On Maximum Size Simultaneous Linear Approximations in Ascon and Keccak and Related Translation and Differential Properties

Nicolas T. Courtois, Frédéric Amiel, and Alexandre Bonnard de Fonvillars

Qualcomm France S.A.R.L.

Abstract. In this paper we study the S-box known as Xi initially proposed by Daemen in 1995 and very widely used ever since in Keccak, Ascon, and many other. This type of ciphers is typically analyzed [in recent research] in terms of subspace trail attacks [TeDi19] and vector space invariants. An interesting question is then, when different spaces are mapped to each other by translations with a constant. In this paper we relax this fundamental question and we consider arbitrary sets of points and their translations. We generalize previous S-box partial linearization results on Keccak and Ascon from Eurocrypt 2017. We basically introduce new ways to linearize the Ascon S-box to the maximum possible extent. On this basis we show further remarkable properties and some surprising connections between [simultaneous] linear and [prominent] differential properties. We exhibit a new family of maximum size and optimal approximation properties with 11 points, beyond the maximum size of any set in the DDT table. We prove a theorem which guarantees that this type of properties are stable by arbitrary input-side translations which holds for all quadratic permutations. All this will be placed in the context of previous work on classification of 5-bit quadratic permutations.

Key Words. Ascon, Keccak, Xi S-box construction, Simultaneous Linear Approximations, LAT, DDT, Mutual Information, rotation invariants, affine space trails, connectors, connectivity tables, invariant attacks, cryptanalysis.

1 Introduction

Linear Cryptanalysis [LC] and Differential Cryptanalysis [DC] are classical attacks in symmetric cryptography [block ciphers, stream ciphers and hash functions]. These methods are typically claimed to be invented either at IBM and NSA in the 1970s, or by academic researchers in late 1980s. In fact it is easy to see that the frequently cited research articles from late 1980 / early 1990s did not invent anything new. It is possible to see that the study of differential and linear properties of ciphers is in many ways much older, directly and indirectly. For example in Section 7 of [CoGr22] we learn that Enigma rotor 3 from 1930s has a very strong linear approximation modulo 26 true with probability 10/26, and that all early German and Swiss Enigma rotors in 1930s had an exceptionally low number of invariant impossible differentials which number has substantially increased in later 1940s Enigma rotors, cf. [CoGr22]. Likewise,

several very specific design criteria which amount to resistance against a variety of linear, differential, higher-order differential and partial collision properties in the block cipher T-310 were already studied in Eastern Germany in 1970s, cf. [CoPoSc08,CSDPOSB17].

It is also important to see that in their very simple or "simplistic" versions, where isolated "single" linear and differential properties are exploited, these basic attacks simply do not work, or they do not work well, on any modern cipher such as AES, Ascon or Keccak. Or so it seems: sometimes an attack works better than predicted and contradicts the theory, cf. [CoQi20]. More importantly, many advanced attacks published in recent years, are all about various ways to combine multiple linear and differential properties with a systematic study of so called "Connectivity Tables" and the DLCT framework, see Section 3 in [HaDeEi24].

This paper studies the question of existence of [large size] simultaneous linear approximations with Ascon or/and Keccak S-box and a number of closely related facts and concepts. At Eurocrypt 2017 researchers work on constructing collisions on up to 6 rounds of Keccak with so called "connectors", cf. Section 4.2. in cf. [QSMG17]. Their "connectors" are based on partial linearization properties with 4 points known as LAS, which points in fact form an affine space of dim 2 on both I/O sides of the S-box. with special focus on LSA properties related to DDT() sets. In this paper we drop the requirement of points forming an affine space of Dim=2,3,4, and we study more general types of linearization properties with arbitrary sets of points. Most of the work inside this paper is applicable to Ascon, Keccak, XooDoo, Icepole, Ketje, Keyak, and few other similar ciphers.

Another important family of cryptanalytic attacks are various subspace trail attacks [TeDi19] which allow to predict the state of a cipher in terms of a sequence of affine spaces. Similar questions occur in many other families of invariant attacks such as in [CARG19,GJNQSS16] and many other research papers such as truncated differential attacks [TeAs16]. Here also we can drop the requirement of points forming a vector spaces. Then the classical question of repeated or reused linear spaces in subspace trail attacks or invariant space attacks can be simplified, and amounts to the study of pairs of sets or points shifted by a bitwise XOR with a constant.

In this paper we study various self-similarity properties of Ascon and other similar S-boxes. We mostly work with the Ascon S-box and we will discover some interesting rather non-trivial properties. This will lead to some new definitions, attempting to propose some relatively robust measures of vulnerability w.r.t. space/set reuse and simultaneous linear approximations. At the end we will compare Ascon to other similar S-boxes and also study their ASIC implementation cost (and few other important parameters) in order to avoid unfair comparisons. At this moment we do not attempt to design an actual invariant or subspace attack on several rounds of Ascon or Keccak (or not in this paper). The universe of potential attacks involving affine space trails and/or simultaneous linear and differential approximations [or equations or relations] is extremely large and diverse [BiCaQu04,CARG19,CoQi20,GJNQSS16,LiIsMeYa21,HaDeEi24].

2 Notation and Basic Definitions

We summarize here our notations.

F_2	Finite field $F_2 = \{0, 1\}$
$\oplus$	Bitwise XOR or bitwise addition modulo 2 in F_2^k
S-box	In this paper all S-boxes are assumed to be bijective
$F[], S[]$	Some cryptographic S-box $F_2^k \to F_2^k$
k	In this paper $k = 5$ most of the time
HW	Hamming Weight
BIBO	Bad Input Bad Output property cf. [LMCFW23]
I/O	Input and Output sides
LIO-5	5 linear relations involving terms from both I/O sides x_i/y_j
LAT	Linear Approximation Table
$\alpha{\cdot}x{+}\beta{\cdot}y{=}0$	One LIO equation from LAT where $\cdot$ is the dot product
A|2	Example of LIO encoding for $y_1 = x_1 \oplus x_3$
DDT	Differential Distribution Table
δ_{in}, δ_{ou}	Two 5-bit I/O differences
MI	Mutual Information
DMI	$\mathrm{MI}(\delta_{in}; \delta_{ou})$
DMI_S	$\mathrm{MI}(\delta_{in}, \delta_{ou} \| x, x' \in S)$
$y = F[x]$	Application of F to x, implies $x, y \in F_2^k$
x_i, y_i	We number bits of x and y from 0 to $k-1$
$co - X$	Complement of set X, $co - X = F_2^5 \setminus X$
LAS-2	Linearizable Affine Subspaces of dim 2
LSS-11	A Linearizable Sub Set of points of size 11
$\sum_{in}(V)$	XORs of all I/O for all $x \in V \subset F_2^5$
$\sum_{ou}(V)$	XORs of all outputs $S[x]$ for all $x \in V \subset F_2^5$
UDB	Undisturbed Bits property $F[x]_j \oplus F[x \oplus \delta_{in}]_j = \mathrm{Cst}$ for several j
S_{in}	Linear function s.t. $S_{in}[x]$ = the input of embedded Keccak S-box
T_{ou}	Affine function s.t. $T_{ou}^{-1}[y]$ = the output of embedded Keccak S-box
$Rot5$	Circular bit rotation on 5 bits; $Rot5[16] = 1$
ρ_{in}	Input-side rotation in Ascon, $\rho_{in}[x] = S_{in}^{-1} \circ Rot5 \circ S_{in}$
ρ_{ou}	Output-side rotation in Ascon, $\rho_{ou}[x] = T_{ou} \circ Rot5 \circ T_{ou}^{-1}$
kX	Values of 5 internal products; equal to $S_{in}[x] \oplus T_{ou}[S[x]]$ in Ascon

2.1 Basic Notions

Definition 1 (LIO relation). *For any subset of points $V \subset F_2^k$ we call an LIO relation for an S-box F any affine or linear combination mixing input and output bits $x_i \in F_2$ and $y_i \in F_2$ which is true with probability 1, i.e. it holds for every pair x, y where $x \in V$ and $y = F[x]$.*

LIO equations are a special case of "implicit equations" in mathematics, a.k.a. "I/O equations" as defined in [CoDe08] which we restrict to consider only implicit equations which are of degree at most 1 in both variables on both sides.

Our LIO and general I/O equations form a linear space stable by addition, and therefore the number of non-zero LIO relations is always of type $2^k - 1$.

Example 1a - Ascon. For we consider the set $V = \{0, 3, 8, 9, 10, 11, 22, 23, 29, 31\}$. For these 10 points by linear algebra we get exactly $3 = 2^2 - 1$ LIO relations which are in hex: $C|B$ $14|0$ $18|B$ which form a linear space of dimension 2. The last one $18|B$ could be transcribed as: $y_0 \oplus y_1 \oplus y_3 = x_4 \oplus x_3$ where $\oplus$ denotes the addition modulo 2.

Example 1b - Ascon. One can do better than size 10. It is possible to see that there exist seven sets of 20 points out of 32, such that exactly 3 distinct linear approximations (dim=2) exist and hold in all 20 pairs x, y and these sets, with corresponding linear I/O masks in hex, are:

- $1, 2, 3, 5, 6, 7, 9, 10, 11, 13, 14, 15, 17, 18, 21, 22, 25, 26, 29, 30$ $\quad 1|6$ $E|4$ $F|2$
- $0, 3, 4, 7, 8, 11, 12, 15, 16, 17, 19, 20, 21, 23, 24, 25, 27, 28, 29, 31$ $\quad F|4$ $13|6$ $1C|2$

It is important to notice that these two sets are equivalent by a XOR with a constant x, this for any $x \in \{18, 22, 26, 30\}$, and this sort of **translation similarity** situation happens extremely frequently in this paper.

Example 2 - Probabilistic Single LIO. Keccak S-box has an undesirable property: it has 5 probabilistic LIO where $y_i = x_i$ with probability of 24/32 or 0.75 each, see Property 2 in [LiIsMeYa21]. In this paper we study only deterministic LIO true with probability 1, when restricted to sets of say 11 values out of 32. This amounts to study of **simultaneous** linear I/O equations and the size of our set can be used to effectively **lower-bound** the probabilities for various sets of linear equations to hold jointly.

Definition 2 (LIO-k). *We say that a set of points $V \subset F_2^k$ is LIO-k when it has exactly $2^k - 1$ LIO (i.e. linear I/O relations).*

An important notion already studied for Ascon and Keccak S-boxes is the notion of LAS introduced at Eurocrypt 2017 cf. [QSMG17].

Definition 3 (LAS = Linearizable Affine Subspace). *Let S be an S-box on k bits. We call LAS or Linearizable Affine Subspace a set of points V which forms an affine subspace such that*

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

where A is $k \times k$ matrix and c is a constant vector in F_2^k.

