Distinguishers for Reduced Round Ascon, DryGASCON, and Shamash Permutations

Cihangir TEZCAN

Institute of Informatics, Department of Cyber Security
MIDDLE EAST TECHNICAL UNIVERSITY, ANKARA, TURKEY

3rd Lightweight Cryptography Workshop at NIST
Gaithersburg USA
5 November 2019

Outline

ASCON

ASCON

- Designed by *Christoph Dobraunig*, *Maria Eichlseder*, *Florian Mendel*, *Martin Schlaffer*
- 2-round candidate in NIST's LWC standardization process
- Primary choice for lightweight AE of the CAESAR competition
- Type: Sponge construction
- Primitive: SPN
  - Block size: 64 or 128 bits
  - State size: 320 bits
  - Key: 128 bits (initial version supported 96 bits)
  - Nonce: 128 bits
  - Tag: 128 bits
  - Rounds: 12

ASCON

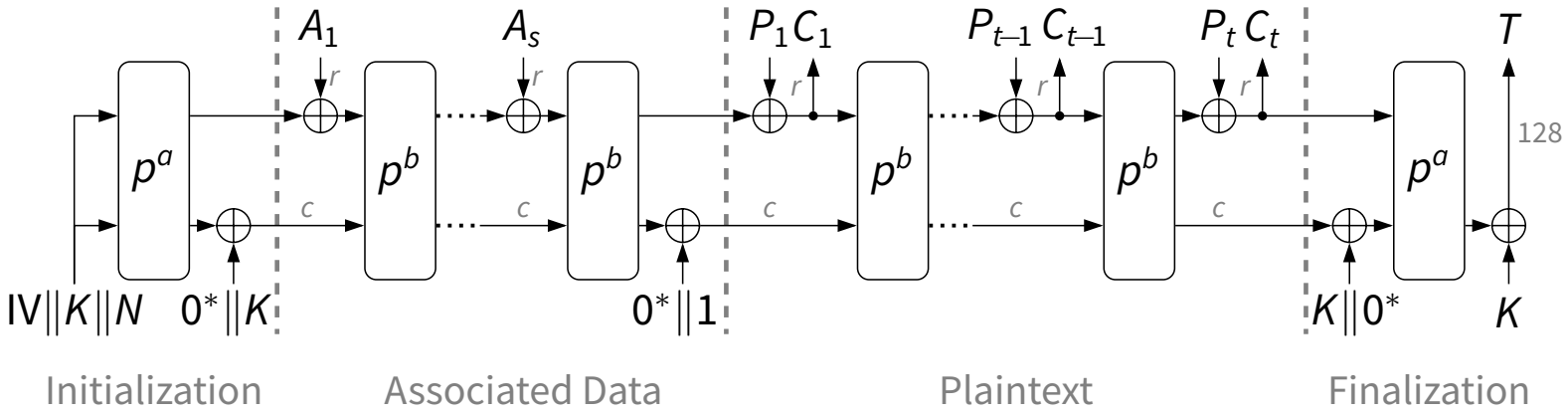


Figure: The encryption of ASCON. p^a means the permutation operation p is performed a times. We have $a = 12$ and $b = 8$.

