation

- Ascon is one of the winners of the CAESAR competition in lightweight applications category
- Finalist (out of 10) of the ongoing NIST lightweight cryptography standardization competition
- Considering (1) nonce-respecting setting and (2) data limit of 2^{64} blocks (associated data + plaintext) per key

Best known attacks cover up to 6 out of 12 rounds

This work: First key recovery attacks and distinguishers on 7-round Ascon AEAD without violating the design's security claims.

Ascon AEAD: Mode of operation



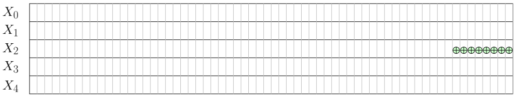
Name	State size	Rate r	Size of			Rounds	
			Key	Nonce	Tag	p^a	p^b
Ascon-128	320	64	128	128	128	12	6
Ascon-128a	320	128	128	128	128	12	8

- Ascon figures adapted from [DEMS14]; Sponge duplex [BDPA12]; Monkey duplex [Dae12]

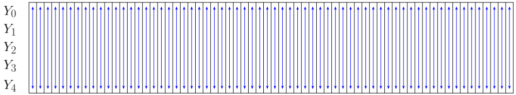
Ascon: Round function (p)

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

p_C

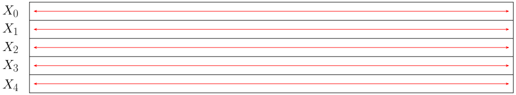


p_S



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

p_L



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

Key-Recovery Attacks on 7-Round

Cube attacks [Vie07, DS09]

- Consider a boolean function f in 6 variables

$$f(k_0, k_1, k_2, v_0, v_1, v_2) = v_0 k_1 + v_1 k_0 + v_0 v_1 (k_0 + k_2 + 1) + v_2$$

where k_0, k_1, k_2 are secret variables and v_0, v_1, v_2 are public variables

- Taking 2-order derivative wrt to v_0 and v_1

$$\begin{aligned} & f(k_0, k_1, k_1, 0, 0, v_2) + f(k_0, k_1, k_1, 0, 1, v_2) + \\ & f(k_0, k_1, k_1, 1, 0, v_2) + f(k_0, k_1, k_1, 1, 1, v_2) \\ & = k_0 + k_2 + 1 \end{aligned}$$

Cube attacks [Vie07, DS09]

- Consider a boolean function f in 6 variables

$$f(k_0, k_1, k_2, v_0, v_1, v_2) = v_0k_1 + v_1k_0 + v_0v_1(k_0 + k_2 + 1) + v_2$$

where k_0, k_1, k_2 are secret variables and v_0, v_1, v_2 are public variables

- Taking 2-order derivative wrt to v_0 and v_1

$$\begin{aligned} & f(k_0, k_1, k_1, 0, 0, v_2) + f(k_0, k_1, k_1, 0, 1, v_2) + \\ & f(k_0, k_1, k_1, 1, 0, v_2) + f(k_0, k_1, k_1, 1, 1, v_2) \\ & = k_0 + k_2 + 1 \end{aligned}$$

- v_0v_1 : 2-dimensional cube; v_2 : non-cube variable
- $k_0 + k_2 + 1$: superpoly of cube v_0v_1
- A superpoly can give partial information about key bits. Recovering the superpoly of a given cube is not easy.

Key-Recovery attack on 7-round

- Initial state with cube variables in X_3^0

1	0	0	0	0	0	0	0	0	1	0	0	0	0	$\cdots$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X_0^0
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}	k_{13}	$\cdots$	k_{50}	k_{51}	k_{52}	k_{53}	k_{54}	k_{55}	k_{56}	k_{57}	k_{58}	k_{59}	k_{60}	k_{61}	k_{62}	k_{63}	X_1^0
k_{64}	k_{65}	k_{66}	k_{67}	k_{68}	k_{69}	k_{70}	k_{71}	k_{72}	k_{73}	k_{74}	k_{75}	k_{76}	k_{77}	$\cdots$	k_{114}	k_{115}	k_{116}	k_{117}	k_{118}	k_{119}	k_{120}	k_{121}	k_{122}	k_{123}	k_{124}	k_{125}	k_{126}	k_{127}	X_2^0
v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	$\cdots$	v_{50}	v_{51}	v_{52}	v_{53}	v_{54}	v_{55}	v_{56}	v_{57}	v_{58}	v_{59}	v_{60}	v_{61}	v_{62}	v_{63}	X_3^0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X_4^0

