Qualcomm

*disclaimer:
no cryptanalysis here,
just remarkable properties

Some Observations About the Ascon and Keccak S-box and Potential Applications in Cryptanalysis

Nicolas T. Courtois, Frédéric Amiel, Roberto Avanzi, Marco Macchetti, Alexandre Bonnard de Fonvillars, William Whyte
Qualcomm France S.A.R.L. Qualcomm Germany GmbH, Qualcomm Wireless GmbH, Qualcomm Technologies, Inc.

Agenda

We study THREE types of “weakness” in Ascon and Keccak [and symmetric cryptography at large]:

- rotation symmetries and theory of Chi
- an Information Theoretic tool: high DMI ⇔ Weak S-box.
- linearization: LAS-2 and LSS properties:
  Differential-Linear Attacks, Vectorial Non-Linearity,
  super-strong translation symmetries,
  two Theorems for All Quadratic S-boxes

- this work is 98% also avail. as NIST public comments at pp. 13-40:

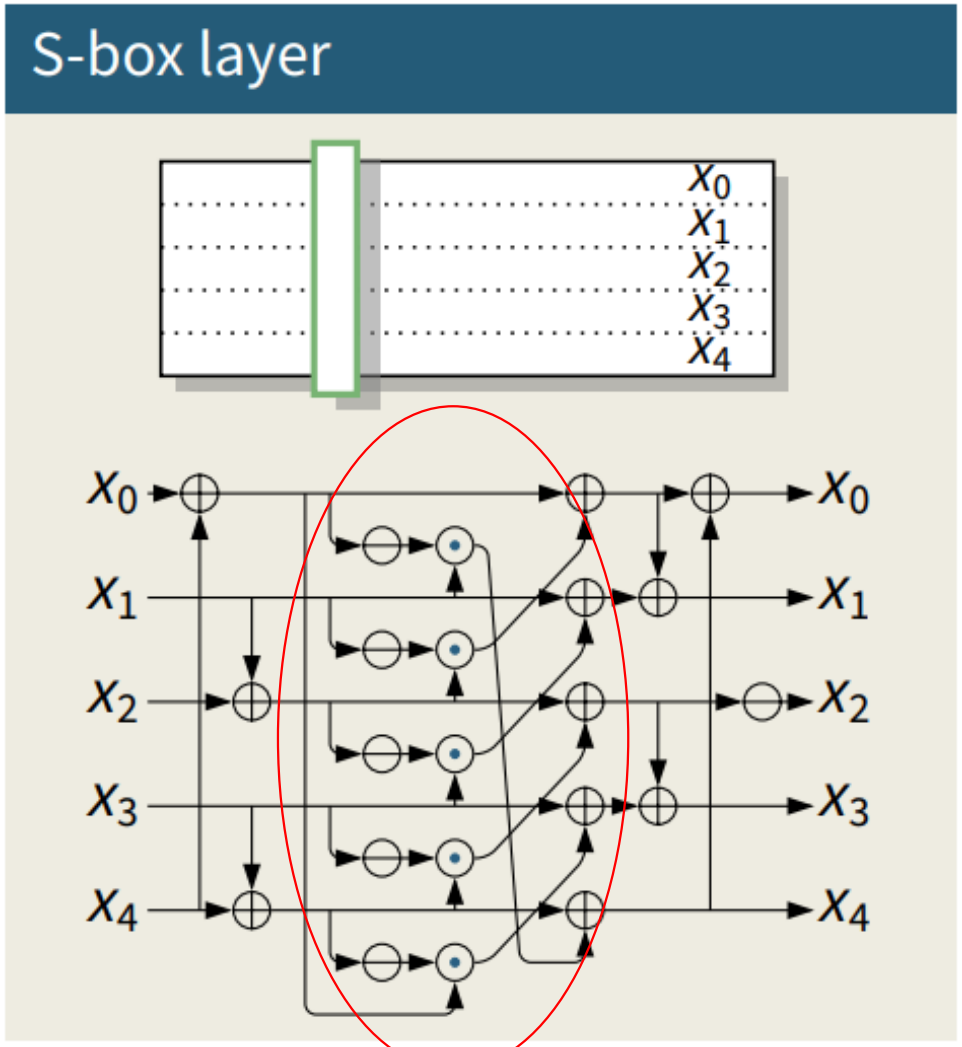
https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

- important resource = eprint.iacr.org/2024/802.pdf

Chi box - Historical Roots - Daemen Thesis 1995

χ = def =

$$b_i = a_i + (a_{i+1} + 1)a_{i+2}$$

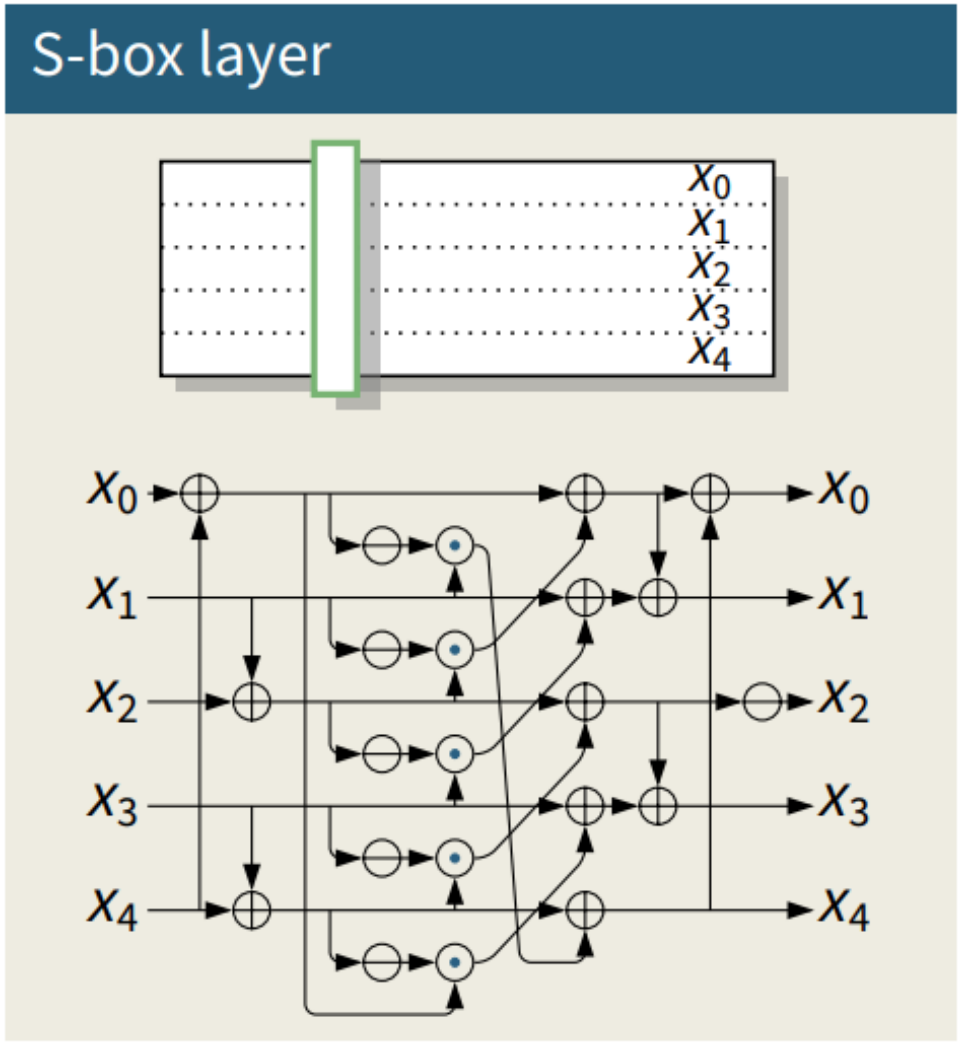


used
in Keccak
Ascon XooDoo
and many other

Rotation Symmetries – Chi S-box χ

cf. our document: https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

χ S-box has subspaces of EXPONENTIAL SIZE where it is FULLY linearized (modelled by 1 single matrix + vector)



class	Ascon input	Keccak Ki	Kx=$Ki \oplus Ko$	Keccak Ko	Ascon output
a	6,13,18,24,27	7,14,19,25,28	1,2,4,8,16	15,23,27,29,30	3,7,9,16,25
b	1,2,8,23,28	3,6,12,17,24	1,2,4,8,16	11,13,21,22,26	11,22,24,27,31
q	9,10,11,22,30	15,23,27,29,30	1,2,4,8,16	7,14,19,25,28	5,8,15,17,18
r	5,7,14,15,25	11,13,21,22,26	5,9,10,18,20	1,2,4,8,16	2,6,12,21,28
s	3,20,21,29,31	5,9,10,18,20	5,9,10,18,20	3,6,12,17,24	0,10,13,20,23
t	4,12,16,17,19	1,2,4,8,16	1,2,4,8,16	5,9,10,18,20	14,19,26,29,30
y	0	0	0	0	4
z	26	31	0	31	1

Table 6. Classification of points at input and output side of Ascon based on the how circular rotations act on the states of the underlying Keccak S-box.

remarkable "stratified" sets size 5 and 10

visible rotation symmetries

*fewer things work at size 6

Intro – “UnDisturbed” Bits

Tezcan 2014:

For a specific input difference of an S-box, some bits of the output difference remain invariant…

single input difference
focus in prior work

Table 2: 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?		

new properties
of arbitrary size and shape

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{bmatrix} 1\,0\,0\,1\,0 \\ 0\,1\,1\,1\,1 \\ 0\,1\,1\,1\,0 \\ 1\,1\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{bmatrix} \cdot \left(x_0, x_1, x_2, x_3, x_4 \right) \oplus \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

B_{11}={5,7,9,10,11,14,15,22,25,26,30}

LSS Dimension = Space Partition + Affine / Linear Models

cf. our document: https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

Fact: Ascon can be modelled by JUST 3 distinct matrices.
LSS-dim = 2.
(all inputs, all outputs, 100% valid)

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 1\,0\,1\,1\,1 \\ 0\,1\,1\,1\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1 \end{bmatrix} \cdot \left(x_0, x_1, x_2, x_3, x_4\right) \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

⇒ we have a plethora of attacks where t

⇒ he 11+11+11+10 (with overlap) => 32 cases total

MAXIMUM STRENGTH POSSIBLE!