ASCON State

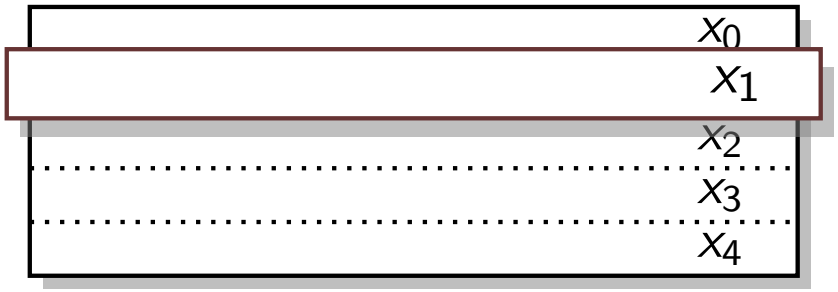


Figure: 320-bit state Ascon

ASCON - Substitution Layer

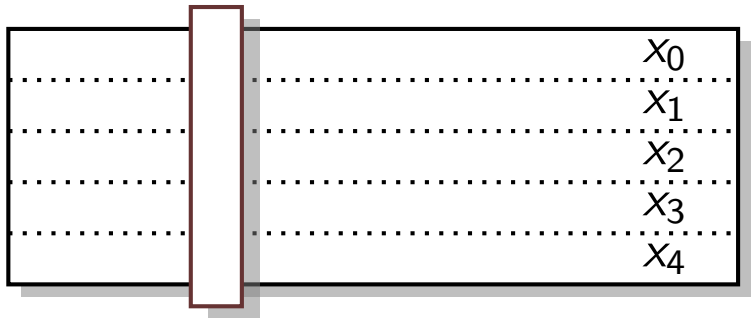


Table: ASCON's 5-bit s-box.

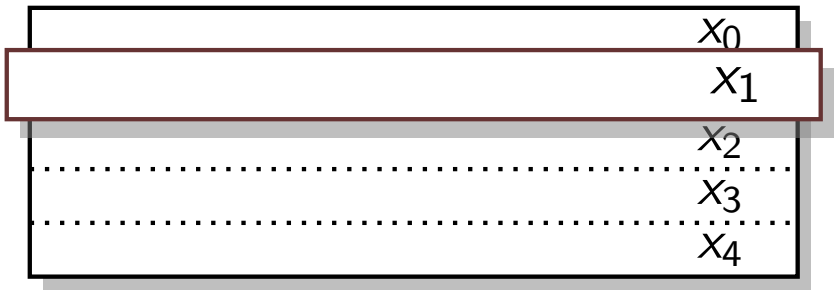
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	4	11	31	20	26	21	9	2	27	5	8	18	29	3	6	28
x	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
S(x)	30	19	7	14	0	13	17	24	16	12	1	25	22	10	15	23

ASCON - DDT

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	10	11	12	13	14	15	16	17	18	19	1a	1b	1c	1d	1e	1f
0	32	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
1	·	·	·	·	·	·	·	·	·	4	·	4	·	4	·	4	·	·	·	·	·	·	·	·	4	·	4	·	4	·	4	·
2	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	4	·	4	·	4	·	4	·	4	·	4	·	4	·	4
3	·	4	·	·	·	4	·	·	·	4	·	·	·	4	·	·	4	·	·	·	4	·	·	·	4	·	·	·	4	·	·	·
4	·	·	·	·	·	·	8	·	·	·	·	·	·	·	8	·	·	·	·	·	·	·	8	·	·	·	·	·	·	·	8	·
5	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	4	·	4	4	·	4	·	4	·	4	·	·	4	·	4
6	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2
7	·	·	4	4	·	·	4	4	·	·	4	4	·	·	4	4	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
8	·	·	·	·	·	·	4	4	·	·	·	·	·	·	4	4	·	·	·	·	·	·	4	4	·	·	·	·	·	·	4	4
9	·	2	·	2	2	·	2	·	2	·	2	·	·	2	·	2	2	·	2	·	·	2	·	2	·	2	·	2	2	·	2	·
a	·	2	2	·	2	·	·	2	·	2	2	·	2	·	·	2	·	2	2	·	2	·	·	2	·	2	2	·	2	·	·	2
b	·	·	2	2	·	·	2	2	·	·	2	2	·	·	2	2	·	·	2	2	·	·	2	2	·	·	2	2	·	·	2	2
c	·	8	·	·	·	·	·	·	8	·	·	·	·	·	·	·	8	·	·	·	·	·	·	·	·	8	·	·	·	·	·	·
d	·	2	·	2	·	2	·	2	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	·	2	·	2	·	2	·	2
e	·	4	4	·	4	·	·	4	·	·	·	·	·	·	·	·	·	4	4	·	4	·	·	4	·	·	·	·	·	·	·	·
f	·	·	·	·	·	·	·	·	4	4	·	·	4	4	·	·	·	·	·	·	·	·	·	·	4	4	·	·	4	4	·	·
10	·	·	·	·	·	·	·	·	·	8	·	8	·	·	·	·	·	·	·	·	·	·	·	·	8	·	8	·	·	·	·	·
11	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	8	·	8	·	8	·	8	·	·	·	·	·	·	·	·
12	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	2	·	2	·	2	·	2	·	2	·	2	·	2	·	2	·
13	·	·	8	·	8	·	·	·	·	·	8	·	8	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
14	·	·	·	·	4	4	4	4	·	·	·	·	4	4	4	4	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·
15	·	·	·	·	·	4	·	4	·	4	·	4	·	·	·	·	·	4	·	4	·	·	·	·	·	·	·	·	·	4	·	4
16	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
17	·	·	4	·	4	·	·	·	·	·	4	·	4	·	·	·	·	·	4	·	4	·	·	·	·	·	4	·	4	·	·	·
18	·	·	·	·	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	2	2	2	2
19	·	·	·	4	·	·	4	·	4	·	·	·	·	4	·	·	4	·	·	·	·	4	·	·	·	·	·	4	·	·	4	·
1a	·	2	2	·	·	2	2	·	2	·	·	2	2	·	·	2	·	2	2	·	·	2	2	·	2	·	·	2	2	·	·	2
1b	·	·	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	2	2	2	2	·	·	·	·	2	2	2	2	·	·
1c	·	4	·	4	·	·	·	·	4	·	4	·	·	·	·	·	4	·	4	·	·	·	·	·	·	4	·	4	·	·	·	·
1d	·	·	·	4	·	4	·	·	4	·	·	·	·	·	4	·	4	·	·	·	·	·	4	·	·	·	·	4	·	4	·	·
1e	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2	·	·	·	·	·	·	·	·	2	2	2	2	2	2	2	2
1f	·	·	4	4	4	4	·	·	·	·	·	·	·	·	·	·	·	·	4	4	4	4	·	·	·	·	·	·	·	·	·	·