Key-Recovery attack on 7-round

- Initial state with cube variables in X_3^0

1	0	0	0	0	0	0	0	0	1	0	0	0	0	$\cdots$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X_0^0
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}	k_{13}	$\cdots$	k_{50}	k_{51}	k_{52}	k_{53}	k_{54}	k_{55}	k_{56}	k_{57}	k_{58}	k_{59}	k_{60}	k_{61}	k_{62}	k_{63}	X_1^0
k_{64}	k_{65}	k_{66}	k_{67}	k_{68}	k_{69}	k_{70}	k_{71}	k_{72}	k_{73}	k_{74}	k_{75}	k_{76}	k_{77}	$\cdots$	k_{114}	k_{115}	k_{116}	k_{117}	k_{118}	k_{119}	k_{120}	k_{121}	k_{122}	k_{123}	k_{124}	k_{125}	k_{126}	k_{127}	X_2^0
v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	$\cdots$	v_{50}	v_{51}	v_{52}	v_{53}	v_{54}	v_{55}	v_{56}	v_{57}	v_{58}	v_{59}	v_{60}	v_{61}	v_{62}	v_{63}	X_3^0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	$\cdots$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X_4^0

- Observation

For $1 \leq r \leq 7$ and $I = \{i_0, i_1, \ldots, i_{2^{r-1}-1}\} \subseteq \{0, 1, \ldots, 63\}$, the coefficient of the monomial $\prod_{i \in I} v_i$ in $X_i^r[j]$ for any $i \in \{0, \cdots, 4\}$ and $j \in \{0, \cdots, 63\}$ can be fully determined by the 2^r equivalent key bits in $\{k_{i_0} + k_{i_0+64}, \cdots, k_{i_{2^{r-1}-1}} + k_{i_{2^{r-1}-1}+64}\}$.

- The above observation was used in [DEMS15] to attack up to 6 rounds. Here, we use this observation with a different technique to attack 7 round.

Goal

Cryptography Research Centre

Recover the superpoly of the cube $v_0 v_1 \cdots v_{63}$ after 7-round for $X_0^7[j]$ for $0 \leq j \leq 63$ with time $< 2^{128}$ 7-round Ascon calls?

$$\Downarrow$$

Enough to recover the superpoly of the cube $v_0 v_1 \cdots v_{63}$ after the 6-round S-box layer, i.e., for $Y_0^6[j]$ for $0 \leq j \leq 63$ (invert the last linear layer)

Goal

Cryptography Research Centre

Recover the superpoly of the cube $v_0 v_1 \cdots v_{63}$ after 7-round for $X_0^7[j]$ for $0 \leq j \leq 63$ with time $< 2^{128}$ 7-round Ascon calls?

$$\Downarrow$$

Enough to recover the superpoly of the cube $v_0 v_1 \cdots v_{63}$ after the 6-round S-box layer, i.e., for $Y_0^6[j]$ for $0 \leq j \leq 63$ (invert the last linear layer)

Our technique: Partial polynomial multiplication !!

Partial polynomial multiplication

- Consider the ANF of first column after round 1

$X_0^1[0]$	$X_1^1[0]$	$X_2^1[0]$	$X_3^1[0]$	$X_4^1[0]$
1	1	k_{127}	1	v_{57}
v_{45}	$v_{25}(k_{25}+k_{89}+1)$	k_{122}	v_{54}	v_{23}
v_{36}	$v_{3}(k_{3}+k_{67}+1)$	k_{64}	v_{47}	v_{0}
v_{0}	$v_{0}\ (k_{0}+k_{64}+1)$	k_{63}	k_{118}	k_{57}
$k_{45}k_{109}$	$k_{25}k_{89}$	k_{58}	k_{111}	k_{23}
$k_{36}k_{100}$	$k_{3}k_{67}$	k_{0}	k_{64}	
$k_{0}k_{64}$	$k_{0}k_{64}$		k_{54}	
k_{109}	k_{89}		k_{47}	
k_{100}	k_{67}		k_{0}	
k_{64}	k_{64}			
k_{45}	k_{25}			
k_{36}	k_{3}			
	k_{0}			

Partial polynomial multiplication

$X_0^1[0]$	$X_1^1[0]$	$X_2^1[0]$	$X_3^1[0]$	$X_4^1[0]$
v_{45}	$v_{25}(k_{25} + k_{89} + 1)$		v_{54}	v_{57}
v_{36}	$v_3(k_3 + k_{67} + 1)$		v_{47}	v_{23}
v_0	$v_0\ (k_0 + k_{64} + 1)$			v_0