LSS Dimension = Space Partition + Affine / Linear Models

cf. our document: https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

Fact: Ascon can be modelled by JUST 3 distinct matrices.
LSS-dim = 2.
(all inputs, all outputs, 100% valid)

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 1\,0\,1\,1\,1 \\ 0\,1\,1\,1\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1 \end{bmatrix} \cdot (x_0, x_1, x_2, x_3, x_4) \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

⇒ we have a plethora of attacks where t

4x LLS property true for some subset x ∈ V

Definition 7 (LSS Affine Dimension). *We call the LSS Affine Dimension of the S-box F, the smallest integer D such that there exist matrices $A_1, \ldots, A_D$ and a constant translation matrix A_0, such that the set of all possible 2^D affine combinations of the form, $A_0 \oplus \sum_i A_i$ corresponds to an LSS property for some set V and union of these sets V is the whole input space.*

Weakness at 5 Bits

cf. our document: https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

Fact: Ascon can be modelled by JUST 3 distinct matrices. LSS-dim = 2. 4th matrix =XOR of 3.
(all inputs, all outputs, 100% valid)

=> we have a plethora of attacks where the space is partitioned in FOUR subsets of size 11+11+11+10 (with overlap).

Fact: AES S-box = just 4 distinct matrices… => 15 linear combinations.

=>these functions are must LESS non-linear than it seems
=>switching between multiple linear approximations
=>simultaneous linear approximations
[no one is studying these anymore?]

ANF deg	class	NL	DMI range	LAS-2 range	LSS range	LSS dim
2	37-52	0	1.96-2.78	104-216	11-13	2
2	35,36	8	2.16	152	13	2
2	53,56-59	8	1.78-2.06	72-104	11	2
2	Ascon,Keccak	8	1.91	80	11	2
2	61-71	8	1.68-2.06	48-120	9-11	2
2	72	8	1.59	40	9	3
2	73	8	1.41	24	8	3
4	Icepole	8	1.81	70	10	3
4	Thakor	8	1.59	45	9	3
4	1-15	10	1.30-1.41	15-25	9-10	3
4	16	10	1.24	10	8	3
4	17	10	1.12	0	9	3
4	Inv-5	10	1.12	0	7	3
2	x^3	12	1.12	0	7	3
2	74/Fides	12	1.12	0	7	3
2	75	12	1.12	0	7	3

Table 1. Results on LSS dimension and closely related parameters for major known permutations on 5 bits.

DDT Connection

cf. our document: https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

Fact: Ascon can be modelled by JUST 3 distinct matrices. LSS-dim = 2. 4th matrix =XOR of 3.
(all inputs, all outputs, 100% valid)

ANF deg	class	NL	DMI range	LAS-2 range	LSS range	LSS dim
2	Ascon,Keccak	8	1.91	80	11	2

=> we have a plethora of attacks where the space is partitioned in FOUR subsets of size 11+11+11+10 (with overlap).

=>

Theorem 4 (Interaction of LSS-11 and DDT Sets). *Let F be the Ascon or Keccak S-box on $k = 5$ bits or an affine equivalent or these boxes. For each LSS-11 set which are always of the form $A_{11} \oplus s$, and any of 20 $DDT(t, u)$ sets of size 8 in existence, where $t \in t^i = \{4, 12, 16, 17, 19\}$, their intersection has exactly 1,2 or 6 points out of 8 and we never observe 0,3,4,5,7,8. For each t, and each (unique) size 6 intersection of one LSS-11 and one DDT-8, these 6 points where LSS and DDT sets intersect are* **exactly** *the 6 defined by:*

$$H_{s,t} = A_{11} \oplus s \ \cap \ A_{11} \oplus t \oplus s.$$

DDT is holographic

DDT = Difference Distribution Table

Theorem 4 (Interaction of LSS-11 and DDT Sets). *Let F be the Ascon or Keccak S-box on $k = 5$ bits or an affine equivalent or these boxes.*
For each LSS-11 set which are always of the form $A_{11} \oplus s$, and any of 20 $DDT(t, u)$ sets of size 8 in existence, where $t \in t^i = \{4, 12, 16, 17, 19\}$, their intersection has exactly 1,2 or 6 points out of 8 and we never observe 0,3,4,5,7,8. For each t, and each (unique) size 6 intersection of one LSS-11 and one DDT-8, these 6 points where LSS and DDT sets intersect are **exactly** *the 6 defined by:*

$$H_{s,t} = A_{11} \oplus s \ \cap \ A_{11} \oplus t \oplus s.$$

- What is NEW? Showing that
- differential DDT and
- linear LSS properties

coincide and are strongly correlated everywhere.

3x MAXIMUM STRENGTH POSSIBLE!

11+11+11+10

Overlap between very different attacks

```
AS = SBox(4,11,31,20,26,21,9,2,27,5,8,18,29,3,6,28,30,19,7,14,0,13,17,24,16,12,1,25,22,10,15,23);#Ascon

print(AS.difference_distribution_table())
```

```
[32  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0]
[ 0  0  0  0  0  0  0  0  0  4  0  4  0  4  0  4  0  0  0  0  0  0  0  0  4  0  4  0  4  0  4  0]
[ 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  4  0  4  0  4  0  4  0  4  0  4  0  4  0  4]
[ 0  4  0  0  0  4  0  0  0  4  0  0  0  4  0  0  0  4  0  0  4  0  0  0  4  0  0  0  4  0  0  0]
[ 0  0  0  0  0  0  8  0  0  0  0  0  0  0  8  0  0  0  0  0  0  0  8  0  0  0  0  0  0  0  8  0]
[ 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  4  0  4  4  0  4  0  4  0  4  0  0  4  0  4]
[ 0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2]
[ 0  0  4  4  0  0  4  4  0  0  4  4  0  0  4  4  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0]
[ 0  0  0  0  0  0  4  4  0  0  0  0  0  0  4  4  0  0  0  0  0  0  4  4  0  0  0  0  0  0  4  4]
[ 0  2  0  2  2  0  2  0  2  0  2  0  0  2  0  2  2  0  2  0  0  2  0  2  0  2  0  2  2  0  2  0]
[ 0  2  2  0  2  0  0  2  0  2  2  0  2  0  0  2  0  2  2  0  2  0  0  2  0  2  2  0  2  0  0  2]
[ 0  0  2  2  0  0  2  2  0  0  2  2  0  0  2  2  0  0  2  2  0  0  2  2  0  0  2  2  0  0  2  2]
[ 0  8  0  0  0  0  0  0  8  0  0  0  0  0  0  0  8  0  0  0  0  0  0  0  8  0  0  0  0  0  0  0]
[ 0  2  0  2  0  2  0  2  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  0  2  0  2  0  2  0  2]
[ 0  4  4  0  4  0  0  4  0  0  0  0  0  0  0  0  0  4  4  0  4  0  0  4  0  0  0  0  0  0  0  0]
[ 0  0  0  0  0  0  0  0  4  4  0  0  4  4  0  0  0  0  0  0  0  0  0  0  4  4  0  0  4  4  0  0]
[ 0  0  0  0  0  0  0  0  0  0  8  0  8  0  0  0  0  0  0  0  0  0  0  0  0  0  8  0  8  0  0  0]
[ 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  8  0  8  0  8  0  8  0  0  0  0  0]
[ 0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2  0  2]
[ 0  0  8  0  8  0  0  0  0  0  8  0  8  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0]
[ 0  0  0  0  4  4  4  4  0  0  0  0  4  4  4  4  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0]
[ 0  0  0  0  0  4  0  4  0  4  0  4  0  0  0  0  0  4  0  4  0  0  0  0  0  0  0  0  0  4  0  4]
[ 0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  0  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2  2]
[ 0  0  4  0  4  0  0  0  0  0  4  0  4  0  0  0  0  0  4  0  4  0  0  0  0  0  4  0  4  0  0  0]
[ 0  0  0  0  2  2  2  2  0  0  0  0  2  2  2  2  0  0  0  0  2  2  2  2  0  0  0  0  2  2  2  2]
[ 0  0  0  4  0  0  4  0  4  0  0  0  0  4  0  0  0  4  0  0  0  0  4  0  0  0  0  0  4  0  0  4]
[ 0  2  2  0  0  2  2  0  2  0  0  2  2  0  0  2  0  2  2  0  0  2  2  0  2  0  0  2  2  0  0  2]
[ 0  0  2  2  2  2  0  0  0  0  2  2  2  2  0  0  0  0  2  2  2  2  0  0  0  0  2  2  2  2  0  0]
[ 0  4  0  4  0  0  0  0  4  0  4  0  0  0  0  0  4  0  4  0  0  0  0  0  4  0  4  0  0  0  0  0]
[ 0  0  0  4  0  4  0  0  4  0  0  0  0  0  4  0  4  0  0  0  0  0  4  0  0  0  0  4  0  4  0  0]
[ 0  0  0  0  0  0  0  0  2  2  2  2  2  2  2  2  0  0  0  0  0  0  0  0  2  2  2  2  2  2  2  2]
[ 0  0  4  4  4  4  0  0  0  0  0  0  0  0  0  0  0  4  4  4  4  0  0  0  0  0  0  0  0  0  0  0]
```

"white box security analysis"
better awareness of basic "linearization" events

Applications and Corollaries = UDB [Tezcan]

space is divided in 4 sets 11+11+11+10

Related Work. All the $\delta_{in} \in t^i$ for which we obtain size 6, have the "undisturbed bits" UDB property extensively studied by Tezcan in multiple papers for Ascon [TeAs16,TeDi19] which is also related to the older concept of "linear structures" [MaTe14].