In this paper we need to relax this notion slightly:

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*

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

2.2 On Rotation Properties

Inside Ascon S-box there is anther S-box embedded: the Keccak S-box. This has some very serious consequences as we will see in this paper. Keccak S-box has many symmetries and in particular it is stable w.r.t. a rotation of five wires like $i \mapsto i+1 \mod 5$. With an affine variable change on each side, the internal circular bit rotations of Keccak can be translated to Ascon as follows. These functions are of order 5 and orbits for these functions are six sets of size 5 and two singletons (size 1). These 6+2 sets play an important role in this paper and will be later called by letters $a, b, q, r, s, t, , y, z$, cf. Table 11 in page 26. We recall that $\rho_{in}[x] = S_{in}^{-1} \circ Rot5 \circ S_{in}$ and $\rho_{ou}[x] = T_{ou} \circ Rot5 \circ T_{ou}^{-1}$. It goes without saying that orbits for ρ_{in} are mapped to orbits for ρ_{ou} by the Ascon S-box.

f	specification
ρ_{in}	0,2,23,21,12,14,27,25,28,30,11,9,16,18,7,5,17,19,6,4,29,31,10,8,13,15,26,24,1,3,22,20
ρ_{in}^{2}	0,23,8,31,16,7,24,15,1,22,9,30,17,6,25,14,19,4,27,12,3,20,11,28,18,5,26,13,2,21,10,29
ρ_{in}^{-2}	0,8,28,20,17,25,13,5,2,10,30,22,19,27,15,7,4,12,24,16,21,29,9,1,6,14,26,18,23,31,11,3
ρ_{in}^{-1}	0,28,1,29,19,15,18,14,23,11,22,10,4,24,5,25,12,16,13,17,31,3,30,2,27,7,26,6,8,20,9,21
ρ_{in}^{5}	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31
ρ_{ou}	10,1,12,7,4,15,2,9,18,25,20,31,28,23,26,17,3,8,5,14,13,6,11,0,27,16,29,22,21,30,19,24
ρ_{ou}^{2}	20,1,28,9,4,17,12,25,5,16,13,24,21,0,29,8,7,18,15,26,23,2,31,10,22,3,30,11,6,19,14,27
ρ_{ou}^{-2}	13,1,21,25,4,8,28,16,15,3,23,27,6,10,30,18,9,5,17,29,0,12,24,20,11,7,19,31,2,14,26,22
ρ_{ou}^{-1}	23,1,6,16,4,18,21,3,17,7,0,22,2,20,19,5,25,15,8,30,10,28,27,13,31,9,14,24,12,26,29,11
ρ_{ou}^{5}	0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31

Table 1. Two linear internal isomorphisms or rotation functions relevant to Ascon.

With rotations, we can introduce a new type of property:

Definition 5 (LRS = Linearizable Rotation Stable Sub-Set). *We call LRS any set of points V, such that for every rotation of type ρ_{in}^{a} for any integer a including $a = 0$, there exist a matrix $A[a]$ and a vector $c[a]$ such that*

$$S[x] = A[a] \cdot x + c[a] \quad \forall x \in \rho_{in}^{a}[V]$$

2.3 On Maximal Size Properties

We also define:

Definition 6 (Maximum Size LAS/LSS/LRS). *Let S be an S-box on k bits and V be a set of points $V \in F_2^n$. We say that V is maximal size LAS / LSS / LRS respectively if*

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

and satisfies one of the previous definitions respectively AND the equality above does no longer hold if we add any additional points to V.

Definition 7 (Maximum Size LIO-k). *We say that V is maximal size LIO-k if at least one of $2^k - 1$ LIO relations is no longer correct for all $x \in V$, if we add any additional points to V.*

2.4 On Mutual Information and DMI

A very nice measure of quality of the S-box is to measure the Mutual Information between the input difference δ_{in} and the output difference δ_{ou} across all possible pairs of values. We call this quantity DMI and a simple formula to compute DMI is given below. DMI is of course motivated by and closely related to Differential Cryptanalysis and the DDT() sets we will study below in Section 3. In this paper we will show that it is also very strongly related and correlated to LC and more advanced forms of LC, and even with technical questions such Multiplicative Complexity (MC) and ASIC implementation cost. We use a standard formula for MI mixing joint and marginal probabilities found in wikipedia [wikiMI]. We define:

Definition 8 (DMI and Restricted DMI$_S$). *We define DMI as follows:*

$DMI = MI(\delta_{in}; \delta_{ou})$, done for all possible pairs of inputs, more precisely:

$$\sum_{\forall \delta_{in}, \delta_{ou} \in F_2^k} Pr_x(S[x] \oplus S[x \oplus \delta_{in}] = \delta_{ou}) \cdot log_2\left(\frac{Pr_x(S[x] \oplus S[x \oplus \delta_{in}] = \delta_{ou})}{2^{-k} \cdot Pr_{x,x'}(S[x] \oplus S[x'] = \delta_{ou})} \right)$$

In this paper we will sometimes restrict this definition to a subset $S \subseteq F_2^5$ as follows, and consider all pairs within a certain subset. Then we see if this MI can increase in specific cases. We define: $DMI_S = MI(\delta_{in}; \delta_{ou} | x, x' \in S)$, i.e.

$$DMI_S = \sum_{\forall \delta_{in}, \delta_{ou} \in F_2^5} Pr_{x,x' \in S}(x \oplus x' = \delta_{in} \wedge S[x] \oplus S[x'] = \delta_{ou}) \cdot log_2\left(\frac{Pr_{x,x' \in S}(x \oplus x' = \delta_{in} \wedge S[x] \oplus S[x'] = \delta_{ou})}{Pr_{x,x' \in S}(x - x' = \delta_{in}) \cdot Pr_{x,x' \in S}(S[x] \oplus S[x'] = \delta_{ou})} \right)$$

2.5 On 5-bit S-boxes and their DMI

In this table we recall some of the most prominent 5-bit S-boxes used in applied and lightweight cryptography.

sbox	specification
Ascon	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
Keccak	0,9,18,11,5,12,22,15,10,3,24,1,13,4,30,7,20,21,6,23,17,16,2,19,26,27,8,25,29,28,14,31
Icepole	31,9,18,11,5,12,22,15,10,3,24,1,13,4,30,7,20,21,6,23,17,16,2,19,26,27,8,25,29,28,14,0
Thakor	10,3,11,22,17,4,1,8,12,28,23,18,26,6,31,20,15,24,29,13,14,19,30,5,25,27,7,0,16,21,2,9
Fides	1,0,25,26,17,29,21,27,20,5,4,23,14,18,2,28,15,8,6,3,13,7,24,16,30,9,31,10,22,12,11,19

Table 2. Various cryptographic S-boxes on 5 bits studied and compared in this paper.

2.6 On Prediction of LAS-2 Properties

A well known folklore result is such that zero of LAS-2 properties exist for APN S-boxes. This also holds for few other classes of cryptographically strong near-optimal S-boxes such as based on power, inverse and exponential functions.

sbox	#0s in DDT	#8s in DDT	DMI	MC	LAS-2
Ascon	707	20	1.910	5	80
Keccak	707	20	1.910	5	80
Icepole	687	10	1.819	6	70
Thakor	637	4	1.589	?	45
Inv-GF32	527	0	1.125	8	0
Fides	527	0	1.125	8	0

Table 3. Basic parameters of S-boxes on 5 bits studied in this paper.

We claim that the number of LAS-2 properties can be predicted with a decent level of precision from DMI and from DMI alone.

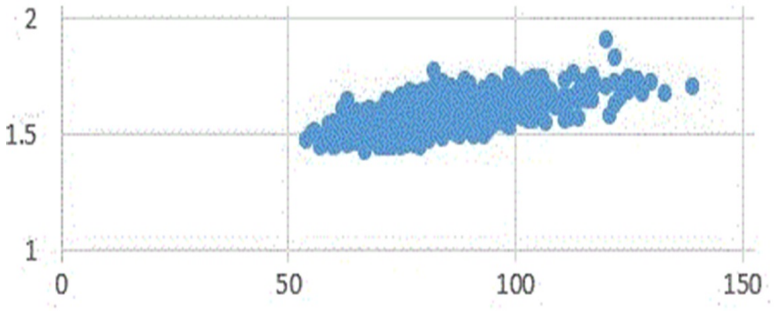

Fig. 1. A near-affine relationship which shows that DMI and LAS-2 properties are related and that the number of LAS-2 mappings drops to zero below $DMI \approx 1.1$.

To show this we have done extensive computer simulations with S-boxes created essentially at random or by mutations from other known S-boxes, to show that there is a strong near-affine relationship between the number of distinct LAS-2 properties and the DMI value, see Table 1. We conjecture also that a similar type of relationship hold for LSS properties and many other.

3 The DDT Connection

The idea of how DDT (Differential Distribution Table) reveals some affine spaces and their transformations is not new, see Section 5.2 in [GJNQSS16]. This paper explores further connections between LAS, LSS and DDT. Following [QSMG17] we define:

Definition 9 (DDT Sets). *Let S be an S-box on k bits. We define the following set:*

$$DDT(\delta_{in}, \delta_{ou}) = \{x \in F_2^n | S[x] \oplus S[x \oplus \delta_{in}] = \delta_{ou}\}$$

In Observation 2 in [QSMG17] the authors already show that the sets of points of type $DDT(\delta_{in}, \delta_{ou})$ are sometimes LAS of size 4 and are affine spaces, sometimes they are of size 8 and not affine spaces, and contain LAS as subsets. In addition we also observed that in many cases DDT sets of size 8 are perfect disjoint unions of two LAS of size 4.

3.1 On Translations of Sets

It is possible to see that in S-boxes generated at random, the sets of type $DDT(\delta_{in}, \delta_{ou})$ behave like random sets which are stable by a translation by δ_{in} and these sets are **not** affine spaces typically (cf. Section 5.2.3. in [GJNQSS16]). However with Ascon or Keccak S-box we get some very special situations. For example in Section 3.3 we will discover that all sets of the form $DDT(0x10, \delta_{ou})$ are disjoint cosets and translations of each other by a constant, and they also fix some bits on both sides in a regular and systematic way.

3.2 On Disjoint Sets of δ_{ou}

We observe that in Ascon and in Keccak there are exactly 20 sets of type $DDT(\delta_{in}, \delta_{ou})$ which are of size 8 and are "behind" each 8 which appears in the DDT table of Ascon. The set of δ_{in} for which this happens contains 5 elements, and there are 5 lines in the DDT table which contain four 8's each. All the output differences are also disjoint across all the four entries in each of 5 lines: the set of 20 δ_{ou} which are used is a set of 20 distinct elements of F_2^5 which is a bit surprising. All δ_{in} for which we obtain have the "undisturbed bits" UDB property extensively studied by Tezcan in multiple papers for Ascon [TeAs16,TeDi19] and other ciphers [MaTe14].

3.3 On DDT-related Sets Which Fix Some Bits

Definition 10 (ioab). *We say that a set of points $V \subset F_2^k$ is ioab for two integers a, b if for every x, y with $y = S[x]$ there are a bits out of 5 fixed on input side and there are b bits out of 5 fixed on the output side.*

Example 1: We consider one of the LAS sets of size 4 already studied in [QSMG17] which is 13,14,29,30↦3,6,10,15 and which has a property which can be summarized as ?11??=>0??1? in binary with 4 bits being fixed. This set is of type io22: two input bits are fixed at input side, and two output bits are fixed at output side, this simultaneously for all 4 points and their transformations $y = S[x]$. In the same way the set 9,10,25,26↦5,8,12,1 has property ?10??=>0??0? and is of type io 22 also.

Example 2: Finally the union of the two sets listed above, which is exactly: $\{9, 10, 13, 14, 25, 26, 29, 30\}$ is of type io11. Moreover this set of 8 values is always in the form (in binary):

$$C_8 = \{9, 10, 13, 14, 25, 26, 29, 30\} \quad ?1x?? => 0??x?$$

where x is the same value, x =0, or 1 on both sides. Moreover all possible translations of this set $C_8 \oplus b$ are also always of type io11, and they are always of the form $DDT(0x10, \delta_{ou})$. Moreover these sets form 4 disjoint cosets with 4 distinct $\delta_{ou} \in \{0x9, 0xB, 0x1A, 0x18\}$ covering the whole space of 32 points. This type of translation uniformity is quite surprising.

Example 3: By exhaustive enumeration we found that there exists exactly 8 sets of type LSS-7 which are io11. For example the set $\{0, 5, 9, 13, 20, 24, 28\}$ which is of type ???0? =>?0??? or set $\{1, 4, 8, 12, 21, 25, 29\}$ which is of type ???0? =>?1???.