ASCON - Linear Diffusion Layer

$$\Sigma_0(x_0) = x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28)$$
$$\Sigma_1(x_1) = x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 39)$$
$$\Sigma_2(x_2) = x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6)$$
$$\Sigma_3(x_3) = x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17)$$
$$\Sigma_4(x_4) = x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 41)$$



ASCON - S-box Analysis

Undisturbed Bits [Tez14]

For a specific input difference of an S-box, if some bits of the output difference remain invariant, then we call such bits *undisturbed*

Table: Undisturbed Bits of ASCON's S-box

Input Difference	Output Difference	Input Difference	Output Difference
00001	?1???	10000	?10??
00010	1???1	10001	10??1
00011	???0?	10011	0???0
00100	??110	10100	0?1??
00101	1????	10101	????1
00110	????1	10110	1????
00111	0??1?	10111	????0
01000	??11?	11000	??1??
01011	???1?	11100	??0??
01100	??00?	11110	?1???
01110	?0???	11111	?0???
01111	?1?0?		

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
I	1000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 1000000000000000000000000000000000000000000000000000000000000000 1000000000000000000000000000000000000000000000000000000000000000

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
I	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
S_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
I	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
S_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
P_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000?000000000000000000000?00
	??0000?000000000000000000000000000000000000000000000000000000000000
	?000000000?000000?000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
I	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
S_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
P_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000?000000000000000000000?00
	??0000?000000000000000000000000000000000000000000000000000000000
	?000000000?000000?000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
S_2	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	?000000000?000000?000000000000000000000?000000000000000000000?00

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
I	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
S_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
P_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000?000000000000000000000?00
	??0000?000000000000000000000000000000000000000000000000000000000
	?000000000?000000?000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
S_2	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	?000000000?000000?000000000000000000000?000000000000000000000?00
P_2	??0?00?000?00000??0??0000?00??0000?0?0??00000?000000000000?00?00
	??0?00??00?000?00?000000000000000000?00??0000?000?000000?0?00??0
	????00??00???000???0000?000000000000000??0000?00000000000000??0
	??0000??00??00?0???0?00?000?000000?0000?000000000?000000?0000?00
	?000?00?00?00000??000000?000000000000??0?0000?0000?000000?00?00