=>

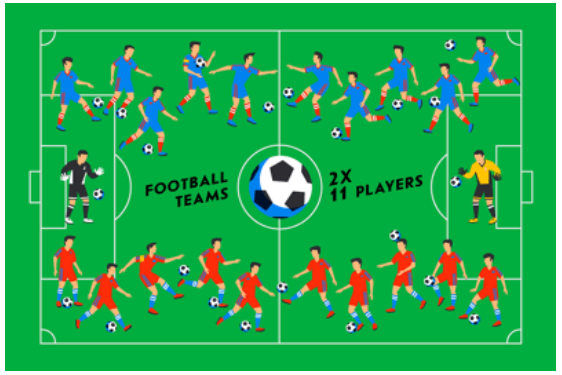
4th reason why this is MAXIMUM STRENGTH POSSIBLE!

Applications in Cryptanalysis. Our Thm. 4 opens avenues of research in advanced combined differential and linear cryptanalysis. It says basically that linear and differential properties of maximum strength, which are in fact those which might interest the attacker, are strongly correlated to each other. In older

More Observations

space is divided in 4 sets

=>



*same stratified sets 6*5 with super strong rotation symmetries

Observations on Self Similarity of A_{11}. We found that:

1. The intersection of A_{11} with another variant $A_{11} \oplus x$ is always not empty except for $B_{11} = A_{11} \oplus 0x1A$, when $x = 26 = 0x1A$.
2. The intersection of A_{11} with another variant $A_{11} \oplus x$ is of maximum size 6 in exactly 5 cases where $x \in \{4, 12, 16, 17, 19\}$ which set is sometimes called t, cf. Table 6 which are exactly five of those lines δ_{in} in the DDT of Ascon/Keccak S-box which contain 8, and which are therefore exactly all the input differentials in Ascon of maximum strength 8/32. These 5 δ_{in} also amount to half of 10 well-known "undisturbed bits" UDB properties in [TeAs16,TeDi19]. The relevant DDT sets of size 8 are also studied in Thm. 4.
3. The intersection of A_{11} with another variant $A_{11} \oplus x$ is of size 4 when $x \in \{1, 2, 3, 5, 7, 8, 14, 15, 20, 21, 23, 25, 28, 29, 31\}$ which set was sometimes studied as a union of 3 sets: $s \cup r \cup b$ cf. Table 6 and which 15 values are **exactly** those lines in DDT table which contain any 4 numbers.
4. The intersection of A_{11} with another variant $A_{11} \oplus x$ is of size 2 when $x \in \{6, 9, 10, 11, 13, 18, 22, 24, 27, 30\}$ which set is a.k.a. $q \cup a$ which 10 values are **exactly** those lines in DDT table except for the special case of $x = 26 = 0x1A$ already used in B_{11}.

Hyper-planes = another method to LINEARIZE any S-box

cf. our document: https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

Key Question: Is it possible that an S-box sends a "large" subset of some (maximum size) affine space of dim 4 at the input side, to a "large" subset of another affine space of dim 4 at the output side?

Super strong symmetries.

For example in one case out of 961 with $\alpha = 20$ and $\beta = 11$ we have:

$$
\begin{aligned}
S^{-1}[L^o] \cap L^i &= 0,3,20,21,29,31 &\mapsto\ & 0,4,10,13,20,23 \\
S^{-1}[L^o] \cap co - L^i &= 4,6,12,13,16,17,18,19,24,27 &\mapsto\ & 3,7,9,14,16,19,25,26,29,30 \\
co - S^{-1}[L^o] \cap L^i &= 1,2,8,9,10,11,22,23,28,30 &\mapsto\ & 5,8,11,15,17,18,22,24,27,31 \\
co - S^{-1}[L^o] \cap co - L^i &= 5,7,14,15,25,26 &\mapsto\ & 1,2,6,12,21,28
\end{aligned}
$$

*same stratified sets …

UNEXPECTED TRANSLATIONS

Always Weak

Key Question: Is it possible that an S-box sends a "large" subset of some (maximum size) affine space of dim 4 at the input side, to a "large" subset of another affine space…

For example in one case out of 961 with $\alpha = 20$ and $\beta = 11$ we have:

$$
\begin{aligned}
S^{-1}[L^o] \cap L^i &= 0,3,20,21,29,31 &\mapsto\ & 0,4,10,13,20,23 \\
S^{-1}[L^o] \cap co - L^i &= 4,6,12,13,16,17,18,19,24,27 &\mapsto\ & 3,7,9,14,16,19,25,26,29,30 \\
co - S^{-1}[L^o] \cap L^i &= 1,2,8,9,10,11,22,23,28,30 &\mapsto\ & 5,8,11,15,17,18,22,24,27,31 \\
co - S^{-1}[L^o] \cap co - L^i &= 5,7,14,15,25,26 &\mapsto\ & 1,2,6,12,21,28
\end{aligned}
$$

UNEXPECTED TRANSLATIONS

50% of time

100% of those which "might" interest the attacker

all	8+8	6+10	4+12	0+16
961	585	336	40	0
WNT inp-shifted	240	**336**	**40**	0
unrelated	345	0	0	0

Table 3. Pairs spaces of the same size which are equivalent by translation with Ascon.

Always vs. Never

Key Question: Is it possible that an S-box sends a "large" subset …

For example in one case out of 961 with $\alpha = 20$ and $\beta = 11$ we have:

$$
\begin{aligned}
S^{-1}[L^o] \cap L^i &= 0,3,20,21,29,31 \mapsto 0,4,10,13,20,23 \\
S^{-1}[L^o] \cap co - L^i &= 4,6,12,13,16,17,18,19,24,27 \mapsto 3,7,9,14,16,19,25,26,29,30 \\
co - S^{-1}[L^o] \cap L^i &= 1,2,8,9,10,11,22,23,28,30 \mapsto 5,8,11,15,17,18,22,24,27,31 \\
co - S^{-1}[L^o] \cap co - L^i &= 5,7,14,15,25,26 \mapsto 1,2,6,12,21,28
\end{aligned}
$$

Ascon/Keccak

50% of time

all	8+8	6+10	4+12	0+16
961	585	336	40	0
WNT inp-shifted	240	**336**	**40**	0
unrelated	345	0	0	0

Table 3. Pairs spaces of the same size which are equivalent by translation with Ascon.

RP

0% of time

Thakor	8+8	7+9	6+10	5+11	4+12	0+16
961	270	420	196	60	15	0
WNT inp-shifted	**0**	**0**	**0**	**0**	**0**	**0**
unrelated	270	420	196	60	15	0

Table 5. Pairs spaces of the same size equivalent by translation with Thakor S-box.

+ Duplication = Thm. 1.

Key Question: Is it possible that an S-box sends a "large" subset of some (maximum size) affine space …

Theorem 1. *We assume that if we translate the 1st set* $S^{-1}[L^o] \cap L^i$ *by a constant* C *we get the last set* $co - S^{-1}[L^o] \cap co - L^i$*, then the two remaining sets on the other diagonal are also related by translation with the same constant* C*.*

TWICE
UNEXPECTED
TRANSLATIONS

Qualcomm Technologies brought you foundational communications technologies.

Can information theory help cryptographers to design better ciphers?