Applications in Cryptanalysis: It is easy to see that if all Ascon S-boxes fix some bit say $y_i = C$ at output of one round, then [avoiding the action of round constants] at least 56 S-boxes in the next round will have $x_i = C$ at the input of next round, for any constant C. This is due to the fact that 0^{64} and 1^{64} are invariants for all five linear diffusion layer permutations used in Ascon. If in addition, our set of say 4 or 7 points is stable by XOR with 4=0x4, then the action of round constants is neutral and has no effect.

On this basis the attacker can try to construct probabilistic invariant properties on full Ascon, which is very difficult task with a lot of coding and processing of large datasets for favorable events, falling outside the scope of this paper.

4 Pairs of Hyperplanes in LAT and Related Sets

We would like to discover different ways how the Ascon can be partly linear in the spirit of and generalizing our notion of LAS. Before we study arbitrary sets of points, which we will do later and which quickly leads to computational limitations, we are going to discover interesting sets of points by an indirect method. We will now re-visit the question of partitioning the Ascon/Kecack S-box space of 32 elements ex-nihilo, ignoring affine spaces or some actual DDT() sets. We rather work in the spirit of LAT (Linear Approximation Table) and we will consider all possible pairs of hyperplanes: (maximum dimension affine spaces). It was already noted in [QSMG17] that we cannot hope that Ascon S-box maps affine spaces of dimension 3 to a space of dim 3. By extension we can hardly hope that this will happen with hyperplanes or at maximal dimension 4, and nothing like this was ever observed for any major cryptographic S-box. Therefore we must consider a question of more probabilistic or approximative nature:

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?

To see this we consider an arbitrary linear space L^i with 16 elements on the input side; and an arbitrary linear space L^o with 16 elements which is intended to be used on the output side. This is related to the well known concepts of Walsh coefficients, LAT tables, sometimes called correlation tables. We define:

$$L^i = \{x \mid \alpha \cdot x = 0\} \quad \textit{and} \quad L^o = \{y \mid \beta \cdot y = 0\}$$

where $\cdot$ is the dot product. There are $961 = 31^2$ possible pairs of linear spaces L^i, L^o. This corresponds to both α, β being non-zero, in other terms we discard the first line and the first column of any LAT table as being degenerated.

In what follows let S^{-1} be the inverse of the Ascon S-box. We will denote the complement by the following notation: $co - X = F_2^5 \setminus X$.

Definition 11 (LAT Hyperplane Pair Approximation Test).
For any **bijective** *S-box $S : F_2^k \to F_2^k$ We consider the following natural partitioning of 2^k elements into 4 sets:*

$$\begin{array}{cccc} S^{-1}[L^o] \cap L^i & \cup & S^{-1}[L^o] \cap co - L^i & \cup \\ co - S^{-1}[L^o] \cap L^i & \cup & co - S^{-1}[L^o] \cap co - L^i & \end{array}$$

In this paper the S-boxes studied are always bijective and $k = 5$. In this case these 4 sets are then a **disjoint** partitioning of 32 elements into 4 sets (which is not true in general). It is then easy to see that the sum of sizes in each line is $2^{k-1} = 16$ and the same is true for each column. Therefore the cardinals of each two sets lying opposite on each diagonal are identical [again because S is bijective].

Let $s_{00}, 16 - s_{00}$ be the sizes of sets defined above in the 1st line. Then in the second line the are swapped: we have $16 - s_{00}, s_{00}$ elements. Then the

number of solutions to the LIO equation $\alpha \cdot x + \beta \cdot y = 0$ is $2s_{00}$ by the union of $S^{-1}[L^o] \cap L^i$ and the other corner with both sets complemented. Likewise the number of solutions to a negated LIO equation namely $\alpha \cdot x + \beta \cdot y = 1$ will be in general $2^k - 2s_{00}$ and both equations are represented typically by the same unique entry in LAT table. We recall that most authors define LAT in terms of relative numbers or "biases" and our numbers are shifted by 2^{k-1} accordingly and therefore we have:

$$LAT(\alpha, \beta) = 2s_{00} - 2^{k-1}$$

Example with Ascon. For example with Ascon S-box we have 336 entries out of 961 with a partitioning of type 6+10+6+10 or vice versa. This means that in LAT we will see 336 entries of type $16 \pm 4 = 2 \cdot 6$ or $2 \cdot 10$ respectively.

Note. We rediscover a well-known fact that for a bijective S-box, all entries in the LAT table are even. In this paper we emphasize the fact that our pairs of sets of the same size are frequently (but not always) more deeply related: by a translation with a constant.

Observations. It is possible to see that 6+10 situations or $LAT(\alpha, \beta) = \pm 4$ are the most common case in all cryptographic S-boxes at size 5, and other situations are less frequent in any cryptographic S-box. We cannot really hope to have a split of type 0+16 or we would have an extremely weak cipher. We also observe very high frequencies of type 8+8 which cases are perfectly balanced. It corresponds to zeros inside an LAT table, and does not lead to any linear bias whatsoever. The situations of type 4+12 are less frequent and correspond to stronger biases with $LAT(\alpha, \beta) = \pm 8$ and happen 40 times out of 961 with Ascon S-box. There are also other possibilities such as 5+11 which do not happen in Ascon/Keccak or other quadratic S-boxes studied, yet they do happen for other S-boxes on 5 bits. In the Table 4 we report how all possible 961 pairs of affine spaces of Dim 4 lead to a variety of situations in Ascon and Keccak.

4.1 Unexpected Properties and Translations

In this process we always generate pairs of sets of the same size. For example we consider $S^{-1}[L^o] \cap L^i$ and $co - S^{-1}[L^o] \cap co - L^i$. Can these two sets be related to each other, for example by a translation (XOR) with a constant?

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

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

It important to see that if these two sets with here $s_{00} = 6$ are related by translation, then also the two other complementary sets of sizes $16 - s_{00} = 10$ are also and always related by the same translation. This is due to the fact that we complement (in several ways) inside affine spaces on two sides, and affine spaces are more likely to be stable by certain (but not all) translations. Can this be guaranteed to work? Yes, and we have the following result:

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.*

Proof. Our translation C is by definition a XOR of one element of L^i with parity=0 and one from $co - L^i$ with parity=1, therefore we have parity=1 and $C \in co - L^i$. Likewise we also have $C \in co - S^{-1}[L^o]$. Therefore our constant belongs to the last set: $C \in co - S^{-1}[L^o] \cap co - L^i$. We define S by adding C to all elements from the second set $S^{-1}[L^o] \cap co - L^i$, in S we always swap the parity on both sides shifting to the other coset of only two, so $S \subseteq co - S^{-1}[L^o] \cap L^i$. Now we know that the sets are of the same cardinality and so $S = co - S^{-1}[L^o] \cap L^i$. This ends the proof. □

4.2 On Sets Related to LAT in Ascon and Other S-boxes

It is easy to see in this process we obtain $4 \cdot 585 + 2 \cdot (336 + 40) = 3092$ distinct sets of points of sizes 4,6,8,10,12. We start by two essential observations.

Fact 4.1. For all quadratic S-boxes on 5 and 6 bits, and for all sizes, all inputs in all four LAT-related sets V add to zero at input side, i.e. $\sum_{in}(V) = 0$.

Counter-Examples. This is not true in AES and for 5-bit S-boxes which are not quadratic, e.g. Icepole.

Can Our Sets Be LSS? We conjecture that for S-boxes which are not quadratic no set of any size generated as above are LSS, not even at size 4 (the easiest). It might seem that many sets of 4 will form an LSS property, and the four I/O pairs can be interpolated by linear algebra in several ways (pairs, space of dimension 5). However this is not true, the system of equations could be contradictory and they systematically are with cryptographic S-boxes. More precisely, all our sets of size 4 for quadratic S-boxes are such that the sum (XOR) of 4 inputs $\sum_{in}(V)$ is zero, and the sum of 4 outputs $\sum_{ou}(V) = 0$ is never zero. This is true in Ascon/Keccak and for all quadratic S-boxes of size 5 where the inverse is not quadratic, following Table 2 in [BoBiSa17]. Then it is impossible to obtain an LSS, because an affine space should be sent to an affine space by our affine transformation with matrix+vector.

In some cases our set of 4 points **can** be LSS, for example when the S-box is quadratic and its inverse is quadratic. This happens for example with S-box class 17 from Table 1 in [BoBiSa17] all of which are quite weak. In this case all 96 sets of sizes 4,6 generated are LSS, and 496 out of 2204 sets of size 8 generated are LSS. Then at size 10 no sets are LSS even though plenty of LSS-10 properties exist for this S-box, which can be easily interpolated from our later Table 13. For Ascon, at size 12 we cannot hope to find an LSS-12 property for this S-box, they simply do not exist, cf. Thm. 2 page 18. So far we never observed an example where a LAT-related sets of size 4, 6 or 8 would be LSS for any "strong" or cryptographically significant S-box.

Corollary and Observation. There is no intersection between two remarkable sets of 80 properties on 80 points: 1) the 80 sets of 4 which are LAS-2 properties studied at Eurocrypt 2017 cf. [QSMG17], and which are also LSS-4, and the 80 sets of size 4 found for Ascon related to LAT and which are all possible

sets of the form $S^{-1}[L^o] \cap L^i$ or similar of size 4. All these 80+80 properties with 4 points are disjoint: $\sum_{ou}(V) = 0$ for the firtst 80 and never zero for the other 80.

Cases where $\sum_{ou}(V) = 0$. We observed that for all quadratic S-boxes such that the inverse is not quadratic, outputs for all sets of size 4, 6 almost never add to zero at output side. For example in Ascon at size 6 there are only 2 such examples out of 672 which is again our special unique pair $\alpha = 20 = \rho_{in}[31]$ and $\beta = 11 = \rho_{ou}^{-1}[31]$ where $\sum_{ou}(V) = 0$.

On Entropy of $\sum_{ou}(V)$. We observed that only some specific output differences happen for various sets of size 4 or 6. For example there are 80 sets of size 4 and the output side sum is always $y \in \{2, 6, 8, 17, 24\}$ which are also exactly those 5 where the output of the Keccak S-box has HW=1, i.e. $T_{ou}^{-1}[y] \in \{1, 2, 4, 8, 16\}$, and each of these 5 values is taken 16 times.

On $\sum_{ou}(V)$ with LSS In Section 8.5 we find 160 examples of LSS-10 where $\sum_{ou}(V) = 0$ is never zero. In contrast with our 32 A_{11} properties all values $\sum_{in}(V)$ and $\sum_{ou}(V)$ are equally probable.

Relevance of $\sum_{ou}(V) = 0$ in Cryptanalysis. In general, rare cases where $\sum_{ou}(V)$ are those which will have an interest in cryptanalysis for various zero sum attacks, cube distinguishers and many related concepts, see for example [HuCu24].

all	8+8	6+10	4+12	0+16
961	585	336	40	0

Table 4. Ascon S-box interacting with 961 pairs of spaces of dim 4 related to LAT

4.3 On Rotation Invariance with our Partitions

It is possible to see that all sets obtained in our 961 partitions match another set by a rotation such as defined previously as ρ_{in}. In our example above, we had $S^{-1}[L^o] \cap L^i = 0, 3, 20, 21, 29, 31$ etc, and this is a very special example which example will be called later called B in Section 5 due to an LIO-6 property. In this case, all our four sets of size 6 and 10 are stable by rotations ρ_{in}. By inspection we verified that this type of internal rotational symmetry happens just once in this exact case with $\alpha = 20 = \rho_{in}[31]$ and $\beta = 11 = \rho_{ou}^{-1}[31]$.

In all other cases, an interesting question is if a rotation of one set can produce another "twin" set of the same size with a different pair of α, β. The answer is that this happens systematically for all sets generated no matter their size.