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
I	1000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 1000000000000000000000000000000000000000000000000000000000000000 1000000000000000000000000000000000000000000000000000000000000000
S_1	0000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
P_1	0000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000?000000000000000000000?00 ??0000?000000000000000000000000000000000000000000000000000000000000 ?000000000?000000?000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
S_2	??0000?000?000000?000000000000000000000?000000000000000000000?00 ??0000?000?000000?000000000000000000000?000000000000000000000?00 ??0000?000?000000?000000000000000000000?000000000000000000000?00 ??0000?000?000000?000000000000000000000?000000000000000000000?00 ?000000000?000000?000000000000000000000?000000000000000000000?00
P_2	??0?00?000?00000??0??0000?00??0000?0?0??00000?000000000000?00?00 ??0?00??00?000?00?000000000000000000?00??0000?000?000000?0?00??0 ????00??00???000???0000?000000000000000??0000?000000000000000??0 ??0000??00??00?0???0?00?000?000000?0000?000000000?000000?0000?00 ?000?00?00?00000??000000?000000000000??0?0000?0000?000000?00?00
S_3	?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0 ?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0 ?????0??00???0?0???0?00??00?000000?0?0????000??00?0?0000?0?00??0 ?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0 ??0??0??00??00?0?????00???0???0000?0?0????000??00?0?0000?0?00??0

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
I	0000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
S_1	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000?000000000000000000000?00
P_1	??0000?000000000000000000000000000000000000000000000000000000000
	?000000000?000000?0000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
S_2	??0000?000?000000?000000000000000000000?000000000000000000000?00
	??0000?000?000000?000000000000000000000?000000000000000000000?00
	?000000000?000000?000000000000000000000?000000000000000000000?00
	??0?00?000?00000??0??0000?00??0000?0?0??00000?000000000000?00?00
	??0?00??00?000?00?000000000000000000?00??0000?000?000000?0?00??0
P_2	????00??00???000???0000?000000000000000??0000?000000000000000??0
	??0000??00??00?0???0?00?000?000000?0000?000000000?000000?0000?00
	?000?00?00?00000??000000?000000000000??0?0000?0000?000000?00?00
	?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0
	?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0
S_3	?????0??00???0?0???0?00??00?000000?0?0????000??00?0?0000?0?00??0
	?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0
	??0??0??00??00?0?????00???0???0000?0?0????000??00?0?0000?0?00??0
	????????0??0???0????????0
	?????0?????????????????????????0?0???????????0??0????0?0?????0???
P_3	???????????????????????????????00??????????0????0????00?????0???
	?????0??????????????????????????0???????????0???0????0?0?????0???
	?????????0??0?????????????????????????0?????????????0???0?????????

3.5-Round Truncated Differential with prob. 1 [Tez16]

	3.5-Round Truncated Differential for Ascon
I	1000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 1000000000000000000000000000000000000000000000000000000000000000 1000000000000000000000000000000000000000000000000000000000000000
S_1	0000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
P_1	0000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000?0000000000000000000?00 ??0000?000000000000000000000000000000000000000000000000000000000000 ?000000000?000000?000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
S_2	??0000?000?000000?000000000000000000000?000000000000000000000?00 ??0000?000?000000?000000000000000000000?000000000000000000000?00 ??0000?000?000000?000000000000000000000?000000000000000000000?00 ??0000?000?000000?000000000000000000000?000000000000000000000?00 ?000000000?000000?000000000000000000000?000000000000000000000?00
P_2	??0?00?000?00000??0??0000?00??0000?0?0??00000?000000000000?00?00 ??0?00??00?000?00?000000000000000000?00??0000?000?000000?0?00??0 ????00??00???000???0000?000000000000000??0000?000000000000000??0 ??0000??00??00?0???0?00?000?000000?0000?000000000?000000?0000?00 ?000?00?00?00000??000000?000000000000??0?0000?0000?000000?00?00
S_3	?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0 ?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0 ?????0??00???0?0???0?00??00?000000?0?0????000??00?0?0000?0?00??0 ?????0??00???0?0?????00???0???0000?0?0????000??00?0?0000?0?00??0 ??0??0??00??00?0?????00???0???0000?0?0????000??00?0?0000?0?00??0
P_3	????????0?????????????????????????????????????0???0????????0 ?????0?????????????????????????0?0????????????0??0????0?0?????0??? ??????????????????????????????00??????????0????0????00?????0??? ?????0?????????????????????????0??????????0???0????0?0?????0??? ?????????0??0?????????????????????????0????????????0???0??????????
S_4	??0????????? ??0????????? ??0????????? ??0????????? ??0?????????