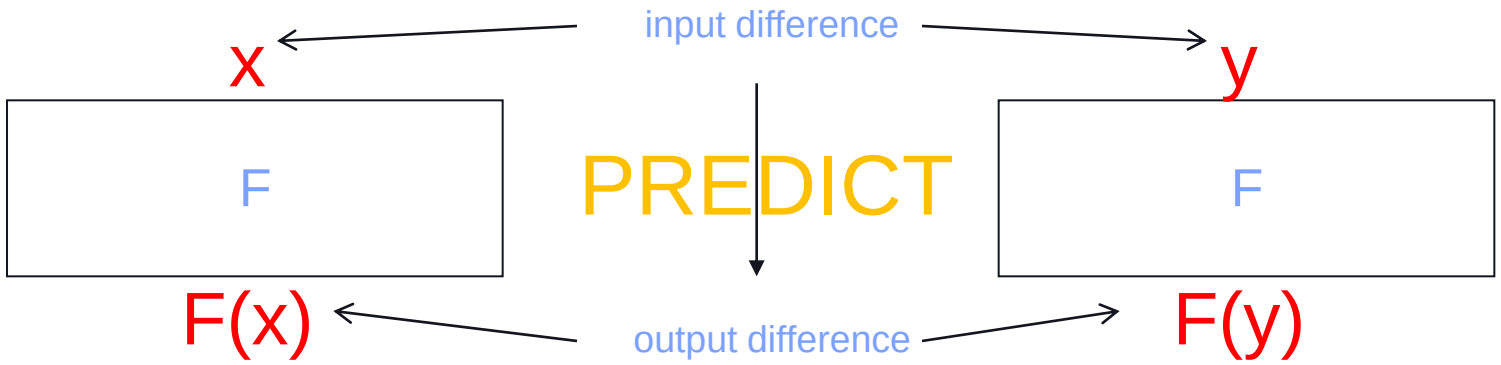
Important Tool:
Mutual Information

DMI

Differential
Prediction

Agenda

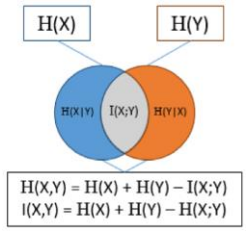
Study of Conditional Entropy and MI



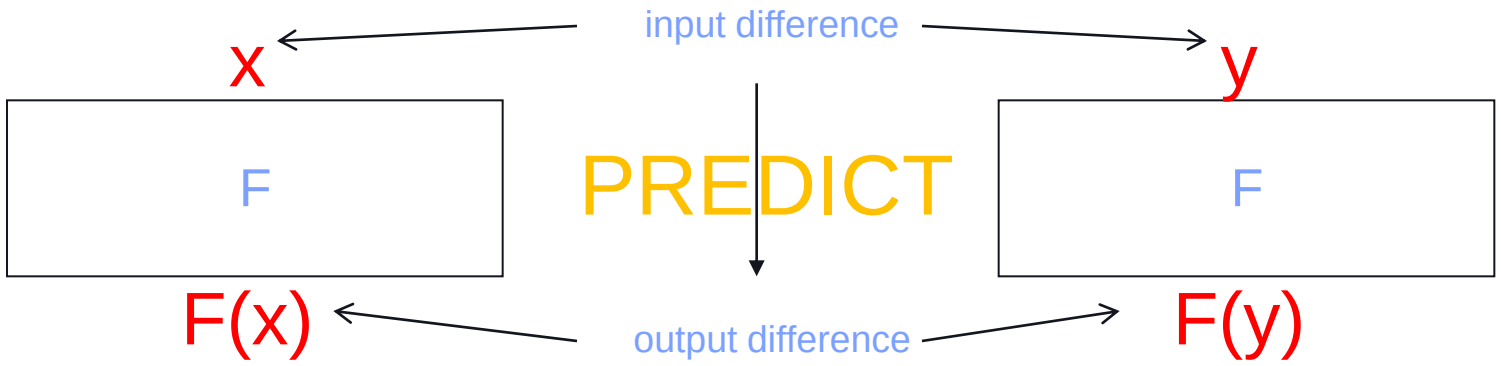
Ĥ G y G ỳ y ỳ ← should be large

Prediction ability <=> Mutual Information = MI =

ŇÍ G y G ỳ y ỳ ← should be small



Prediction approach based on MI = Mutual Information



Entropy:

DMI = Differential Mutual Information

for 5 bits we get:

Fides x^{-1} APN	RP	Ascon/ Keccak
3.875	3.5	4.10
1.125	1.5	1.90

2x bad

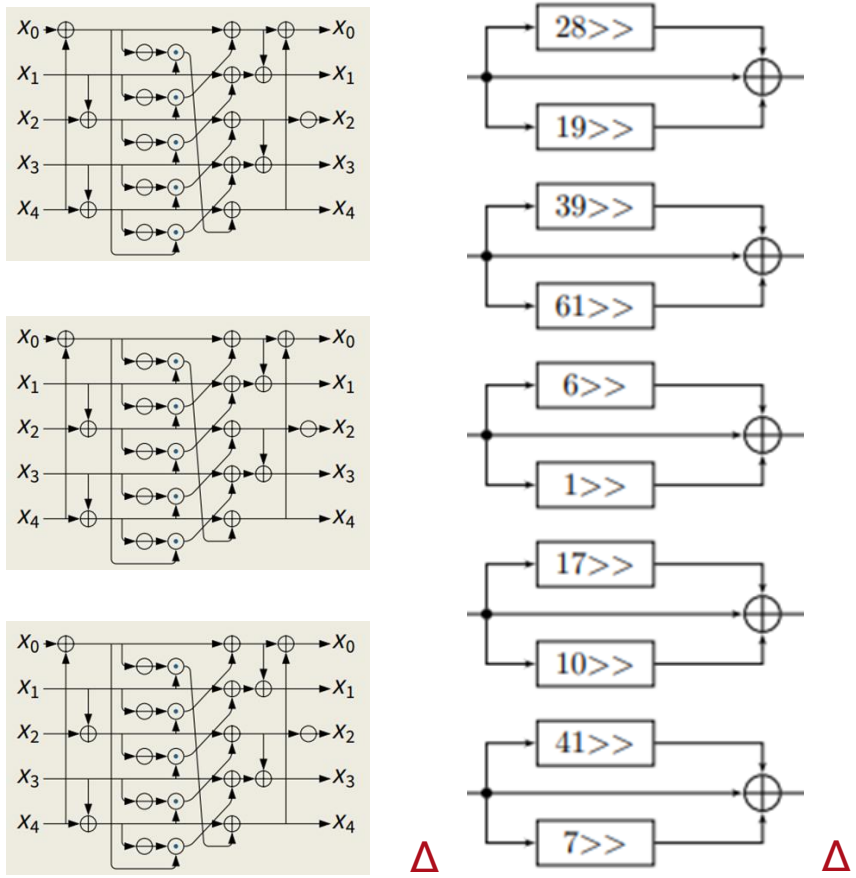
*RP=Random Permutation

Ascon S-box is Semi-Transparent!

- 6,8,12 rounds like this:

122 bits total

would be only 42 bits total if we used the AES S-box



Information-theoretic undeniable information leakage

1.1 for APN
1.5 for RP
1.9 for Ascon
DMI

=max= totally transparent MI

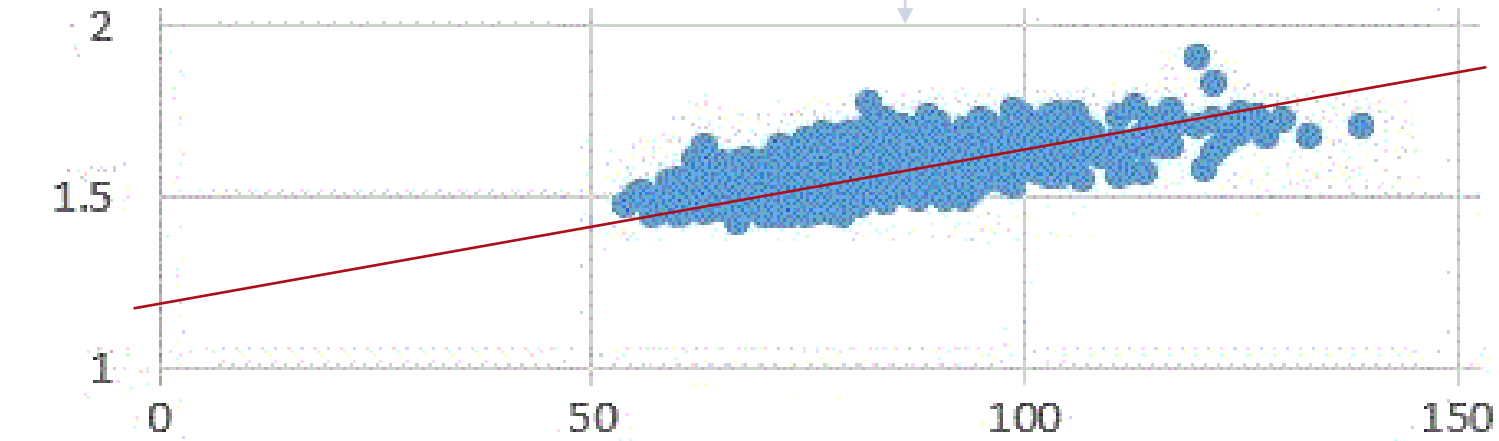
High DMI => always leads to

Partial Linearization properties on 4 points

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 1\,0\,1\,1\,1 \\ 0\,1\,1\,1\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1 \end{bmatrix} \cdot (x_0, x_1, x_2, x_3, x_4) \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

*for some subset $x \in V$

DMI and LAS-2 for 5-bit S-boxes



DMI is 2x bigger =>

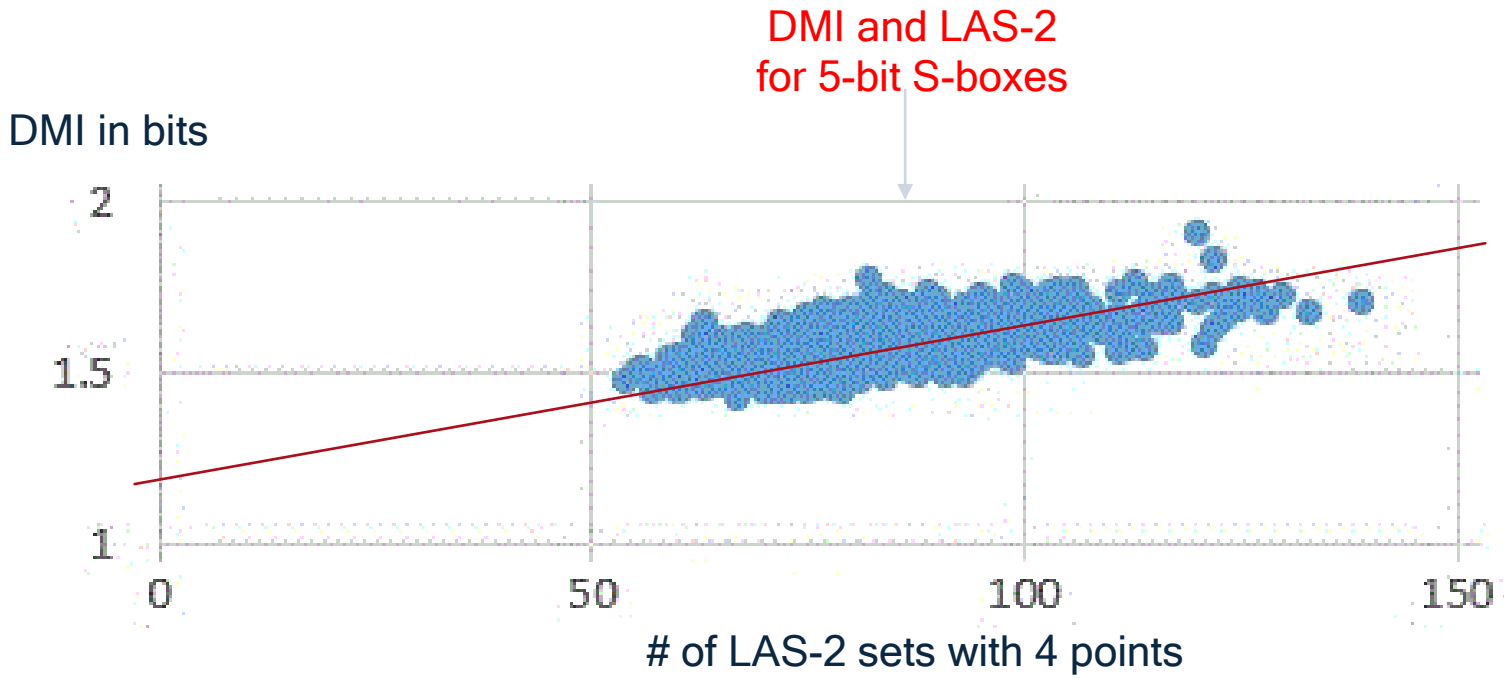
the amount of information the attacker "already knows" doubles!!