4.4 Translation Similarities

We have tried all 961 possibilities and found that in balanced cases 8+8, sometimes we get related sets of 8 points, and in **all** unbalanced cases 6+10 or 4+12 we **always** get related sets without any exception.

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

Table 5. Pairs spaces of the same size which are equivalent by translation with Ascon.

This is a bizarre situation like winning in a game of heads/tails in 336+40 cases in a row, which are exactly those cases which are **unbalanced** like 6+10, and therefore potentially cryptographically significant. In fact however this property is not specific to Ascon. Similar things happen to all other quadratic S-boxes, cf. Table 15 in Appendix. In contrast it is important to see that this does not happen **at all** for random S-boxes, not even with a low frequency, in other terms we switch from 100% to 0% for all unbalanced pairs, as we will see in Table 7 below in page 14. First we will look at what happens in Icepole, when the S-box is altered slightly by adding two high degree products, cf. Table 6 below.

Icepole	8+8	7+9	6+10	5+11	4+12	0+16
961	435	220	240	36	30	0
inp-shifted	120	10	160	6	20	0
unrelated	315	210	80	30	10	0

Table 6. Pairs of spaces equivalent by translation with Icepole S-box.

Finally we see that no weakness whatsoever is observed for Thakor, which has DMI close to that of a typical random S-box, cf. Fig. 1.

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

Table 7. Pairs spaces of the same size equivalent by translation with Thakor S-box.

In spite of random S-boxes being devoid of this type of vulnerability, in Table 15 in Appendix we show that most or all cryptographically significant quadratic S-boxes have significant translation properties of this type.

4.5 Output Side Translations

We also note that nothing like this happens in a comparably strong proportion at the output side of the Ascon S-box, cf. Table 8 below.

all	8+8	6+10	4+12	0+16
961	585	336	40	0
out-shifted	60	80	40	0
unrelated	525	256	40	0

Table 8. Equivalence by translation at the output side with Ascon.

5 On Discovery of New I/O Partitioning Properties

We have examined all the 961 possible pairs of dim 4 spaces, and looked at various sets of sizes 4,6,8,10,12 to see if some of them achieve some particularly large numbers of simultaneous LIO relations.

cases	dim	LIO-2	LIO-3	LIO-4	LIO-5	LIO-6	LIO-7
LIO	#	3	7	15	31	63	127
4 from 4+12	40+40	0	0	0	0	0	80
6 from 6+10	336+336	0	0		670	2	0
8 from 8+8	$4 \cdot 585$	0	700	1260	360	20	0
10 from 6+10	336+336	272	320	80	0	0	0

Table 9. Different LIO dimensions in all 961 pairs of spaces tried.

By brute force enumeration of 961 spaces we discover that there exist exactly 22 pairs of dim 4 linear spaces with as many as 63 simultaneous LIO relations. These 22 selected simultaneous linear approximations of Ascon split into two categories:

A 10 pairs L^i, L^o of balanced type 8+8 already studied in [QSMG17] without realizing that we obtain a large number of 63 LIO relations at size 8.
B 1 unique special (not previously studied) unbalanced pair of L^i, L^o of type 6+10 with also 63 LIO albeit at size 6.

Observations on Set A of $8 \cdot 8$ points. For each of 10 pairs L^i, L^o we get two sets of 8 points. These 20 sets of points are **exactly those** which are "contained" in the 20 Ascon DDT table entries equal to 8, and all of which can be decomposed in 6 different ways as a disjoint (fact not noticed or not emphasized before) union of one of 80 possible LAS (see Observation 1 in [QSMG17]). This set of 20 sets of 8 points from DDT() is stable by arbitrary translations by a constant.

Observations on Set B of $6+6$ points. On the surface, the latter case is just 1 of 336 of "inp-shifted" cases reported above with $\{0, 3, 20, 21, 29, 31\}$ or the same set XORed with 26 generated from the same pair L^i, L^o. This partitioning is however quite special and will also be relevant in few other places as we will see below. We have $L^i_B = \{0, 1, 2, 3, 8, 9, 10, 11, 20, 21, 22, 23, 28, 29, 30, 31\}$ and $\alpha = 20 = \rho_{in}[31]$ and
$L^o_B = \{0, 3, 4, 7, 9, 10, 13, 14, 16, 19, 20, 23, 25, 26, 29, 30\}$ and $\beta = 11 = \rho^{-1}_{ou}[31]$.

6 Do Stronger Properties Exist?

We are now going to show a surprising result: it is possible to achieve 31 LIO (dimension 5) with 11 points (larger than ever before) and this is the best we can hope for with Ascon. Furthermore we will show that all our LIO-5 properties of size 11 are also LSS-11, and that additional strong translation symmetry properties hold.

We have used a SAT solver coding which allows to enumerate **all** possible solution to this problem and show that no other solutions exist and that solutions of size 12 or better do not exist. We found that exactly 32 solutions exist and that they come in two pairs of 11 disjoint points, forming 16 joint dual LIO-5 approximations of Ascon spanning 22 out of 32 points. In order to study these properties we define:

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

This set will be later also called $s^i + t^i + \{0\}$ and it forms an LSS-11 property for Ascon. We further define a special well-chosen dual or translation of A_{11} which will be called $B_{11} = A_{11} \oplus 0x1A$, which is the same as shifting by 26 in decimal. It is easy to see that $B_{11} = \{5, 7, 9, 10, 11, 14, 15, 22, 25, 26, 30\}$ which set will sometimes also be called $r^i + q^i + \{26\}$ later, cf. Table 11 in page 26.

Disjoint Sets. We observe that A_{11} and B_{11} are disjoint, which is not obvious at all, as these sets are not affine spaces and the maximum size of intersection of any of these sets with any affine space of Dim 4 is at most 8 not 16. However at the output side, these sets are contained inside an affine space and its complement, which provides an easy explanation why they are disjoint. Moreover this special L^o is **precisely** from the one special and unique case obtained above out of 961 and called "Set B", with 63 LIO and $\alpha = 20 = \rho_{in}[31]$ and $\beta = 11 = \rho_{ou}^{-1}[31]$. We have $L_B^o = \{0, 3, 4, 7, 9, 10, 13, 14, 16, 19, 20, 23, 25, 26, 29, 30\}$ and $S[A_{11}] = \{0, 4, 10, 13, 14, 19, 20, 23, 26, 29, 30\}$.

New LSS-11 Properties. Now we observe that all our $32 = 16 \cdot 2$ properties of size 11 are also LSS-11, which is not obvious at all here, and is not true in general for other LIO-5 properties. To better visualize these properties, we list only those 5 out of our 31 LIO properties which use exactly one output bit.

- $A_{11} = 0, 3, 4, 12, 16, 17, 19, 20, 21, 29, 31$ $\quad B|1\ 1C|2\ F|4\ 17|8\ 16|10$
- $B_{11} = 5, 7, 9, 10, 11, 14, 15, 22, 25, 26, 30$ $\quad 12|1\ F|2\ E|4\ 1D|8\ B|10$

Translation Invariance. It is important to see that the fact that we found 32 properties is not accidental. In fact our property is invariant by arbitrary input-side translation by a constant (but not on the output side) as we will see later, see Thm. 3 below page 22. Moreover the 32 properties here work in pairs, we get 16 pairs of disjoint 11+11 points obtained by translation from A_{11}, B_{11} which all give pairs of distinct LSS-11 approximations with disjoint supports. These properties span uniformly the whole space, and for different configurations of points there will be typically several way to approximate them using these properties.

To summarize here is our strongest Ascon/Keccak simultaneous approximation LSS-11 result:

Theorem 2 (Ascon Family of LSS-11 Properties). *There exists exactly 32 sets of size 11 such that the Ascon S-box is fully linearized on each set of 11 points under the form*

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

which are all of the form $A_{11} \oplus b$ *where*
$A_{11} = \{0, 3, 4, 12, 16, 17, 19, 20, 21, 29, 31\}$ *and no solution exists with 12 points. All solutions at size 11 are isomorphic by a translation with a constant.*

Proof. We have obtained this result by 2 methods. First by an automated proof with a SAT solver returning UNSAT or enumerating 32 solutions. We have used the CryptoMiniSAT 5.8 solver developed by Mate Soos. We have also obtained the same result with a brute force method coded on GPU. □

Output Side Translations. Nothing even remotely similar happens for output side translations. All 1024 output side translations of all 32 set of type $A_{11} \oplus s$ are distinct sets of 11 points.

On Cryptographic Quality of LIO Equations. The 5 equations we listed above e.g. $B|1$ $D|4$ etc, could be qualified as BO or Bad Output, and Keccak is in this respect substantially weaker than Ascon, see notions of BIBO for DDT and LUT tables and comparison in Table 8 in [LMCFW23].

Do Better S-boxes Exist? If we replace the Ascon S-box by Fides S-box which is an APN, then the highest possible number of points to achieve the same type of full S-box linearization drops from 11 to 7, see Table 12 page 31.

On Inverse S-boxes. We have verified that the maximum size of LSS property with the inverse S-box for Ascon is LSS-10. This is related to the fact that in general cubic S-boxes are stronger and our LSS-11 properties are one-sided properties.

On LIO and S-boxes with Quadratic Inverses. We have also verified that quadratic S-boxes which have quadratic inverses achieve systematically bigger or worse LSS values, for example LSS-14 or even higher. This is true for all such S-boxes without any exceptions (!). Therefore ONLY quadratic permutations in size 5 which have a cubic inverse qualify for cryptographic applications. All the other are easily **disqualified**: for example they always have differentials with probability at least of at least 0.5=16/32, see Table 1 in [BoBiSa17]. Detailed results on maximum achievable LSS-sizes in different S-boxes will be later shown in Table 12 in page 31.

Applications. All the results in this paper apply also to Keccak S-box by a simple affine variable change. This with a notable exception of Section 3.3, where we look at some individual bits in Ascon.

7 Further Study of LSS-11 Properties Based on A_{11}

We give here two examples of matrices obtained in LSS-11 properties, with for A_{11} and $B_{11} = A_{11} \oplus 26$. In the case of A_{11} we have:

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

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

In the case of B_{11} we have:

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

For example with input $22 = 10110 = x0x1x2x3x4$ we get output $17 = 10001 = y0y1y2y3y4$ in binary where $x4/y4$ represent the least significant bit.

On Rank of LSS Matrices. We have verified that for all affine shifts of our LSS-11 property, which are always of the form $A_{11} \oplus x$, the matrices are invertible in 30/32 cases for all $x \neq 0$ and $x \neq 26$. In 2/32 cases which are exactly A_{11} and B_{11} for which the matrices are shown above, the rank drops to 4. It is a bit surprising to discover that the right kernel space of each matrix is the same and contains exactly one non-zero element which is in both cases the same and equal to 26.

Further Observations. In general the 32 matrices we find here are not exactly random matrices and live in a space of a small dimension, see Section 8.3 below. Constant parts do not behave like random numbers either. In Section 8.4 we will discover that in half or 16/32 of these approximations of type $A_{11} \oplus x$, the constant part on 5 bits is the same and equal to $4 = 00100$.

7.1 Interaction of A_{11} and DDT Sets

The reader might think that the 11 points are related to DDT() sets, and have a deep connection to differential cryptanalysis, while by its origin it was derived from linear cryptanalysis. This is what we are going to show now. Initially, research for some DDT set connection seems to fail very badly. We have checked that the set of 11 and their 32 translations do NOT contain any of the total 2594 sets of 4,6,8 or 10 points studied in Section 5, nor one would be included inside any one set of 12 points obtained in this process. However we discovered that very interesting things happen when we study how these sets interact with themselves (their own affine shifts):

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 will later be called t, 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 "undisturbed bits" UDB properties in [TeAs16,TeDi19].
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 will later be called $s \cup r \cup b$ 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 will later be called $q \cup a$ which 10 values are **exactly** those lines in DDT table except for the special case of $x = 26 = 0x1A$ already used in B_{11}.