- Superpoly recovery: Apply to 7-round Ascon in two steps:
  - Enumerate all 32-dimensional cubes and their corresponding superpolies after 6 rounds
  - Multiply all partial polynomials to obtain the superpoly of 64-dimensional cube
- Filter the equivalent key using the cube-sum value, and then the master key

Offline phase

- Goal: Recover the superpolies of cube $v_0 v_1 \cdots v_{63}$ for $Y_0^6[j]$ for $0 \leq j \leq 63$
- We show the procedure for $Y_0^6[0]$ only

Offline phase

- Goal: Recover the superpolies of cube $v_0 v_1 \cdots v_{63}$ for $Y_0^6[j]$ for $0 \leq j \leq 63$
- We show the procedure for $Y_0^6[0]$ only

$$Y_0^6[0] = X_4^6[0]X_1^6[0] + X_3^6[0] + X_2^6[0]X_1^6[0] + X_2^6[0] + X_0^6[0]X_1^6[0] + X_1^6[0] + X_0^6[0]$$

$$\Downarrow$$

Only need to compute $X_1^6[0](X_4^6[0] + X_2^6[0] + X_0^6[0])$

Offline phase (1)

Cryptography Research Centre

- Example of a data structure

$X_1^6[0]$	$X_4^6[0] + X_2^6[0] + X_0^6[0]$
0xFFFFFFFF00000000 $[1, k_0, k_{64}, \cdots]$	0xEFFFFFFF10000000 $[k_1, k_{65}, \cdots]$
$\vdots$	$\vdots$
0xAFFFFFFF10000000 $[k_2, k_{66}, \cdots]$	0x00000000FFFFFFFF $[0]$

- Memory: $\binom{64}{32} \times 2^{32} \times 320 \approx 2^{101}$

Offline phase (2)

- Time (worst cases)
  - Step 1 : Finding cubes + superpolies of 6-round

$$\underbrace{\binom{64}{32}}_{\text{cubes}} \times \underbrace{2^{32}}_{\text{dimension}} \times \underbrace{\sum_{i=0}^{15} \binom{32}{i}}_{\text{monomials}} \approx 2^{123.48}$$

  - Step 2: Memory accesses for partial polynomial multiplication

$$\underbrace{\binom{64}{32}}_{\text{cubes}} \times \underbrace{\sum_{i=0}^{15} \binom{32}{i} \times \sum_{i=0}^{15} \binom{32}{i}}_{\text{monomials}} \approx 2^{122.26}$$

- Step 2 can be computed in a parallel fashion

Offline phase (3)

Cryptography Research Centre

- Generating the comparison tables for key candidates

- Define a vectorial Boolean function $F : \mathbb{F}_2^{64} \rightarrow \mathbb{F}_2^{64}$ mapping $(\kappa_0, \kappa_1, \ldots, \kappa_{63})$ to $(\mathrm{Coe}_{Y_0^6[0]}(\prod_{i=0}^{63} v_i), \ldots, \mathrm{Coe}_{Y_0^6[63]}(\prod_{i=0}^{63} v_i))$ where $\kappa_j = k_j + k_{j+64}$
- Store each $(\kappa_0, \kappa_1, \ldots, \kappa_{63}) \in \mathbb{F}_2^{64}$ into a hash table $\mathbb{H}$ at address $F(\kappa_0, \kappa_1, \ldots, \kappa_{63})$, which requires about $2^{64} \times 64 = 2^{70}$ bits of memory

Online phase

- Denote the cube sum as $(z_0, z_1, \ldots, z_{63})$. Then the equivalent key candidates are just obtained from $\mathbb{H}[(z_0, z_1, \ldots, z_{63})]$. On average, one key candidate is obtained.

- Perform an exhaustive search over the 64-bit key space $\{k_0, k_1, \ldots, k_{63}\}$. For each guess of $\{k_0, k_1, \ldots, k_{63}\}$, we first compute $k_{64+i} = k_i + \kappa_i$ for $i \in \{0, 1, \ldots, 63\}$ and then determine the right key by testing a plaintext and ciphertext pair.