	APN AES-like, Fides	RP typical	Ascon/ Keccak
DMI	1.125	1.55	1.90
LAS-2	0	60	80 Eurocrypt 2017 LAS

eprint.iacr.org/2024/802.pdf

2x bad

High DMI => More LAS-2



2x bad

	APN AES-like, Fides	RP typical	Ascon/ Keccak
DMI	1.125	1.55	1.90
LAS-2	0	60	80 Eurocrypt 2017 LAS

eprint.iacr.org/2024/802.pdf

Related Work

Tezcan 2014:

Undisturbed Bits (UDB)

For a specific input difference of an S-box, some bits of the output difference remain invariant…

Table 2: 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?		

DMI = A Measure of "Average Quality" in this table

Agenda

How high MI implies

“Undesirable Properties”

or does it?

*NIST Workshop 2023 – Affine Space Mappings in DES

DMI =

a PRECISE and RELIABLE

measure of quality of ciphers!

Δ

MI

Δ

Table 9. Selected best 16 mappings of affine spaces U of dimension 2 which can be mapped to an affine space W of dimension 2, classified by input linear spaces, we report how many times $K = 0, \ldots 10$ they are re-used in distinct affine spaces.

1.71 2.11 1.67 bits

		DES S-box										s^5DES S-box										S∗DES S-box									
$U1$	$U2$	1	2	3	4	5	6	7	8	$U1$	$U2$	1	2	3	4	5	6	7	8	$U1$	$U2$	1	2	3	4	5	6	7	8
1	4	1	3	–	–	1	–	7	–	1	2	2	4	**8**	6	2	4	2	2	1	2	–	–	–	–	3	2	1	2
1	8	1	2	5	4	3	5	5	2	1	4	4	2	4	4	6	6	2	4	1	4	1	3	–	2	–	–	1	–
1	C	1	1	–	–	2	–	5	3	1	8	5	4	5	3	4	3	6	2	1	6	1	1	2	3	2	1	–	2
1	E	5	1	1	4	1	1	–	–	2	4	6	4	6	6	**8**	4	4	4	1	8	3	3	3	3	4	4	–	3
2	4	4	7	3	4	–	4	4	6	2	5	4	**8**	**8**	**10**	2	**10**	4	**8**	2	4	6	5	5	3	3	4	**8**	6
2	8	–	2	3	4	–	1	–	–	2	8	5	2	2	1	5	3	2	3	2	5	–	1	1	–	1	2	1	3
3	4	1	3	2	4	1	1	2	–	3	4	4	4	6	2	4	4	6	2	2	C	2	–	2	3	1	2	1	2
3	5	–	–	4	–	1	2	2	1	3	5	2	2	6	2	6	**8**	2	6	3	5	1	2	2	1	2	1	–	3
3	8	1	1	1	4	1	1	1	1	3	8	4	3	6	3	3	1	4	4	3	8	1	3	3	1	–	–	2	–
3	C	3	–	2	4	1	2	2	–	4	8	4	4	1	3	5	3	2	3	3	D	1	2	3	4	2	2	3	1
3	D	–	2	5	4	1	3	1	3	5	8	5	3	2	4	3	4	4	6	4	8	3	1	–	–	3	1	–	2
4	A	4	3	1	–	2	1	1	1	5	A	2	3	4	5	1	2	3	6	4	A	3	2	–	1	1	3	–	–
5	A	3	2	–	–	2	–	2	1	7	8	4	7	4	3	4	7	**8**	2	4	B	1	–	3	4	2	–	–	2
5	B	2	4	3	4	2	4	2	4	7	9	1	4	5	–	3	4	3	3	5	A	1	1	1	3	4	3	2	3
6	B	3	1	1	4	3	–	1	2	7	A	–	7	6	3	1	6	2	4	5	B	1	2	4	4	4	2	3	2
7	B	3	2	–	4	2	2	3	2	7	B	3	4	5	–	2	5	5	1	7	B	3	2	4	–	–	2	–	1
total		255								total		505								total		236							

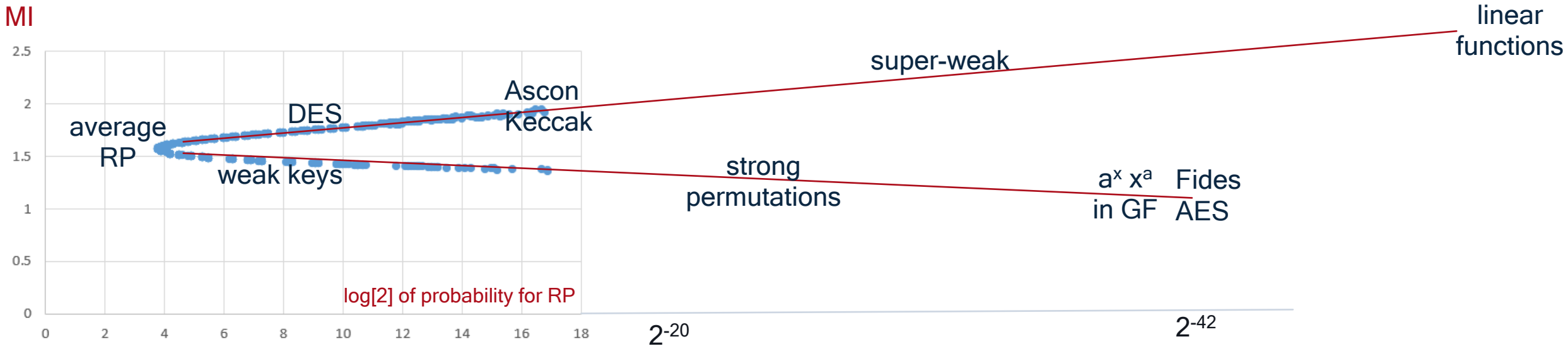
*note: the more repetition, like 8 or 10, the more we approach the concept of “space trails”

Example:
Compare 3 versions of DES on
DMI and LAT-2 mappings.

DMI = prediction of
# of LAS-2 forbidden mappings

Random Permutations, APN and Ascon S-box

A new way of classifying S-boxes from strong to weak on a 2D scale.



CLAIM: we need to contemplate the large distance which separates the Ascon S-box (MI=1.91) and an ideal S-box not in terms of differential and linear properties (the distance seems small) but in terms of:

- How hard it is for a RP to move to this area – close to impossible!
- The combinatorial explosion of undesirable properties [previous slide].

Agenda

*Some Thoughts on Cryptanalysis of Ascon

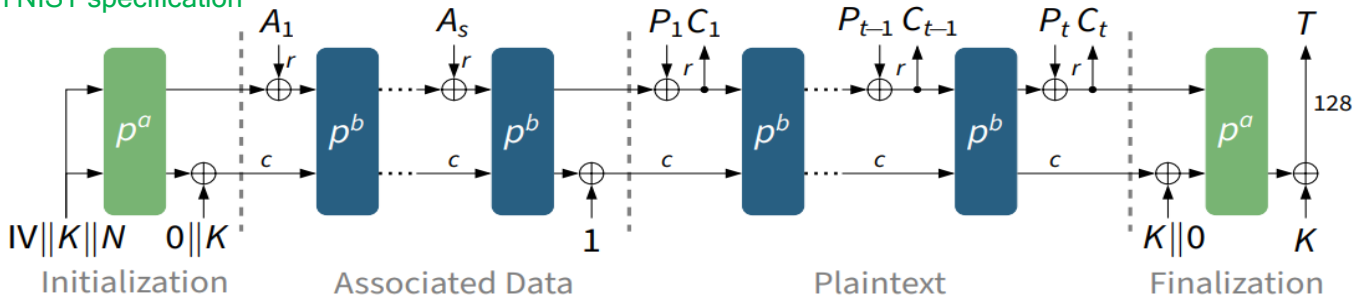
Ascon Cryptanalysis Agenda

- We claim that there exists a ROBUST transparent way for evaluating a security of a cipher seen as a communications channel trying to maximize the “channel capacity”.

- Methodology:
  - showing how attacks can be modelled as a union of small scale “combinatorial events”

(which exist in small finite numbers because the S-box is tiny)

Ascon NIST specification



eprint.iacr.org 2016/490

Table 10: Summary of attacks on ASCON.

Type	Rounds	Time	Method
Key Recovery	6/12	2^{66}	Cube-like
Key Recovery	5/12	2^{35}	Cube-like
Key Recovery	5/12	2^{36}	Differential-Linear
Key Recovery	5/12	2^{58} or $2^{127.99}$	Truncated/Improbable
Key Recovery	4/12	2^{18}	Differential-Linear
Key Recovery	4/12	3^{48}	Truncated/Impossible
Forgery	4/12	2^{101}	Differential
Forgery	3/12	2^{33}	Differential

Modelling Ascon as a Communications Channel

For 9 years Ascon was studied and seems very secure. All because of “strong diffusion”.
Any simple perturbation expand very quickly.
Game over = no hope to attack Ascon???

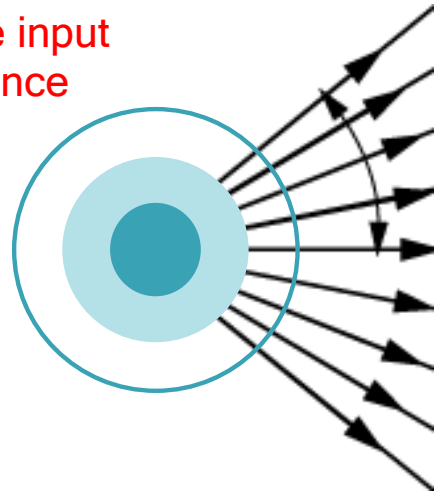
It should be critical to consider attacks that AGGREGRATE input perturbations.