Remark on A_{11} and Differential Cryptanalysis. Each time when intersection of two A_{11} is of maximum size 6, we obtain a property which concerns 16/32 points and yet captures 6/8 of the points which might interest the attacker the most: those concerned by differentials true with maximum probability of 8/32. This question is further studied in Section 12 and leads to the study of the notion of a DMI profile. This is also expected to lead new types of differential-linear attacks, guess then determine collision finding attacks, or/and algebraic key recovery attacks, where the attacker makes several assumptions about input differences of several S-boxes, and these properties entail $2 \cdot 31$ additional linear I/O relations between 20 bits.

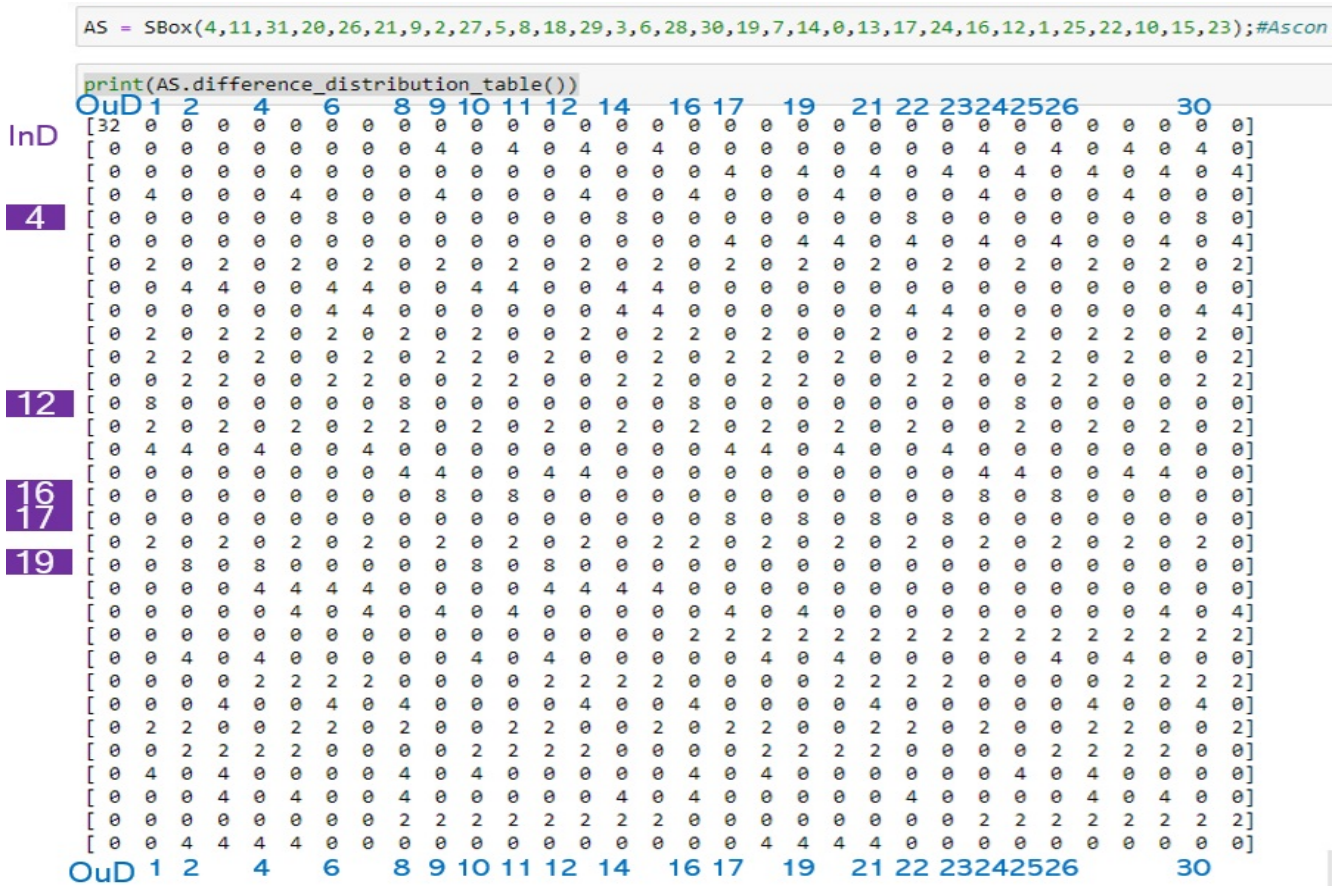

Table 10. The DDT table for Ascon with focus on 5x4 sets DDT() of size 8.

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. In mathematics, the process of "polarization" of a polynomial in produces a unique symmetric bi-linear homogeneous form, from which the original polynomial can be recovered. In the case of multivariate quadratic S-boxes, also known in the literature as Dembowski-Ostrom polynomials, researchers typically study their "difference function" cf. Section 8 in [FeHAPa21] or their "polar form" cf. Appendix 1 in [PaGo98]. There are some cosmetic differences between these notions such the presence of certain terms which are constants (e.g. $F[0]$). In this paper we define:

$$\Delta_F(x, d) = F[0] \oplus F[x] \oplus F[d] \oplus F[x \oplus d].$$

It is easy to show that our polar form is a bi-linear multivariate function in $k + k$ variables, and when one variable is fixed, it becomes a multivariate linear function in k variables, also known as a "linearized polynomial". These well-known facts are sufficient to prove our theorem. By the initial property we have $F[x] = A \cdot x + a \quad \forall x \in V$ and we are now going to replace $F[x]$ by $\Delta_F(x, d) \oplus F[0] \oplus F[d] \oplus F[x \oplus d]$ which gives:

$$F[x \oplus d] = (\Delta_F(x, d) \oplus A \cdot x) + (a \oplus F[0] \oplus F[d]) \quad \forall x \in V$$

which is the same as:

$$F[x] = (\Delta_F(x \oplus d, d) \oplus A \cdot (x \oplus d)) + (a \oplus F[0] \oplus F[d]) \quad \forall x \in V \oplus d$$

and given that when d is fixed our $\Delta_F(x, d)$ becomes linear, we obtain:

$$F[x] = (\Delta_F(x, d) \oplus A \cdot x) + (\Delta_F(d, d) \oplus F[0] \oplus a \oplus F[d] \oplus A \cdot d) \quad \forall x \in V \oplus d$$

which provides an explicit formula of type $F[x] = B \cdot x + b \quad \forall x \in V \oplus d$ which is exactly the explicit simultaneous linearization property we claimed. □

Corollary. It follows that all the 80 of LAS-2 properties from Eurocrypt 2017 cf. [QSMG17] are also stable by arbitrary translations at the input side. A detailed enumeration shows that they split into two disjoint classes of 40 cosets stable by arbitrary translations and that properties spanned with $15 \cdot 8$ sets DDT() of size 4 and $5 \cdot 4$ sets DDT() of size 8, both cover uniformly the whole set of 80 LAS-2 properties several times.

Observations. Our result is somewhat very surprising, because we have first fully linearized a **non-linear** S-box on a subset, where it is equal to a multivariate linear function with a matrix and a constant, and then we claim that simple transformed variants of our linear property cover the whole space F_2^k several times, very much **as if** the original S-box $F[]$ was linear.

Output Side. This result very rarely holds with output side translations like $y \oplus S[A_{11} \oplus x]$. Moreover, with numerous cryptographic S-boxes we checked, we found that the maximum LSS size of an inverse S-box, is typically strictly lower than the best LSS size for the initial S-box. This with some exceptions when for example the inverse box is quadratic (in Ascon/Keccak the inverse is cubic). A quadratic inverse never happens for any "good" cryptographic S-boxes in size 5, or all S-boxes which are quadratic in both directions are extremely weak, as shown very clearly by comparison of Table 1 and Table 2 in [BoFiPe13].

Violations of Thm. 3. We have verified that our result is NOT true for Thakor and Icepole S-box, which are not quadratic. Therefore these two ciphers could have **better** resistance against various attacks with translations of affine spaces, and with translations of arbitrary sets, and with multiple related simultaneous linear approximations, leading simply to a bigger variety of affine spaces and sets which will be harder to connect together in some attack.

Applications of Thm. 3. Our similarity result of Thm. 3 holds for an overwhelming majority of 5-bit S-boxes used in applied cryptography including SHA-3, SHAKE and Ascon.

8.1 Ascon, Dual or More Low-MC Approximations

An interesting question is, since A_{11} and B_{11} are disjoint, is it possible to combine both these very "simple" entirely linear approximations of the whole S-box, into one single "super-approximation" true with a larger probability of 22/32. A key question is how, and what might be a reasonable way to evaluate the "quality" of such approximations which will no longer be linear. One possible measure of quality could be the MC (Multiplicative Complexity). For example we checked that for 13 points but not more, the whole S-box can be approximated by a function with MC=1. This should have some serious consequences in probabilistic variants of current attacks on Ascon with zero sums and cube distinguishers. In this paper we propose another quality metric for such approximations, and this metric is studied in later Section 12.

8.2 On Unicity of Matrices A

Following on A_{11} and all their shifts, we have checked that these matrices are unique and no more solutions exist. In general these matrices do not have to be unique at smaller sizes. The matrix unicity here is easy with 11 points, however it will not hold for 80 LAS-2 properties from [QSMG17], with 4 points only, the solutions A cannot be unique for just 4 points. Two examples of actual matrices are shown in Section 7 which section also explains that these matrices are invertible in all 30/32 cases except precisely with A_{11} and B_{11} themselves.

8.3 On Affine Dimension of Set of Matrices A

Now we are going to show that the set of matrices A here is much smaller and simpler than expected, and forms an affine space of small dimension. We start by observing that our proof technique for Thm. 3 provides an interesting bonus property and some insights. Let $k = 5$ and consider the Ascon S-box. Here potentially this space of unique matrices could span a linear space of large dimension up to 25. However, in our proof we see that every new matrix is of the form $(\Delta_F(x, d) \oplus A \cdot x)$ discarding any constants. Knowing that Δ_F is bi-linear, we can consider some basis of 5 elements for d, we obtain that our set matrices must be an affine space and has dimension at most 5. In spite of this property, we found that all 32 these matrices are all distinct, for both Ascon and Keccak S-box.

8.4 On Entropy of Constant Parts in A_{11} Approximations

Let us denote by $M^{11}[d]$ a unique matrix such that:

$$F[x] = M^{11}[d] \cdot x + \phi[d] \quad \forall x \in A_{11} \oplus d.$$

where each entry of our 5x5 matrix $M^{11}[d]$ is an affine function of 5 bits of d, and for some "constant part" function $\phi : F_2^5 \to F_2^5$. Then we can observe that in 16 out of 32 cases, the constant $\phi[x] = F[0] = 4$. A similar result is true for Keccak: in half of cases that constant is equal to $0 = F[0]$.

8.5 Almost-Maximal size LSS-10 Properties

It is easy to see that the number of LSS$-m$ properties increases as m goes down. For example, any subset of 10 inside an LSS-11 property form a valid albeit trivial LSS-10 property. In addition we found there exists exactly 5 **non-trivial** LSS-10 properties. They form 5 distinct classes or orbits w.r.t. translations of LSS-10 properties of Ascon. Each these 5 classes generates 32 distinct translations of size 10 following Thm. 3. We list these remarkable sets of 10 here together with a XOR of all elements at output side, which is a translation invariant for all these sets being of even size. We have exactly 5 classes each containing 32 affine shifts:

- 0,1,3,4,5,9,16,19,20,24 $\Sigma_{ou}(V)$=5
- 0,3,4,15,16,17,19,20,21,28 $\Sigma_{ou}(V)$=7
- 0,4,8,11,17,21,23,24,25,27 $\Sigma_{ou}(V)$=14
- 0,2,3,4,12,14,16,19,20,31 $\Sigma_{ou}(V)$=15
- 0,2,4,12,14,16,17,20,21,29 $\Sigma_{ou}(V)$=25

Note. The set of 5 sums $\Sigma_{ou}(V)$ we obtain here is not at all a random set of 5 points, it is the same set which we will later denote by $r^i = \{5, 7, 14, 15, 25\} \subset B_{11}$.