DryGASCON

DryGASCON

- Designed by *Sebastien Riou*
- 2-round candidate in NIST's LWC standardization process
- Type: Sponge construction
- Primitive: DrySponge and Ascon
  - Block size: 128 bits
  - State size: 320 or 576 bits
  - Key: 128 or 256 bits
  - Nonce: 128 bits
  - Tag: 128 bits
  - Rounds: 11 or 12 (depends on key length)

DryGASCON vs Ascon

DryGASCON vs Ascon

- 5×5 S-box is the same except it is little endian
- 2 rotations are changed in the linear layer
- Each 64-bit word is in bit interleaved representation
- DryGASCON-256 uses 9×9 S-box
- Author shows that 3.5-round truncated differentials of Ascon are not valid for DryGASCON-128

$$
\begin{aligned}
\Sigma_0(x_0) &= x_0 \oplus (x_0 \ggg 19) \oplus (x_0 \ggg 28) \\
\Sigma_1(x_1) &= x_1 \oplus (x_1 \ggg 61) \oplus (x_1 \ggg 38) \\
\Sigma_2(x_2) &= x_2 \oplus (x_2 \ggg 1) \oplus (x_2 \ggg 6) \\
\Sigma_3(x_3) &= x_3 \oplus (x_3 \ggg 10) \oplus (x_3 \ggg 17) \\
\Sigma_4(x_4) &= x_4 \oplus (x_4 \ggg 7) \oplus (x_4 \ggg 40) \\
\Sigma_5(x_5) &= x_5 \oplus (x_5 \ggg 31) \oplus (x_5 \ggg 26) \\
\Sigma_6(x_6) &= x_6 \oplus (x_6 \ggg 53) \oplus (x_6 \ggg 58) \\
\Sigma_7(x_7) &= x_7 \oplus (x_7 \ggg 9) \oplus (x_7 \ggg 46) \\
\Sigma_8(x_8) &= x_8 \oplus (x_8 \ggg 43) \oplus (x_8 \ggg 50)
\end{aligned}
$$

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	10000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
S_1	?000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	1000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
S_1	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
P_1	?0000000000000000?0000000000000000000000000000000000000000?000000000
	1000000000000100000000000000000001000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000
	?0000000000000000000000000?0000000000000000000000000000?00000000
	?00000000000?000000000000000000000000000000000000000000000000?000

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	1000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
S_1	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
P_1	?0000000000000000?0000000000000000000000000000000000000000?000000000
	1000000000000100000000000000000001000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000?000000000000000000000000000?00000000
	?00000000000?0000000000000000000000000000000000000000000000000?000
S_2	?00000000000??0000?00000000?00000?0000000000000000000??0000?000
	?00000000000??0000?00000000?00000?0000000000000000000??0000?000
	?00000000000?1000000000000?00000100000000000000000000?0000?000
	?00000000000?10000?00000000?00000100000000000000000000??0000?000
	?00000000000??0000?00000000?00000?0000000000000000000??0000?000

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	1000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
S_1	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000000000000000000000
P_1	?0000000000000000?0000000000000000000000000000000000000000?000000000
	1000000000001000000000000000001000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000?000000000000000000000000000?00000000
	?00000000000?0000000000000000000000000000000000000000000000?000
S_2	?00000000000??0000?00000000?00000?0000000000000000000??0000?000
	?00000000000??0000?00000000?00000?0000000000000000000??0000?000
	?00000000000?1000000000000?00000100000000000000000000?0000?000
	?00000000000?10000?00000000?00000100000000000000000000??0000?000
	?00000000000??0000?00000000?00000?0000000000000000000??0000?000
P_2	?000?0000000???000??0000?00?00??0???0000??0000?00?0?00??0000?000
	?00?0000?000??0000?00000????00??0?0??0000?000??0000?00??0000?000
	?10000000?10?10000000000??00???000100000000?10000000?00?0??0?01?
	?000000?1000????00?0?0?0010?0000010?10000?0000000??000??0000?000
	?000000?0000??0000???000??0?00?00???0000??000??0000000??0000?000