[Tezcan 2014]

Table 2: 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?		

simple input difference

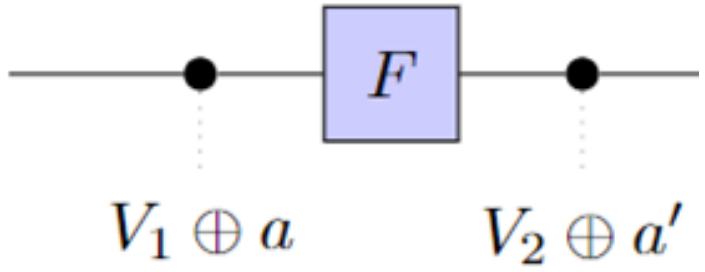


"diffusion cone"

nb. of active bits at output!

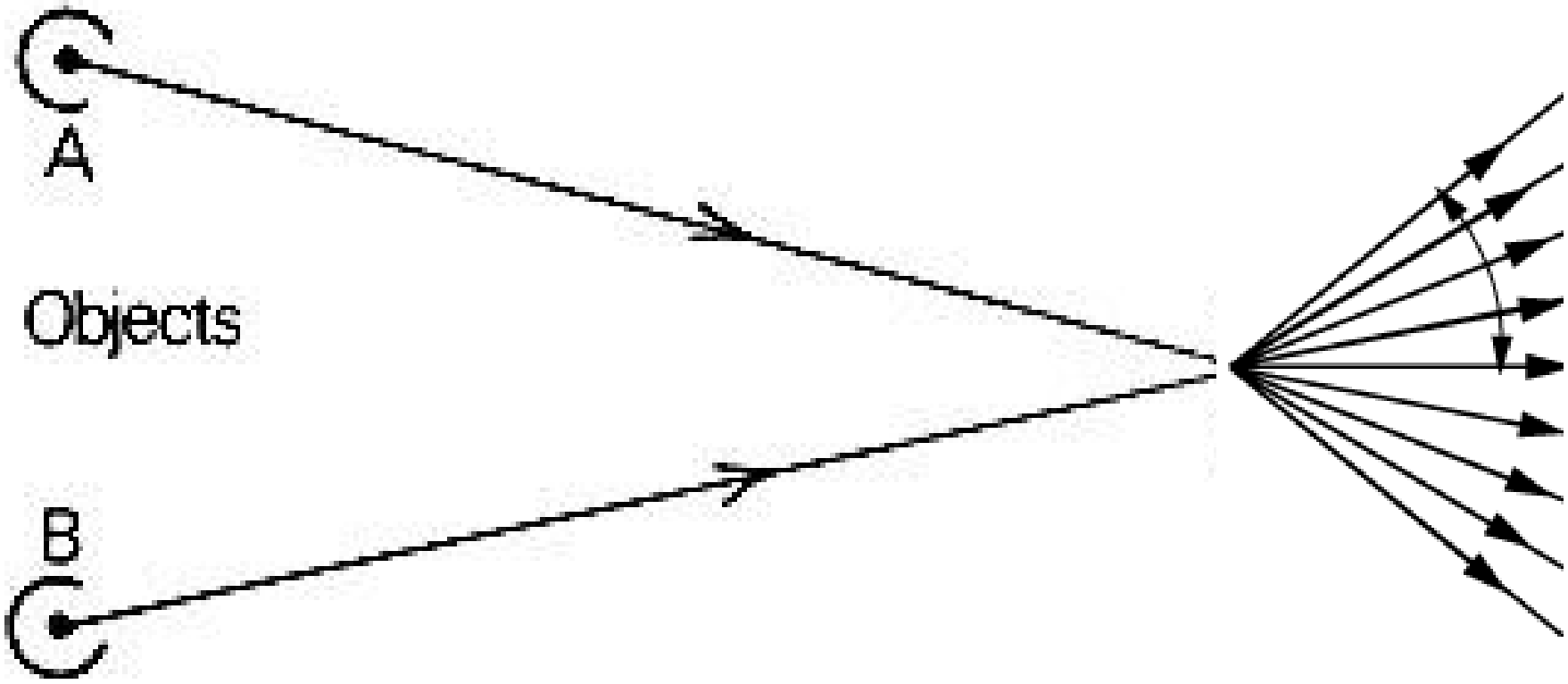
Cipher	r_e	d
ASCON [Dob+16]	3	298
GIFT [Ban+17]	3	60
KECCAK [Ber+11]	2	546
PRESENT [Bog+07]	3	43
PRIDE [Alb+14]	2	31
QARMA [Ava17]*	2	36

Grassi, Rechberger and Rønjom, 2016,
Subspace Trail Cryptanalysis



Philosophy : Aggregate Perturbations

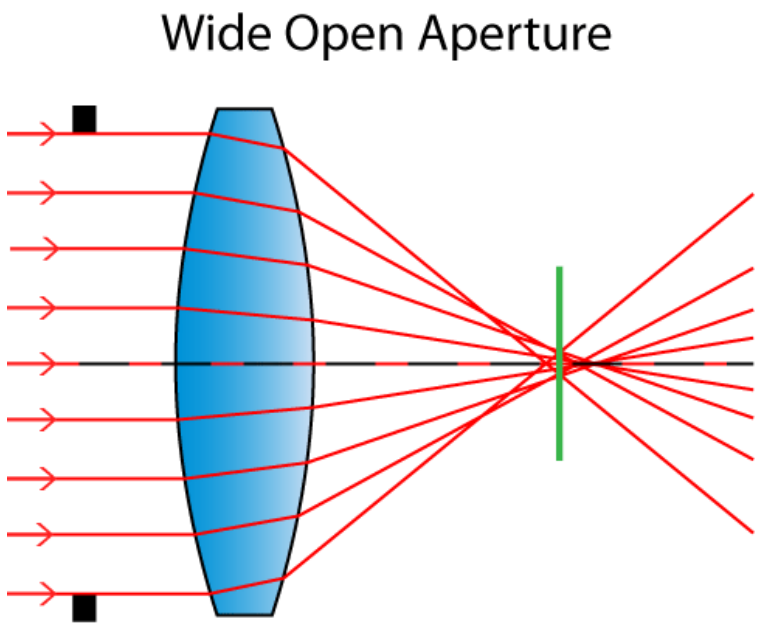
- Can several perturbations converge somewhat? Attacker does either A or B.
- We need to improve the “channel capacity” to increase information conveyed or the likelihood of detection.

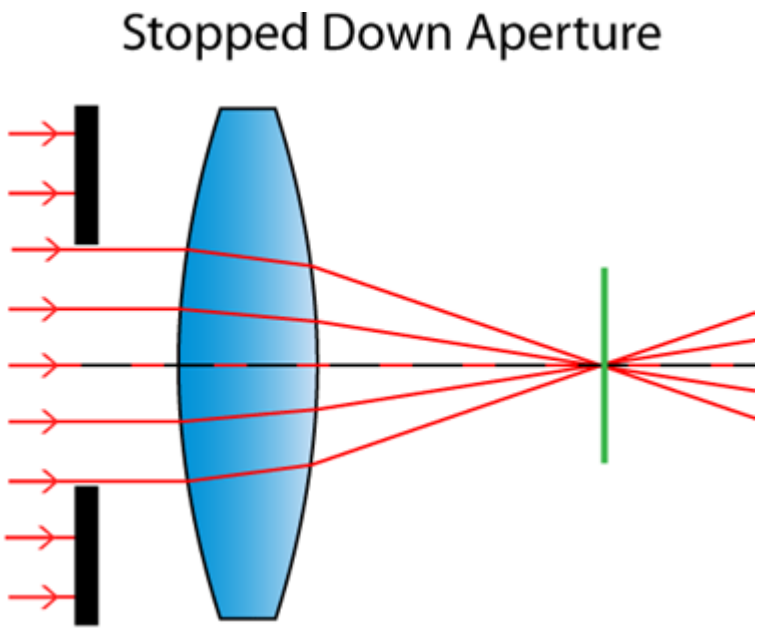


A Known Problem – Analogy with Optics

Not if we have TOO many sources!

Must restrict the input diversity.





a better transmission channel!

Ascon S-Box - Proof of Concept

best =

Ent(oD) = 2.00 bits when x-y=4

Ent(oD) = 2.00 bits when x-y=12

Ent(oD) = 2.00 bits when x-y=16

Ent(oD) = 2.00 bits when x-y=17

av. Output Δ Ent = 2.00 bits

single differences
vs.
quadruple differences

we compute the entropy for the output difference

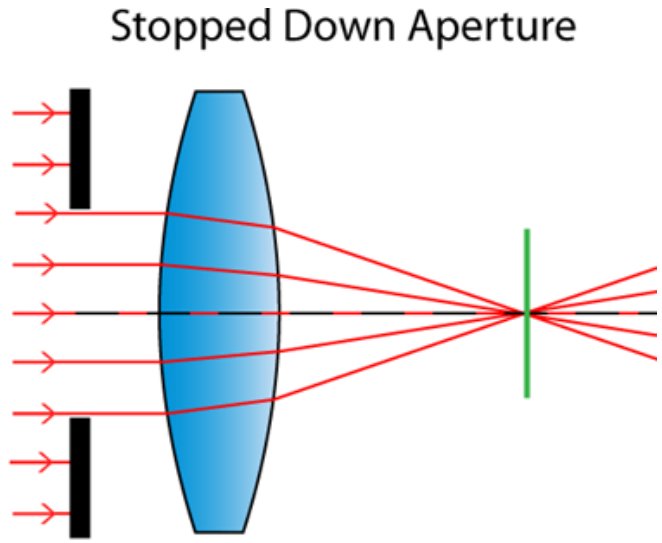
Ent(oD) = 3.69 bits when x-y \in {1,3,16,18}

Ent(oD) = 3.69 bits when x-y \in {4,8,20,24}

Ent(oD) = 3.66 bits when x-y \in {5,16,17,21}

We gain something:

av. Output Δ Ent = only 3.69 bits
instead of 4 bits



Executive Summary:

Many cryptanalytics attacks can be MAPPED to combinations of discrete combinatorial events which are pure information theoretic events:

=>union of small scale undesirable local linearity properties.