On Matrices Involved. This class of properties leads to $5 \cdot 32 = 160$ distinct approximation matrices. Most of these matrices are invertible however a large number of these are not invertible and of rank 4.

Rotation Invariance of all 160 of non-trivial LSS-10.
It is possible to see that all internal rotations due to embedded Keccak S-box such as say ρ_{in}^2, cf. Table 1, will act on these 5 classes with their shifts, transforming sets of 10 into different sets of 10 from another class. Hence we have obtained 160 LRS-10 properties. It goes without saying that the sums of all elements in these sets are also preserved by rotations, and the set of $r^i = \{5, 7, 14, 15, 25\}$ is stable by our rotations such as type ρ_{in} and their combinations.

Rotation Invariance of LSS-11. In contrast, rotations do not always transform sets of type LSS-11 into other sets of type LSS-11. We have verified that only exactly 2/32 properties of type $A_{11} \oplus b$ obtained from Thm. 2 are invariant by rotations. These 2/32 are also exactly those where approximation matrices are not invertible, cf. Section 7.

On Dual Action and Group Theory Questions. We have a set of 160 sets of 10 points where two transformations: arbitrary translations such as ρ_{in}^2, and arbitrary translations with a XOR with a constant, both act and stay within the same set of 160 properties. It is important to note that shift

Rotations also act at the output side, but translations typically do not work on the output side. We leave for future research the study of the group generated by these two operations. It goes without saying that there are many remarkable identities there to be discovered and this work can be extended to other S-boxes based on Daemen Xi family and other sets of sizes other than 10.

9 Order Emerging From Chaos

It is time to define a new classification of points in Ascon S-box and introduce some new notations. The same exact things could be done for the Keccak S-box. It is important to see that S-boxes in odd size have some interesting properties, and more specifically at size 5 we can have some very unique properties which other S-boxes of size say 6 will not have, or things will be very different there. We claim that there exists a **unique** and natural partitioning of all the 32 points into 6 sets of 5 points and two sets of size 1. The easiest way to define our partitioning is to consider that, buried inside Ascon S-box, is the Keccak S-box which is stable by simultaneous rotation on both sides, i.e. it is SI or Shift-Invariant, see Def. 6.1 page 111 in [DaPhD95]. We simply partition all 32 points into sets stable by rotation.

However, with Ascon things are less simple than with Keccak. tWe have two rotation functions different on each side of the S-box, which were specified in Table 1. At the end we get pairs of rotation-stable sets which are different on each side of the Ascon S-box, which however are the same from the point of view of the Keaccak S-box hidden inside. In the following table we report the input of the Ascon S-box, the output, and two "internal" values: corresponding to input of Keccak S-box which is called Ki, and the output of the Keccak S-box, which is called Ko. In addition in the middle column we report also the XOR of these two values Ki and Ko which quantity we call Kx. To summarize we obtain the following partitioning of Ascon set of 32 states into:

name	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 11. Our special space partitioning in Ascon which corresponds to classes of points stable by rotation for the embedded internal Keccak S-box.

If there is no ambiguity we will denote these sets by single letters a, b, q, r, s, t, y, z. At places where it is not clear on which side of the S-box we are, or when we mix both sides, we will use the exponents such as a^i and a^o to distinguish input and output sides, which is a common notation used in in [CARG19] in the study of non-linear invariant attacks on block ciphers. For example we write

$$t^i = \{4, 12, 16, 17, 19\}$$

If there is no ambiguity we denote by the $S[]$ the Ascon S-box, and we have by definition and by construction:

$$S[a^i] = a^o \quad S[t^i] = t^o \quad \text{etc..}$$

Likewise we are going to also sometimes use a Keccak variants of some sets, to write things like,

$$t^{Ki} = \{1, 2, 4, 8, 16\} \qquad and \qquad t^{Ko} = \{5, 9, 10, 18, 20\}$$

9.1 Initial Observations About Our Sets

All our sets come in pairs, however the pairing is not the same on both sides:

$$a^i = b^i \oplus 26 \oplus 0 \qquad t^i = q^i \oplus 26 \oplus 0 \qquad s^i = r^i \oplus 26 \oplus 0 \qquad y^i = z^i \oplus 26 \oplus 0$$

$$a^o = r^o \oplus S[26] \oplus S[0] \;\; t^o = b^o \oplus S[26] \oplus S[0] \;\; s^o = q^o \oplus S[26] \oplus S[0] \;\; y^o = z^o \oplus S[26] \oplus S[0]$$

In Section 7.1 we discovered that lines in Ascon DDT table can be partitioned into disjoint sets of lines with highly uniform content and properties:

1. 1 line with $\delta_{in} \in y^i$ which contains zeros and 32.
2. 11 lines $\delta_{in} \in z^i \cup q^i \cup a^i$ which contain only 2s.
3. 15 lines $\delta_{in} \in s^i \cup r^i \cup b^i$ which contain only 4s.
4. 5 lines $\delta_{in} \in t^i$ which contain only 8s.

It is further possible to see that content of $DDT()$ sets in various lines can be bijectively mapped to the content of other $DDT()$ sets in other lines of the same class by more or less arbitrary translations of sets by a constant.

We observe that the set $t^i = \{4, 12, 16, 17, 19\}$ which are exactly five input differentials δ_{in} in Ascon of maximum strength (DDT=8). These 5 are also half of 10 known "undisturbed bits" UDB properties in [TeAs16,TeDi19]. There are two special singleton sets y and z stable by translation $0, 26$ which were those involved in flipping between A_{11} and B_{11}. They correspond to two fixed points in Keccak. These two points play an important role and are involved in countless remarkable identities. For example sum of all five values in t^i is $26{=}z^i$. Sum of all five value in t^o is $4{=}y^o$. Similar properties hold for all six classes and on both input and output sides. We can relate these sets to our pair of a unique special maximum size linear spaces called L^i/L^o and discovered in Property B in Section 5, a special and unique partitioning of type 6+10 leading to LIO-63. Then we observe that s is the complement of A_{11} inside L^i excluding the special point. One can define a as a unique set of 5 which is a complement of $S[A11]$ inside our special linear space L^o of dim 4, this at the output side, i.e. $S[a]$ and $S[A11]$ forms a linear space which linear space is actually the same as L^o

9.2 Further Remarkable Identities

Here we define multiple derived sets. For example we write $z^i \oplus b^i$ to enumerate all possible XORs on 5 bits of an element from z on input side, with an element from b on the input side. Given that the origins of these sets is the study of various mappings in Ascon which match other when we translate them by a

constant and in relation to various affine spaces, we frequently obtain sets which can also be obtained in a different way.

Fact 9.1. The reader can verify that the following identities hold:

$$\begin{array}{ll} a^i = z^i \oplus y^i \oplus b^i & a^o = z^o \oplus y^o \oplus r^o \\ q^i = z^i \oplus y^i \oplus t^i & b^o = z^o \oplus y^o \oplus t^o \\ r^i = z^i \oplus y^i \oplus s^i & q^o = z^o \oplus y^o \oplus s^o \end{array}$$

Fact 9.2. There are also many identities which involve basic sets of 11 points.

$$\begin{array}{ll} s^i \cup q^i \cup y^i = b^i \oplus b^i & r^i \cup t^i \cup z^i = a^i \oplus b^i \\ b^i \cup q^i \cup y^i = s^i \oplus s^i & a^i \cup t^i \cup z^i = r^i \oplus s^i \\ s^i \cup b^i \cup y^i = q^i \oplus q^i & r^i \cup a^i \cup z^i = t^i \oplus q^i \end{array}$$

which bears some similarity and could be compared to:

$$\begin{array}{ll} A^i_{11} = s^i \cup t^i \cup y^i & B^i_{11} = q^i \cup r^i \cup z^i \\ A^o_{11} = s^o \cup t^o \cup y^o & B^o_{11} = q^o \cup r^o \cup z^o \end{array}$$

Fact 9.3. Many more such identities exist with XORs of 3 elements, many of which also give sets of exactly 11 points:

$$\begin{array}{ll} a^o \cup s^o \cup y^o = t^o \oplus t^o \oplus y^o & b^o \cup q^o \cup z^o = r^o \oplus r^o \oplus z^o \\ a^o \cup t^o \cup y^o = s^o \oplus s^o \oplus y^o & b^o \cup r^o \cup z^o = q^o \oplus q^o \oplus z^o \\ t^o \cup s^o \cup y^o = a^o \oplus a^o \oplus y^o & r^o \cup q^o \cup z^o = b^o \oplus b^o \oplus z^o \end{array}$$

$$\begin{array}{ll} a^i \cup r^i \cup z^i = t^i \oplus t^i \oplus z^i & s^i \cup q^i \cup y^i = b^i \oplus b^i \oplus y^i \\ a^i \cup t^i \cup z^i = r^i \oplus r^i \oplus z^i & s^i \cup b^i \cup y^i = q^i \oplus q^i \oplus y^i \\ r^i \cup t^i \cup z^i = a^i \oplus a^i \oplus z^i & b^i \cup q^i \cup y^i = s^i \oplus s^i \oplus y^i \end{array}$$

$$\begin{array}{ll} r^o \cup b^o \cup z^o = q^o \oplus q^o \oplus z^o & s^o \cup a^o \cup y^o = t^o \oplus t^o \oplus y^o \\ q^o \cup b^o \cup z^o = r^o \oplus r^o \oplus z^o & s^o \cup t^o \cup y^o = a^o \oplus a^o \oplus y^o \\ r^o \cup q^o \cup z^o = b^o \oplus b^o \oplus z^o & t^o \cup a^o \cup y^o = s^o \oplus s^o \oplus y^o \end{array}$$

Many more similar identities exist with longer XORs of various sets.

Fact 9.4. For example here are some identities involving 16 points:

$$\begin{array}{ll} a^i \oplus a^i \oplus a^i = r^i \cup t^i \cup a^i & a^o \oplus a^o \oplus a^o = t^o \cup s^o \cup a^o \\ r^i \oplus r^i \oplus r^i = a^i \cup t^i \cup r^i & r^o \oplus r^o \oplus r^o = q^o \cup b^o \cup r^o \\ s^i \oplus s^i \oplus s^i = q^i \cup b^i \cup s^i & s^o \oplus s^o \oplus s^o = t^o \cup a^o \cup s^o \\ b^i \oplus b^i \oplus b^i = s^i \cup q^i \cup b^i & b^o \oplus b^o \oplus b^o = q^o \cup r^o \cup b^o \\ q^i \oplus q^i \oplus q^i = s^i \cup b^i \cup q^i & q^o \oplus q^o \oplus q^o = r^o \cup b^o \cup q^o \\ t^i \oplus t^i \oplus t^i = r^i \cup a^i \cup t^i & t^o \oplus t^o \oplus t^o = a^o \cup s^o \cup t^o \end{array}$$

Fact 9.5. More remarkable identities: with A_{11} and B_{11} there are more substantial differences about what happens on each side [input/output].

$$A^i_{11} = s^i \cup t^i \cup y^i \qquad B^i_{11} = q^i \cup r^i \cup z^i$$
$$A^o_{11} = s^o \cup t^o \cup y^o \qquad B^o_{11} = q^o \cup r^o \cup z^o$$
$$A^i_{11} \cup s^i \cup t^i = B^i_{11} \oplus z^i \qquad B^i_{11} \cup q^i \cup r^i = A^i_{11} \oplus z^i$$
$$A^i_{11} \oplus A^i_{11} = F_2^5 \setminus 26 \qquad B^i_{11} \oplus B^i_{11} = F_2^5 \setminus 26$$
$$A^o_{11} \oplus A^o_{11} = a^o \cup s^o \cup t^o \cup y^o \qquad B^o_{11} \oplus B^o_{11} = a^o \cup s^o \cup t^o \cup y^o$$
$$A^o_{11} = a^o \cup a^o \cup y^o \qquad B^o_{11} = b^o \cup b^o \cup z^o$$
$$A^o_{11} = a^o \cup r^o \cup z^o \qquad B^o_{11} = b^o \cup t^o \cup y^o$$
$$A^o_{11} \cup a^o = A^o_{11} \oplus A^o_{11} = B^o_{11} \oplus B^o_{11}$$
$$B^o_{11} \cup b^o = B^o_{11} \oplus a^o = A^o_{11} \oplus B^o_{11}$$

There are many other interesting observations about these 6 sets of 5 points.