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	10000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000
S_1	?0000000000000000000000000000000000000000000000000000000000000000000000000000000 10000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 ?0000000000000000000000000000000000000000000000000000000000000000000000000000000 ?0000000000000000000000000000000000000000000000000000000000000000000000000000000
P_1	?000000000000000000?000000000000000000000000000000000000?000000000 10000000000001000000000000000000010000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 ?0000000000000000000000000?000000000000000000000000000?00000000 ?000000000000?000000000000000000000000000000000000000000000?000
S_2	?000000000000??0000?00000000?00000?000000000000000000000??0000?000 ?000000000000??0000?00000000?00000?000000000000000000000??0000?000 ?000000000000?10000000000000?000001000000000000000000000?0000?000 ?000000000000?10000?00000000?000001000000000000000000000??0000?000 ?000000000000??0000?00000000?00000?000000000000000000000??0000?000
P_2	?000?0000000???000??0000?00?00??0???0000??0000?00?0?00??0000?000 ?00?0000?000??0000?00000????00??0?0??0000?000??0000?00??0000?000 ?10000000?10?10000000000??00???000100000000?10000000?00?0??0?01? ?000000?1000????00?0?0?0010?0000010?10000?0000000??000??0000?000 ?000000?0000??0000???000??0?00?00???0000??000??0000000??0000?000
S_3	??0??00????0????00???0??????????0????000??0????00????0??0??0?0?? ??0??00????0????00???0??????????0????000??0????00????0??0??0?0?? ?10?000???10????00???0??????????0????000??0?1??00????0??0??0?01? ?10??00???10????00???0??????????0????000??0?1??00????0??0??0?01? ?00??00??000????00???0?0????00??0????000??000??00???00??0000?000

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	10000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000
S_1	?0000000000000000000000000000000000000000000000000000000000000000000000000000000 10000000000000000000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 ?0000000000000000000000000000000000000000000000000000000000000000000000000000000 ?0000000000000000000000000000000000000000000000000000000000000000000000000000000
P_1	?000000000000000000000000000000000000000000000000000000000000000?000000000 10000000000001000000000000000000010000000000000000000000000000000000 00000000000000000000000000000000000000000000000000000000000000000000000000000000 ?0000000000000000000000000?000000000000000000000000000?000000000 ?000000000000?0000000000000000000000000000000000000000000000000?000
S_2	?000000000000??0000?00000000?00000?0000000000000000000000??0000?000 ?000000000000??0000?00000000?00000?0000000000000000000000??0000?000 ?000000000000?1000000000000?000001000000000000000000000?0000?000 ?000000000000?10000?00000000?000001000000000000000000000??0000?000 ?000000000000??0000?00000000?00000?0000000000000000000000??0000?000
P_2	?000?0000000???000??0000?00?00??0???0000??0000?00?0?00??0000?000 ?00?0000?000??0000?00000????00??0?0??0000?000??0000?00??0000?000 ?10000000?10?10000000000??00???000100000000?10000000?00?0??0?01? ?000000?1000????00?0?0?0010?0000010?10000?0000000??000??0000?000 ?000000?0000??0000???000??0?00?00???0000??000??0000000??0000?000
S_3	??0??00????0????00???0??????????0????000??0????00????0??0??0?0?? ??0??00????0????00???0??????????0????000??0????00????0??0??0?0?? ?10?000???10????00???0??????????0????000??0?1??00????0??0??0?01? ?10??00???10????00???0??????????0????000??0?1??00????0??0??0?01? ?00??00??000????00???0?0????00??0????000??000??00???00??0000?000
P_3	????????????????????????????????????0???????????????0??????? ??0?? ?? ???????????????0?????????????????????1???????????????1??????? ?????????0???????0???0?0????00???????000????0???????????0???????