We claim that Ascon/Keccak are unnecessarily weak:

1. Low DMI. Many tiny S-boxes are somewhat inherently weak: like 42 => 122 bits of Mutual Information
2. Rotation Symmetries
3. Quadratic S-boxes => Several holographic properties

Open problem: is there a better S-box?

- lower HW cost and low depth (possibly avoiding any XORs which are slow).
- is easy to protect against SCA…
- has a much lower DMI… and has zero or “near zero” of undesirable linear mappings.
- has higher LSS dimension>2 leading to much greater fragmentation and less alignment [Thm 4.] in linear approximations compared DDT and Tezcan Undisturbed Bit properties.

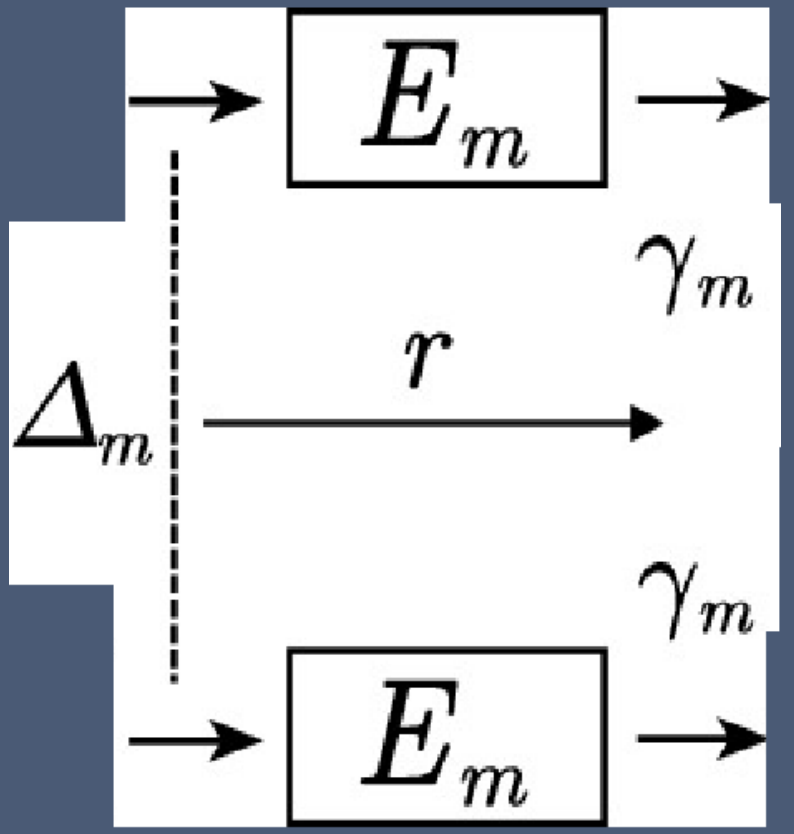
Agenda

More/ Stronger Linearization

Motivation: key concept in Differential-Linear Attacks:

-connectors / connectivity tables

Induction: produce linear relations at 2 outputs

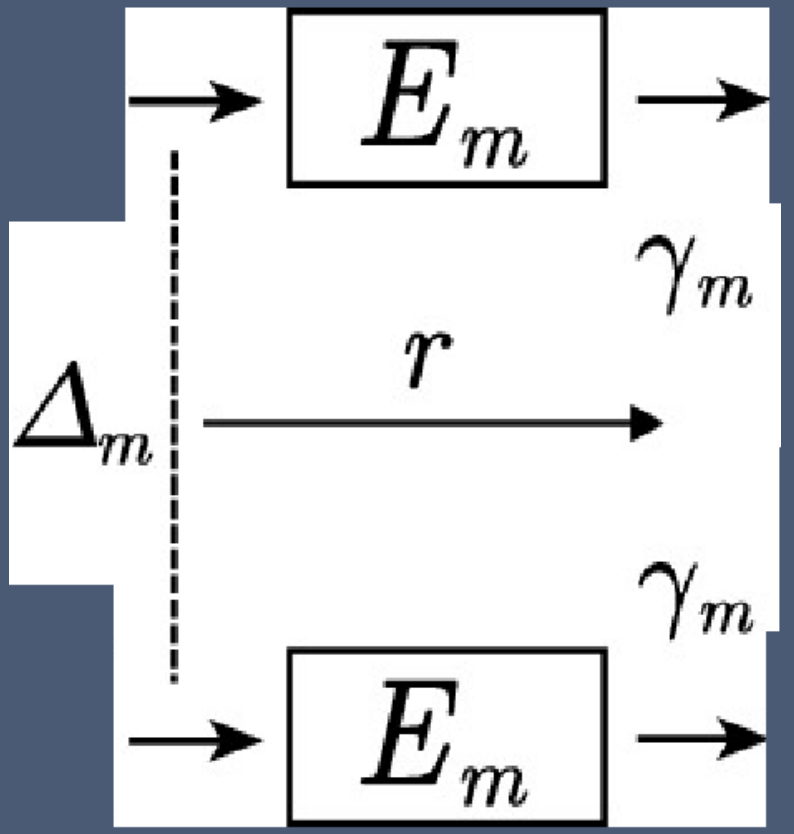


5G

Motivation: key concept in Differential-Linear Attacks:

-connectors / connectivity tables

Induction: produce linear relations at 2 outputs constrained by a set of states



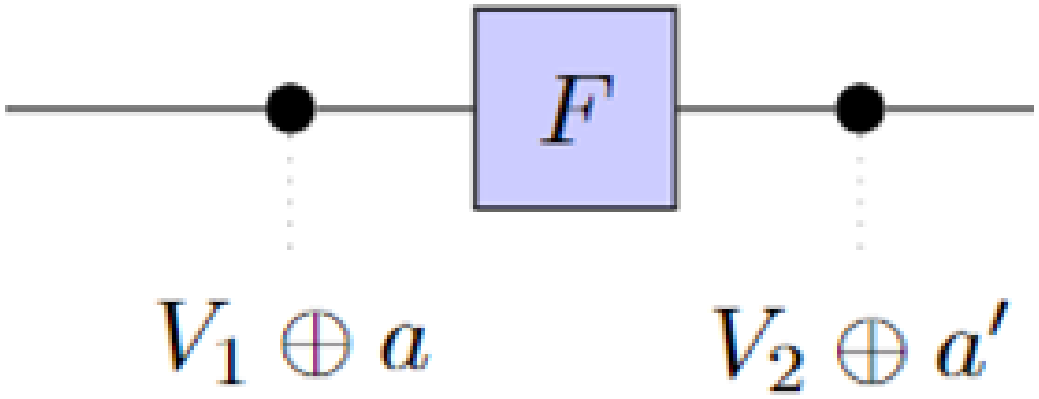
⇒ affine spaces V are NOT required
⇒ purely "combinatorial" properties
⇒ WANTED: affine approximations of the WHOLE S-box

5G

Background

[Grassi, Rechberger and Rønjom, 2016]

Subspace Trail Cryptanalysis



Eurocrypt 2017=2017/128

[16]= Qiao, K., Song, L., Liu, M., Guo, J.:
New collision attacks on round-reduced Keccak, Eurocrypt 2017

def:

LAS = Linearizable Affine Subspaces

Definition 1 *(Linearizable affine subspace [16]). Linearizable affine subspaces are affine input subspaces on which S-box substitution can be re-written as a linear transformation. If V denotes a linearizable affine subspace of an S-box operation $S(\cdot)$, $\forall x \in V, S(x) = A \cdot x + b$ where A is a matrix and b is a constant vector.*

$$y = \begin{pmatrix} 1&0&0&0&1 \\ 0&0&1&0&0 \\ 1&0&0&0&0 \\ 1&0&0&1&1 \\ 1&1&0&0&0 \end{pmatrix} \cdot x + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{9}$$

MAXIMUM LAS
SIZE
POSSIBLE
in Ascon/Keccak
= 4 points

?CANNOT IMPROVE?

New definition

eprint.iacr.org/2024/802

def:

LSS = Linearizable Sub - Sets

Definition 4 (LSS = Linearizable Sub Set). *Let S be an S-box on k bits. We call LSS or Linearizable Sub Set any set of points V such that*

$$S[x] = A \cdot x + c \quad \forall x \in V.$$

MAXIMUM LSS SIZE POSSIBLE in Ascon/Keccak = 11 points

huge improvement from 4 points

Example: A_{11}={0,3,4,12,16,17,19,20,21,29,31}

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 1\,0\,1\,1\,1 \\ 0\,1\,1\,1\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1 \end{bmatrix} \cdot \left(x_0, x_1, x_2, x_3, x_4 \right) \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

eprint.iacr.org/2024/802.pdf

For example with input $4 = 00100 = x0x1x2x3x4$ we get output $26 = 11010 = y0y1y2y3y4$ in binary where $x4/y4$ represent the least significant bit.

Agenda

Cloning = Super Strong Translation Properties of Quadratic S-boxes

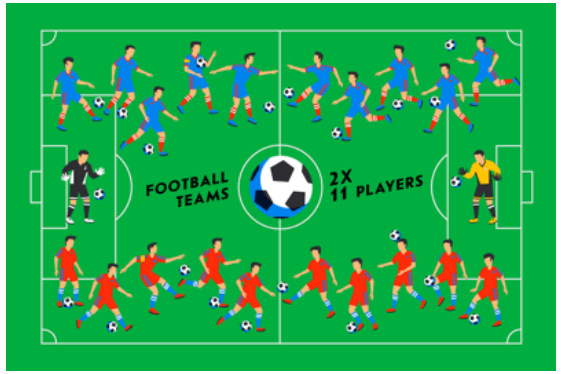
Holographic Property - Cloning Our Team of 11

EASY TRANSFER:

by translation with a constant!