Fact 9.6.i. At input side sets t^i, a^i, r^i form a basis for the whole space and the other three do not form a basis and their sum is 0. Together, these 16 elements $s^i + b^i + q^i + y^i$ form a linear space of maximum dimension 4 known as L^i in Property B of Section 5, with $\alpha = 20 = \rho_{in}[31]$, with $L^i_B = \{0, 1, 2, 3, 8, 9, 10, 11, 20, 21, 22, 23, 28, 29, 30, 31\}$ and its elements are exactly all the unions of 0,2 or 4 distinct elements of t^i.

Fact 9.6.o. At output side sets b^o, r^o, q^o form a basis for the whole space and the other three do not form a basis and their sum is $S[0]$ and together these 16 elements $a^o + s^o + t^o + y^o$ form a linear space of maximum dimension 4 known as L^o in Property B of Section 5 with $\beta = 11 = \rho^{-1}_{ou}[31]$, with $L^o_B = \{0, 3, 4, 7, 9, 10, 13, 14, 16, 19, 20, 23, 25, 26, 29, 30\}$ and its elements are exactly all the unions of 1,3 or 5 distinct elements of t^o.

We now consider some remarkable identities which are mixing "apples and oranges": sets and affine spaces from both I/O sides of the S-box. This type of properties could be exploited in some invariant attacks (yet to be discovered). We call I the intersection of the 2 remarkable spaces of dimension 4 above.

Fact 9.7. We have $I = \{0, 3, 9, 10, 20, 23, 29, 30\}$. This space I creates a partitioning of the whole set of 32 points into 4 affine spaces or cosets which are:

name	either side
I	0,3,9,10, 20,23,29,30
J	1,2,8,11, 21,22,28,31
K	4,7,13,14 16,19,25,26
L	5,6,12,15 17,18,24,27

It is hard to imagine that these sets of 8 can align well with various sets of 5, while mixing both sides of the S-box, however there are still some remarkable identities at size 16 to report:

$$L^i_B = I \cup J = s^i \cup q^i \cup b^i \cup y^i \qquad K \cup L = a^i \cup t^i \cup r^i \cup z^i$$
$$S[I] \cup S[J] = s^o \cup q^o \cup b^o \cup y^o \qquad S[K] \cup S[L] = a^o \cup t^o \cup r^o \cup z^o$$
$$L^o_B = I \cup K = a^o \cup s^o \cup t^o \cup y^o \qquad J \cup L = b^i \cup q^i \cup r^i \cup z^i$$

9.3 Keccak Only Section

We should also observe the following: Keccak S-box has two fixed points y^{Ki} and z^{Ki} and all other points can be ordered in two cycles of size 2 and 4 operating on sets of 5 bits as follows:

$$a^{Ki} \mapsto q^{Ki} \mapsto a^{Ki} \qquad\qquad b^{Ki} \mapsto r^{Ki} \mapsto t^{Ki} \mapsto s^{Ki} \mapsto b^{Ki}$$

$$\{7, 14, 19, 25, 28\} \mapsto \{15, 23, 27, 29, 30\} \mapsto \{7, 14, 19, 25, 28\}$$

$$\{3, 6, 12, 17, 24\} \mapsto \{11, 13, 21, 22, 26\} \mapsto \{1, 2, 4, 8, 16\} \mapsto \{5, 9, 10, 18, 20\} \mapsto \{3, 6, 12, 17, 24\}$$

Ascon does no longer have any comparable cycling properties. However we can construct multiple derived functions such as

$$x \mapsto S^{-1}[\ S[\ x\ ] \oplus 5\ ]$$

and such functions have short cycles operating on sets of size 5.

10 Comparison to Other Quadratic Permutations

There exist exactly 75 affine equivalence classes of quadratic permutations on 5 bits, cf. Table 1 in [BoBiSa17], and Ascon/Keccak S-box belongs to class 68. Is the Ascon/Keccak S-box A_{11} property a typical case or is it a particularly weak quadratic permutation? We have run our SAT solver tool on all 75 classes from [BoBiSa17] and looked at the maximum size set LSS. In most cases these S-boxes are substantially weaker than Ascon and Keccak, direct comparison makes little sense, and no one would agree to use such S-boxes in cryptography. Therefore we restrict our study to all classes out of 75 where $DMI(\delta_{in};\delta_{ou}) \leq 2.2$ bits knowing that in Ascon/Keccak we have $DMI = 1.91$ and $DMI = 1.12$ in the best case. The results obtained with two independent implementations of our tool are reported below in Table 12. These results are optimal and cannot be improved.

Other S-boxes. We have not included Thakor and Icepole because these S-boxes are not quadratic. For these S-boxes LSS=11, same as in Ascon/Keccak.

classes	also known as	best LSS size	max DTT size	MC	$DMI(\delta_{in};\delta_{ou})$
28,36		13	16	5	2.16
52,56,58		11	16	5	2.06
58		11	16	5	2.06
61,62,65		11	8	6	2.06
47		10	16	5	1.97
59		11	8	5	1.94
68	Ascon,Keccak	11	8	5	1.91
53,70		11	8	5	1.88
57		10	8	6	1.78
69		10	8	6	1.72
63,64		9	8	6	1.69
71		10	4	6	1.69
72		9	4	5	1.59
66		10	8	6	1.56
67		9	8	6	1.56
73		8	4	6	1.41
75		7	2	7	1.12
74	Fides,Primates	7	2	8	1.12

Table 12. Maximum size LSS properties for all cryptographically "not too weak" equivalence classes of quadratic permutations on 5 bits according to [BoBiSa17].

Analysis. In Table 12 it is possible to see that the maximum LSS property size behaves in a highly regular way and could be actually quite reliably predicted from the value of DMI. We observe that LSS-11 property occurs for S-boxes with $1.88 \leq \text{DMI} \leq 1.94$. We must conclude that LSS-11 property is **a typical property of an S-box with** $DMI \approx 1.9$.

Remark. In spite of the fact Ascon S-box has some rotational symmetries which other S-boxes do not have, and the value Kx inside this S-box is biased, not uniformly distributed and always has a small HW, the results in Table 12 do not confirm the idea that Ascon S-box would be very special or weaker than other comparable S-boxes.

Comparison with DDT Sets. An interesting transition occurs in our table: in the upper part, best LSS properties are not as large as best DDT() sets, which means that we **can hardly expect**, even in the worst case, that very large sets obtained from DDT can be fully linearized in a LSS property. We can eventually hope that, as observed above, DDT() sets are supersets [or disjoint unions] of LSS sets. We then expect that for such (weaker) s-boxes, traditional DC with single differentials will perform well. Then for most of cryptographically significant S-boxes, roughly in the lower half of Table 12, best LSS size can be substantially larger than best DDT() size. Here, while there is hope to break these ciphers by simple DC, the attacker should try to exploit combinations of LSS properties and also some closely related [weaker] differential properties which can be sometimes amplified by such subsets, cf. Section 12.

Can We Do Better? Ascon and Keccak cipher could be made arguably and measurably more secure against simultaneous linear approximation attacks, by changing the S-box to an S-box in classes 74/75, or rather a well-chosen affine equivalent without any BI or BO properties [LMCFW23], and with a low ASIC implementation depth.

11 ASIC Implementation Considerations

In this paper we intend to study and evaluate several S-boxes not only on security w.r.t. some new precise differential and linear security metric, but also on an ASIC implementation cost metric. This as a first approximation and [for now] without considering side channels or/and threshold implementations [BGST23].

In Table 12 we already studied the MC (Mutliplicative Complexity) metric [BoPePo00] which is expected to "heuristically" approximate the overall ASIC cost, cf. [BoPe10]. Another important heuristic is the number of high degree monomials, cf. [BGST23]. Here we do not have any high degree monomials therefore we will try to approximate ASIC cost by the overall number of homogeneous quadratic monomials with multiplicity. For example if a monomial say x_2x_3 appears twice in say y_0 and y_2, we count it twice. We call "hom-MQ size" this total number of quadratic terms in a any given S-box.

In the table which follows we are going to study whole classes of S-boxes and also compare them to existing individual S-boxes. In order to avoid comparison of apples and oranges, we write *68* for a whole class of S-boxes known as 68 in [BoBiSa17], with two stars which correspond to our ability to add two arbitrary affine transformations on the input and output side. Finally we write just Ascon/Fides if there is no modification to an existing S-box.

At this moment we only report results where $DMI(\delta_{in};\delta_{ou}) \leq 2.2$ bits. We conjecture that the combination of best LSS size, our hom-MQ metric and the classical MC metric allow to predict and anticipate with great precision the

actual GE (Gate Equivalent) cost of silicon with best available tools. We also conjecture that the GE cost is roughly proportional to our hom-MQ metric, while the older MC metric is simply not precise enough to be used in practice as a tool for predicting the ASIC cost, and in rare cases it is inaccurate and misleading. Our ASIC implementation results are presented in Table 13 below.

classes	best LSS	min(hom-MQ size)	MC	DMI
28	13	5	5	2.16
36	13	6	5	2.16
52	11	7	5	2.06
62	11	8	6	2.06
56,*58*	11	8	5	2.06
61,*65*	11	9	6	2.06
47	**10**	**8**	5	1.97
59	11	8	5	1.94
Ascon	11	11	5	1.91
68,*Ascon*,*Keccak*	**11**	**10**	5	1.91
53	11	10	5	1.88
70	11	12	5	1.88
63	9	11	6	1.69
71	10	13	6	1.69
72	9	13	5	1.59
66	10	11	6	1.56
67	9	13	6	1.56
73	8	14	6	1.41
75	7	14	7	1.12
74,*Fides*,*Inv*	7	15	8	1.12
Fides	7	18	8	1.12

Table 13. Comparison of LSS, MC and our [simplified] ASIC implementation cost metric for various S-boxes on 5 bits and full classes with affine equivalence

Note. Our ASIC cost metric is not an ideal one, it inly applies to quadratic S-boxes. We can of course count cubic monomials like in [BGST23], or degree 4 monomials in S-boxes from [MeBi19], however it is hard with method to compare an ASIC implementation cost of two S-boxes which do not have the same degree. One solution to this problem is to consider the "latency complexity" metric defined in [LatRa22]

12 Study of DDT and DMI Limited to Specific Sets

In Section 7.1 we discovered that our subsets of 11 points have exceptionally large coverage of 6/8 of the points which should interest the attacker the most: those involved in DDT() sets of maximum size 8/32. In this section we define a **more precise** methodology in order to compare quality of arbitrary sets of point from a purely differential cryptanalysis point of view. This inspiration for this work is the Table 12 above, where we see that DMI seems to a very decent overall measure of a quality of an S-box, and reproduces the ordering of S-boxes of Table 1 in [BoBiSa17] in a very predictable and near-monotonous way from weaker to stronger. In comparison the authors [BoBiSa17] have classified the S-boxes by 3 key parameters based on 3 most prominent notions of "non-linearity", which are [the sizes of] DDT,LUT and MC, cf. [BoFiPe13] and we obtain a simpler yet very similar classification.