3.5-Round Truncated Differential with prob. 1

	3.5-Round Truncated Differential for DryGASCON-128
I	1000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
S_1	?000000000000000000000000000000000000000000000000000000000000000 1000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000000000000000000000000000000000000000000
P_1	?0000000000000000?0000000000000000000000000000000?000000000 1000000000001000000000000000001000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 ?000000000000000000000000?000000000000000000000000?00000000 ?0000000000?0000000000000000000000000000000000000000?000
S_2	?0000000000??0000?00000000?00000?0000000000000000000??0000?000 ?0000000000??0000?00000000?00000?0000000000000000000??0000?000 ?0000000000?1000000000000?00000100000000000000000?0000?000 ?0000000000?10000?00000000?00000100000000000000000??0000?000 ?0000000000??0000?00000000?00000?0000000000000000000??0000?000
P_2	?000?0000000???000??0000?00?00??0???0000??0000?00?0?00??0000?000 ?00?0000?000??0000?00000????00?0?0??0000?000??0000?00??0000?000 ?10000000?10?10000000000??00???000100000000?10000000?00?0??0?01? ?000000?1000????00?0?0?0010?0000010?10000?0000000??000??0000?000 ?000000?0000??0000???000??0?00?00???0000??000??0000000??0000?000
S_3	??0??00????0????00???0??????????0????000??0????00????0??0??0?0?? ??0??00????0????00???0??????????0????000??0????00????0??0??0?0?? ?10?000???10????00???0??????????0????000??0?1??00????0??0??0?01? ?10??00???10????00???0??????????0????000??0?1??00????0??0??0?01? ?00??00??000????00???0?0????00??0????000??000??00???00??0000?000
P_3	????????????????????????????????????0???????????????0??????? ??0?? ?? ???????????????0?????????????????????1???????????????1??????? ?????????0???????0???0?0????00??????000????0???????????0???????
S_4	????????????????????????????????????x???????????????y??????? ????????????????????????????????????x???????????????y??????? ????????????????????????????????????x???????????????y??????? ????????????????????????????????????x???????????????y??????? ????????????????????????????????????x???????????????y???????

Shamash

Shamash

- Designed by *Daniel Penazzi* and *Miguel Montes*
- 1-round candidate in NIST's LWC standardization process
- Type: Sponge construction
- Primitive: Ascon
  - Different S-box (5 undisturbed bits)
  - Different rotations at the linear layer
  - Extra matrix multiplication after rotations
  - Another rotation after matrix multiplication
  - Rounds: 9
- We found 1.5-round prob. 1 truncated differentials

Subspace Trails

Subspace Trails [GrassiRR16]

Let $(U_1, U_2, \ldots, U_{r+1})$ denote a set of $r+1$ subspaces with $\dim(U_i) \leqslant \dim(U_{i+1})$. If for each $i = 1, \ldots, r$ and for each a_i, there exists (unique) $a_{i+1} \in U_{i+1}^c$ such that

$$F(U_i \oplus a_i) \subseteq U_{i+1} \oplus a_{i+1},$$

then $(U_1, U_2, \ldots, U_{r+1})$ is a *subspace trail* of length r for the function F.

Subspace Trails

Table: Obtained longest probability one subspace trails both for forward r_e and backward r_d directions and their dimensions d with theoretical upper bounds for Ascon, DryGASCON and Shamash

Cipher	Theoretical/Obtained r_e (d)	Theoretical/Obtained r_d (d)
Ascon	4 (298) / 4 (313)	2 (125) / 2 (309)
DryGASCON-128	4 (293) / 3 (154)	2 (125) / 2 (308)
DryGASCON-256	4 (408) / 4 (558)	2 (217) / 1 (9)
Shamash	2 (45) / 2 (149)	-

(Enhanced) Differential-Linear

(Enhanced) Differential-Linear

- By Langford and Hellman (1994)
- Biham et al. enhanced it by allowing differentials with prob. < 1
- Combines differential with prob. p and linear approx. with bias q
- Overall bias becomes $2pq^2$
- Data complexity is $O(p^{-2}q^{-4})$ CP

Differential-Linear Distinguishers

Ascon

- Designers provided a 4-round differntial-linear key recovery attack combining 2-round differential with probility 2^{-5} and 2-round linear approximation with bias 2^{-8}
- Hence overall bias is $2pq^2 = 2^{-20}$
- We show that same linear approximation can be combined with a 2-round differential with probability 1
- Hence overall bias reduces to $2pq^2 = 2^{-15}$