$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{bmatrix} 1\,0\,1\,1\,0 \\ 1\,0\,1\,1\,1 \\ 0\,1\,1\,1\,1 \\ 1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1 \end{bmatrix} \cdot (x_0, x_1, x_2, x_3, x_4) \oplus \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

A_{11}={0,3,4,12,16,17,19,20,21,29,31}



$$\begin{pmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{bmatrix} 0\,1\,0\,1\,1 \\ 1\,1\,1\,0\,1 \\ 0\,1\,1\,1\,0 \\ 0\,1\,1\,1\,1 \\ 1\,0\,0\,1\,0 \end{bmatrix} \cdot (x_0, x_1, x_2, x_3, x_4) \oplus \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

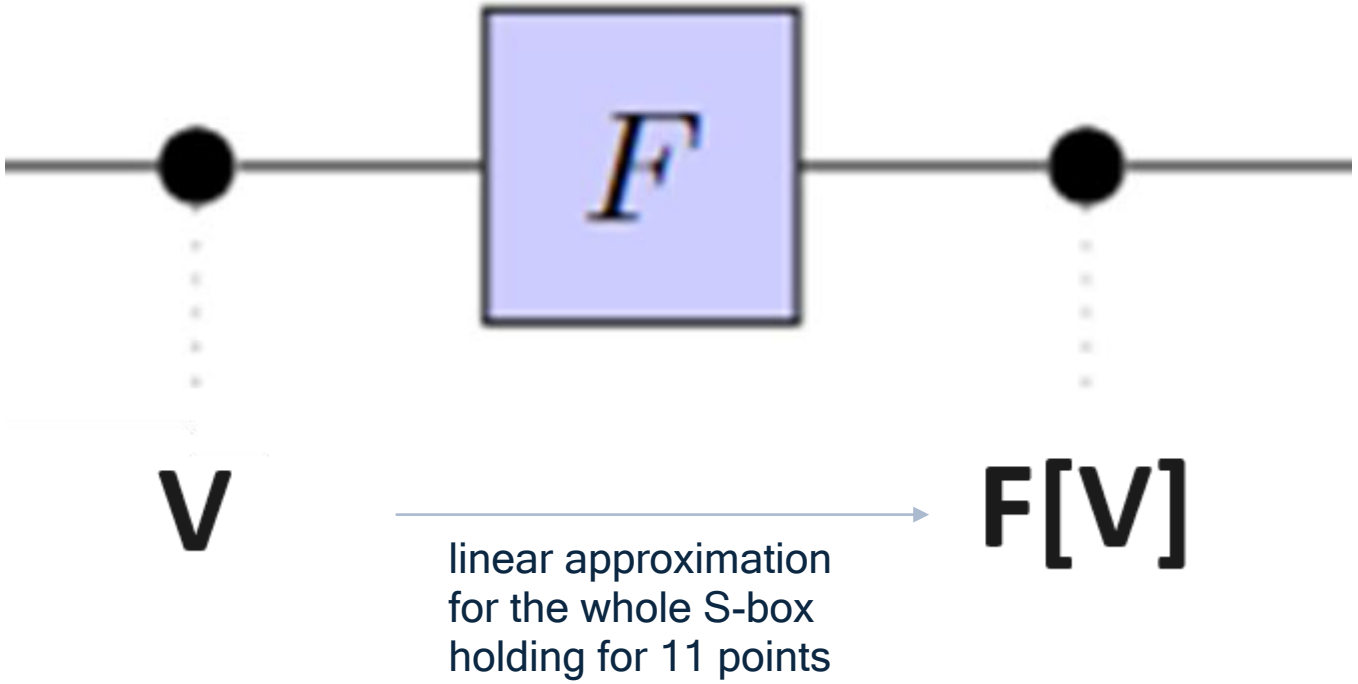
B_{11}={5,7,9,10,11,14,15,22,25,26,30}

FACT: each such property
has many ``clones'' which cover
the WHOLE space uniformly.

How is this possible???

For a non-linear function simply CANNOT duplicate a property by a simple translation…

Yes, you can, with a different matrix B.



Holographic Property - Quadratic S-boxes

Surprising?

8 A General Result for all Quadratic S-boxes

We recall that we call LSS or Linearizable Sub Set any set of points V such that

$$F[x] = A \cdot x + a \quad \forall x \in V.$$

Theorem 3 (Translation Invariance of LSS for All Quadratic S-boxes). *Let F be a quadratic S-box on k bits. If there exists a set V forming an LSS-k property for $F[]$ for some integer $|S| = k > 0$,* **then** *for any affine constant d the shifted set $V \oplus d$ also forms another distinct LSS-k property, i.e. there exists another matrix B and vector b such that:*

$$F[x] = B \cdot x + b \quad \forall x \in V \oplus d.$$

Proof: we use the polar form of a quadratic form. See the paper.

*Summary:

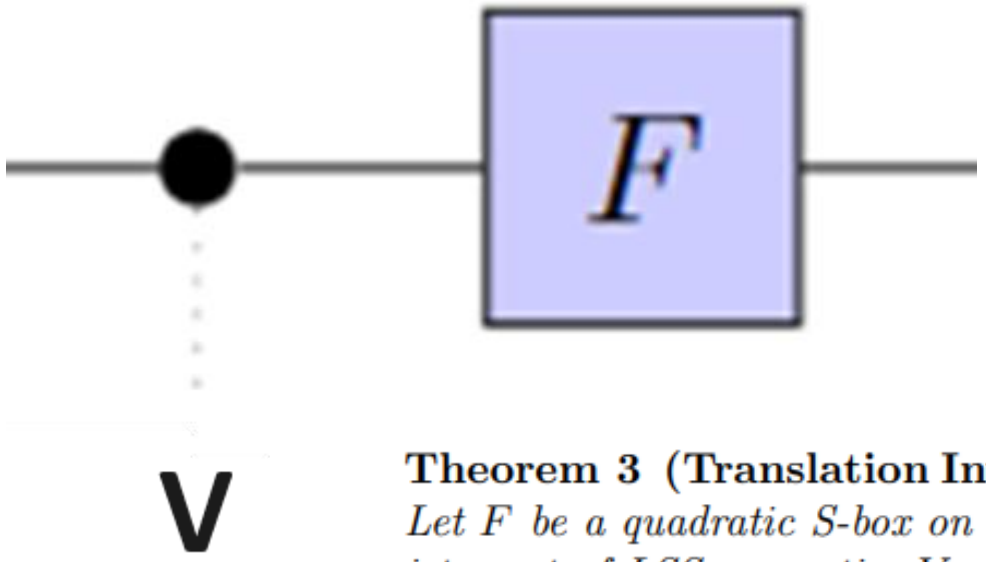
1. Large DMI => more linearization properties with a vector and a matrix
2. We relax previous notions => STRONGER and larger S-box approximations of size 11
3. For MQ S-boxes these properties can ALWAYS be cloned to obtain many other similar properties
4. Applications: differential-linear attacks, polynomial invariant attacks, etc.

Bonus

Agenda

Holographic Property - Level 2

Translating whole configuration by ANY input difference



7.1 A Level Two Theorem for all Quadratic S-boxes

Initially it might seem that this type of extensions of our result would be trivial. After all, if we had say a configuration of four LSS of size say 5+11+5+11, which definitely exist for Ascon, we can shift all these sets of points by a common constant a, and Thm. 2 says it will be again four LSS properties of the same size. However until now our theorem was existential, it just says that a certain matrix exists, and as such it cannot possibly guarantee that these matrices would form an affine space of a surprisingly small dimension, related or equal to the initial (small) dimension. If this happened this would be either accidental, or it needs to happen due to a deeper next level theorem. This result is new and was not published before.

Theorem 3 (Translation Invariance of LSS Dimension for MQ S-boxes). *Let F be a quadratic S-box on k bits. We assume that for a certain D there exist a set of LSS properties V_i such that the associated matrices A_i lie inside an affine space, and the sets V_i cover the whole space (not always disjoint). Then for any constant a (same for all sets) the shifted sets $a \oplus V_i$ also cover the whole space and there exist a set of associated matrices A'_i forming an affine space of dimension at most D.*

*Longer Conclusion

cf. our document: https://csrc.nist.gov/files/pubs/sp/800/232/ipd/docs/sp800-232-ipd-public-comments-received.pdf

3x weakness

Executive Summary for NIST. In our full report (same title) we read:

1. Every S-box can be linearized to some extent, best result=LSS-11.
2. Ascon/Keccak S-boxes are outliers exhibiting vast quantities of surprisingly large size and highly regular simultaneous linear approximations.
3. LAT, LSS and DDT sets in Ascon/Keccak interact very strongly and exhibit very high levels of regularity and a plethora of remarkable identities cf. Sections 3.2, 3.4, 4.1-4.4, 5, 6, 7.1, 8.5 and 9.X in [CoAmFo24].
4. Large LSS properties form super-structures stable by translation covering the whole space such as 11+11+11+10 with DDT and UDB alignment.
5. We don't have an attack (or not yet) but we have a concern.
6. We suggest that Ascon should be **upgraded** and use S-boxes which are **neither rotation symmetric nor quadratic** and have a lower DMI value.
7. This should be possible without significantly impacting Ascon speed and resource needs.

Thank you

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

© Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.

Qualcomm and Snapdragon are trademarks or registered trademarks of Qualcomm Incorporated.
Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.

Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries. Qualcomm patents are licensed by Qualcomm Incorporated.

Follow us on:

For more information, visit us at qualcomm.com & qualcomm.com/blog