- Time : 2^{64} 7-round Ascon

Overall attack complexities

Cryptography Research Centre

- Data: 2^{64}
- Memory: $2^{101} + 2^{70}$ (discard 2^{101} memory after superpolies are recovered)
- Time: 2^{123} 7-round Ascon calls

New Distinguishers

New cube distinguishers

Cryptography Research Centre

- Initial state

1	0	0	0	0	0	0	0	0	1	0	0	0	0	$\cdots$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	X_0^0
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{11}	k_{12}	k_{13}	$\cdots$	k_{50}	k_{51}	k_{52}	k_{53}	k_{54}	k_{55}	k_{56}	k_{57}	k_{58}	k_{59}	k_{60}	k_{61}	k_{62}	k_{63}	X_1^0
k_{64}	k_{65}	k_{66}	k_{67}	k_{68}	k_{69}	k_{70}	k_{71}	k_{72}	k_{73}	k_{74}	k_{75}	k_{76}	k_{77}	$\cdots$	k_{114}	k_{115}	k_{116}	k_{117}	k_{118}	k_{119}	k_{120}	k_{121}	k_{122}	k_{123}	k_{124}	k_{125}	k_{126}	k_{127}	X_2^0
v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	$\cdots$	v_{50}	v_{51}	v_{52}	v_{53}	v_{54}	v_{55}	v_{56}	v_{57}	v_{58}	v_{59}	v_{60}	v_{61}	v_{62}	v_{63}	X_3^0
v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	$\cdots$	v_{50}	v_{51}	v_{52}	v_{53}	v_{54}	v_{55}	v_{56}	v_{57}	v_{58}	v_{59}	v_{60}	v_{61}	v_{62}	v_{63}	X_4^0

- For $0 \leq j \leq 63$, set $X_4[j] = X_3[j]$

$$\begin{cases} Y_0[j] \leftarrow X_3[j]X_1[j] + X_3[j] + X_2[j]X_1[j] + X_2[j] + X_1[j]X_0[j] + X_1[j] + X_0[j] \\ Y_1[j] \leftarrow X_3[j]X_2[j] + X_3[j]X_1[j] + X_2[j]X_1[j] + X_2[j] + X_1[j] + X_0[j] \\ \color{red}{Y_2[j]} \leftarrow X_2[j] + X_1[j] + 1 \\ \color{red}{Y_3[j]} \leftarrow X_2[j] + X_1[j] + X_0[j] \\ Y_4[j] \leftarrow X_3[j]X_1[j] + X_1[j]X_0[j] + X_1[j] \end{cases}$$

Upper bounds of degree

Cryptography Research Centre

- Upper bounds on the algebraic degree of Ascon in cube variables using 3 subset bit based division property [HLM+20]

Round r	Bits in word				
	X_0^r	X_1^r	X_2^r	X_3^r	X_4^r
2	2	1	1	2	2
3	3	3	4	4	3
4	7	8	7	7	6
5	15	15	13	14	15
6	30	29	29	30	30
7	59	59	60	60	58

- Cube variables $\{v_i, v_{i+8}, v_{i+16}, v_{i+17}, v_{i+34}, v_{i+63}\}$ do not multiply with each other after round 2. Choosing any 5 out of 6 gives a distinguisher with 32 nonces for 4 rounds.

Summary

Type	#Rounds	Time	Method	Validity	Ref.
Key recovery	4/12	2^{18}	Differential-linear	✓	[DEMS15]
	5/12	2^{36}	Differential-linear	✓	[DEMS15]
	5/12	2^{35}	Cube-like	✓	[DEMS15]
	5/12	2^{24}	Conditional cube	✓	[LDW17]
	6/12	2^{66}	Cube-like	✓	[DEMS15]
	6/12	2^{40}	Cube-like	✓	[DEMS15]
	7/12	$2^{103.9}$	Conditional cube	✗	[LDW17]
	7/12	2^{77}	Conditional cube‡	✗	[LDW17]
	7/12	2^{97}	Cube-like	✗	[LZWW17]
	7/12	2^{97}	Cube tester	✗	[LZWW17]
	7/12	2^{123}	Cube	✓	Ours
Distinguishers	4/12	2^{9}	Degree	✓	[DEMS15]
	5/12	2^{17}	Degree	✓	[DEMS15]
	6/12	2^{33}	Degree	✓	[DEMS15]
	4/12	2^{5}	Division Property	✓	Ours
	5/12	2^{16}	Division Property	✓	Ours
	6/12	2^{31}	Division Property	✓	Ours
	7/12	2^{60}	Division Property	✓	Ours

‡ : Weak key setting

Thank you!

https://github.com/raghavrohit/ascon_cube_distinguishers

https://tosc.iacr.org/index.php/ToSC/article/view/8835

Technology Innovation Institute

Cryptography Research Centre

tii.ae