4-round Differential-Linear Attack on Ascon

	2-Round Truncated Differential for Ascon
I	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000010000000000000000000000000000000000000000000000000000000 0000000010000000000000000000000000000000000000000000000000000000
S_1	000000000?0000000000000000000000000000000000000000000000000000000 000000000?0000000000000000000000000000000000000000000000000000000 000000000?0000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 000000000?0000000000000000000000000000000000000000000000000000000
P_1	000000000?0000000000000000000?0000000?0000000000000000000000000 000000?00?0000000000000000000000000000000000000?0000000000000 000000000??0000?0000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 000000000?000000?0000000000000000000000000000000?0000000000000
S_2	000000?00??0000??0000000000?0000000?000000000?0?0000000000000 000000?00??0000??0000000000?0000000?000000000?0?0000000000000 000000?00??0000??0000000000000000000000000000?0?0000000000000 000000?00??0000??0000000000?0000000?000000000?0?0000000000000 000000?00?000000?0000000000?0000000?000000000?0?0000000000000
P_2	0?0?0??00??0?0???00000000?00??0000??0??0000??00??0?00000?0000000 000?00??0??0??0??000000?0?00?00000?00?0000000?0????000??00000000 000000??0????00???000??0000000000000000000000000????00?0?0000000 0?0?00?00??0000??00??00?0????000??000??000000?0??0?000?000?0?000 00000??00?000??0?000000?0?0??000000?0?000000?00??0?0000?0?000000

Table: 2-round linear approximation for Ascon permutation with bias 2^{-8}

Round	State				
0	.....	.....2.4..	.....2.4.1	.....2.....8.	.....2.....8.
1	.....	.....	.....	1	1
2	9224b6d24b6eda49	.....	.....	.....	.....

Differential-Linear Distinguishers

DryGASCON-128

- We found a 5-round differntial-linear by combining 2-round differential with probility 1 and 3-round linear approximation with bias 2^{-15}
- Hence overall bias is $2pq^2 = 2^{-29}$
- To the best of our knowledge, this is the first 5-round distinguisher for DryGASCON-128

5-round Differential-Linear for DryGASCON-128

	2-Round Truncated Differential for DryGASCON-128
I	0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000001000000000000000000000000000000000000000 0000000000000000000000001000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000
S_1	00000000000000000000000?0000000000000000000000000000000000000000 00000000000000000000000?0000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 00000000000000000000000?0000000000000000000000000000000000000000
P_1	000000000000?000000000000?000000000000000000000?000000000000000 0000000?0000000000000000?0000000000000000000000000000000?0000 0000000000000000000000000000000000000000000000000000000000000000 0000000000000000000000000000000000000000000000000000000000000000 000000?000000000000000000?0000000000000000000000000?000000000
S_2	000000??0000?000000000000?000000000000000000000?00000?0000?0000 000000??0000?000000000000?000000000000000000000?00000?0000?0000 000000??00000000000000000?00000000000000000000000?0000?0000 000000??0000?000000000000?000000000000000000000?00000?0000?0000 000000??0000?000000000000?000000000000000000000?00000?0000?0000
P_2	000000??0000??0000?00000???000?000?00000?0000?00?00000?0000???00 000000??0000?00000???000???00?00000?000??0000?00?00000?0000?0?00 000??0??000000000000??00??000000000??000000000000?00?0??0?0000 0??000???000?0?0000?0?0000?00000000?0000000?0000??0000?0000?0??0 000000??0000??0000??0000?0?0000000??000??0000000?00000?0000??000

Table: 3-round linear approximation for DryGASCON-128 with bias 2^{-15}

Round	State
0	1.....8.21.1.21 ....18. 1.....8.21.11a.
1	....8..1....1 .....8..1....1
2	1
3	..... e37c4f1b6e8d53e6 e.8629e8e4b766af ....

Summary

Summary

1. Provided prob. 1 subspace trails for Ascon, DryGASCON, Shamash
2. Provided 3.5-round prob. 1 truncated diff. for DryGASCON-128
3. Improved 4-round diff.-linear attack on Ascon
4. Provided 5-round diff.-linear distinguisher for DryGASCON-128

Thanks

Thank You for Your Attention