It is easy to see that the classical mathematical definition of DMI which can be found in wikipedia [wikiMI] applies also to arbitrary subsets of points, see Definition 8 in page 6. This amounts to the we study DDT restricted all pairs x, x' inside a subset S. We get therefore a yet more precise measure of overall quality of an S-box w.r.t. differential cryptanalysis provided that the attacker is indeed able to achieve a certain peculiar probability distribution for a set of points. This leads to a new refined optimization problem in cryptanalysis which is very closely related to almost everything we do in this paper.

Definition 12 (DMI Profile of an S-box for Arbitrary Probability Distributions). *For every $H \leq 5$ bits, what is a probability distribution with input Shannon entropy H, which maximizes the value $MI(\delta_{in}; \delta_{ou})$ and what is the highest possible value of DMI? We call a graph representing all possible pairs H, DMI_{max} the DMI Profile of an S-box.*

The computation of the profile defined above is extremely difficult and can only be approximated. We define:

Definition 13 (Simplified DMI Profile of an S-box with Arbitrary Subsets:). *For every $n \leq 2^5$, and assuming uniform distribution inside a set S of n values out of 2^k, we call the "Simplified DMI Profile" a graph made with pairs (n, DMI_{max}) where DMI_{max} is the maximum of*

$$MI(\delta_{in}; \delta_{ou} | x; x' \in S)$$

over all possible sets of size $\#S = n$.

In the table below we display some values which compare the Simplified DMI Profile of Fides and Ascon/Keccak S-boxes.

LSS size	7-9	10-15	16-19	20-22
Xi/Ascon/Keccak	4.375	4.806	3.808	2.999
Fides/Primate/InvGF32	4.357	4.046	3.124	2.482

Table 14. Simplified DMI Profile for two S-boxes.

Interpretation of Results. We claim that the Simplified DMI Profile provides a precise and robust measure of vulnerability of an S-box against Differential Cryptanalysis when restricted to sets of n distinct values. It is also possible to see that for each S-box there exists an optimal size which maximizes this quantity. This does not however mean that this is the value on which the attacker should concentrate his algorithmic efforts. It is not easy to see if 2.99/5.0 of bits of shared information between input and output differences for a property which is true for a large fraction of 22/32 of the whole space, would advantage the attacker more; than the very impressive 4.8/5.0 bits of shared information for a property concerning a substantially smaller fraction of 11/32 the whole space.

Open Problems. The values reported in this table were obtained in a long GPU computation on the best effort basis and are not guaranteed to be optimal at the moment. It is an open problem to design an efficient optimized algorithm to compute the Simplified DMI Profile of an S-box. In practice it can be approximated by some heuristics such as for example considering unions of various affine spaces, DDT() sets, LSS sets, sets related to LAT, etc.

13 Conclusion

The main topic of this paper is the discovery of the strongest possible simultaneous linear approximations of a cryptographic S-box. We focus in particular on the peculiar S-box called Xi and used in Ascon, Keccak and many other ciphers, and few other comparable S-boxes. At Eurocrypt 2017 researchers have constructed collisions on up to 6 rounds of Keccak with so called "connectors"'. These connectors exploit a set of 80 partial linearization LAS properties with 4 points which form an affine space of dim 2 on both sides. The same LAS properties also work for Ascon.

In this paper, starting from observations about further remarkable sets involved in a variety of simultaneous linear, differential and translation properties, we have generalized and extended previous work in several ways. The notion of of functional approximations (LAS) within affine spaces was extended to consider to sets of arbitrary points (LSS) and to the study of arbitrary linear I/O relations which are no longer functions (LIO). In this new framework, the classical question of repeated affine spaces with applications in cryptanalysis is extended and becomes the study of pairs of sets equivalent by a translation with a constant. We have done an exhaustive study of how pairs of maximum dimension affine spaces can approximate the Ascon S-box and exhibit several interesting sets and spaces which maximize the number of linear I/O relations. Our new functional approximations are optimal and the strongest possible.

13.1 Summary of Results

It is possible to be surprised by how frequently different sets of points such $DDT()$ sets and all sets related to LAT are related to each other by translation, cf. Table 5, Table 15 and Table 17. Some of these properties are explained by internal hidden rotational symmetry of the Xi/Keccak S-box. Some other are related to our LSS-k translation property of Thm. 3. Other are not LSS, and will still be similar to (fewer) other sets. All these suggest that cryptanalysis with arbitrary subsets of points is in fact less complex than it seems with 5-bit S-boxes. For random S-boxes, even at size 5, translation properties happen very rarely or only by coincidence, and typically not all, cf. Table 7 and Table 12. Zero translation similarities like those those studied here occur with the AES S-box (size 8).

In our research we have studied many natural ways of approximating our S-box by linear functions, or LIO relations, or by linearity when restricted to subsets, and found many new properties at sizes 6,8,10,11 and 12 which are stronger, more general and **larger** than those previously studied. Our best result is a class of "maximal" linear approximation properties with as many as 11 points, cf. Thm. 2, which is optimal. We have shown that arbitrary translations of such sets give equally strong full matrix+vector linearization LZS-11 properties. This result holds for **all** quadratic S-boxes cf. Thm. 3, and therefore for an overwhelming majority of 5-bit S-boxes used in practical applications [Ascon,SHA3,SHAKE,etc..], but not in Thakor/Icepole.

We also observed that mutual intersections between various translations of our maximum size set, are in a one to one correspondence with the set of all lines of the DDT table of Ascon classified by relative strength.

13.2 Is There Anything Wrong With Ascon or Keccak?

A detailed analysis based on a classification of all quadratic permutations, shows however that it is not possible to claim that Ascon or Keccak S-box are special or dangerous or worse than other quadratic S-boxes. In fact Table 12 demonstrates very clearly that they behave like typical quadratic S-boxes with $DMI \approx 1.9$ and a cubic inverse.

The only reasonable way to make these ciphers **arguably and measurably more secure** is to use an S-box with lower DMI. Here $DMI \approx 1.1$, and LSS=7 is the best property we can hope for. This is optimal, and we confirmed that APN and few other boxes are strongest possible. Here with respect to a new "global" security notion based on simultaneous linear approximations such as LSS. In Table 13 we show that though reducing max LSS size very slightly to 10 is possible with classes 68 and 47. Then we see that reducing it further is impossible with quadratic permutations at size 5, without increasing the expected ASIC area / implementation cost by up to 50%. In addition this paper provides new arguments which suggest to mistrust all quadratic S-boxes in general, see Thm. 3, and switch to the likes of Thakor and Icepole or to 4-17 quartic type. An open problem is to find yet better S-boxes with LSS$<$ 11 and similar or better ASIC implementation cost.

13.3 Future Research

These properties are expected to lead many new ways of attacking Ascon with a mix of linear and differential properties where the S-boxes will be (under certain conditions) modeled by linear equations and where differentials act in predictable ways [or/and with quite large probabilities]. It is possible to see that best known attacks on Ascon,Keccak and many other ARX ciphers are differential-linear attacks, cf. for example [TeDi19,HaDeEi24]. We postulate that attackers need to construct and find new forms of invariant differential-linear attacks, combined with state partitioning with sets of certain type, which will be very different than any currently known differential-linear attacks [with connectors] where differential and linear properties occurred in different and disjoint parts of the cipher.

One example of how an invariant attack with affine spaces can work together with predictable differentials at every round inside one single attack can be found in [CoQi20]. Future work should try to construct similar attacks which would no longer use perfect affine spaces but rather more irregular sets.

References

[BGST23] Anubhab Baksi, Sylvain Guilley, Ritu-Ranjan Shrivastwa, Sofiane Takarabt: *From Substitution Box To Threshold,* At https://eprint.iacr.org/2023/633.pdf.

[BiCaQu04] Alex Biryukov, Christophe De Cannière, and Michael Quisquater: *On Multiple Linear Approximations,* In eprint.iacr.org/2004/057.

[BoFiPe13] Joan Boyar, Magnus Find, and René Peralta: *Four measures of nonlinearity,* In CIAC, LNCS 7878, pp. 61-72, 2013.

[BoPePo00] Joan Boyar, René Peralta, and Denis Pochuev. *On the multiplicative complexity of Boolean functions over the basis (∧,⊕,1).* In Theor. Comput. Sci., 235(1):4357, 2000.

[BoPe10] Joan Boyar and René Peralta: *A new combinational logic minimization technique with applications to cryptology,* In SEA, LNCS 6049, pp. 178189, 2010.

[DaPhD95] Joan Daemen: *Cipher and Hash Function Design Strategies based on linear and differential cryptanalysis,* PhD thesis, March 1995, reformatted in January 2004.

[PaGo98] Jacques Patarin, Louis Goubin, Nicolas T. Courtois: *C*-+ and HM: Variations Around Two Schemes of T. Matsumoto and H. Imai.* In Asiacrypt 1998, LNCS 1514, pp. 35-49, October 1998.

[BoBiSa17] Dušan Božilov, Begül Bilgin and HacıAli Şahin: *A Note on 5-bit Quadratic Permutations' Classification,* In TOSC 2017 Iss. 1, pp. 398-404, March 2017.

[CoDe08] Nicolas T. Courtois, Blandine Debraize: *Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0.* In ICICS 2008: pp. 328-344, October 2008.

[CARG19] Nicolas T. Courtois, Matteo Abbondati, Hamy Ratoanina, Marek Grajek: *Systematic Construction of Nonlinear Product Attacks on Block Ciphers,* In ICISC 2019, pp. 20-51, Springer LNCS 11975, 2019.

[CoQi20] Nicolas T. Courtois, Jean-Jacques Quisquater: *Can a Differential Attack Work for an Arbitrarily Large Number of Rounds?,* In ICISC 2020, pp. 157181, Springer, 2020.

[CoPoSc08] Nicolas Courtois, Maria Bristena Oprisanu, and Klaus Schmeh: *Linear cryptanalysis and block cipher design in East Germany in the 1970s,* In Cryptologia, volume 43, issue 1, pp. 2-22, December 2018.

[CoGr22] Nicolas T. Courtois, Marek Grajek, *On latin squares, invariant differentials, random permutations and historical Enigma rotors,* In Cryptologia, vol. 46, issue 5, pp. 387-421, December 2021.

[CSDPOSB17] Nicolas T. Courtois, Klaus Schmeh, Jrg Drobick, Jacques Patarin, Maria-Bristena Oprisanu, Matteo Scarlata, and Om Bhallamudi: *Cryptographic Security Analysis of T-310,* In eprint.iacr.org/2017/440.pdf, last revised in March 2019.

[FeHAPa21] Neranga Fernando, Sartaj Ul Hasan, Mohit Pal: *Dembowski-Ostrom polynomials and reversed Dickson polynomials,* arxiv.org/abs/1905.01767, May 2021.

[GJNQSS16] Jian Guo, Jérémy Jean, Ivica Nikolić, Kexin Qiao, Yu Sasaki, Siang Meng Sim: Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs. In TOSC 2016, No. 1, pp. 3-56, Springer.

[HaDeEi24] Hosein Hadipour, Patrick Derbez and Maria Eichlseder: *Revisiting Differential-Linear Attacks via a Boomerang Perspective with Application to AES, Ascon, CLEFIA, SKINNY, PRESENT, KNOT, TWINE, WARP, LBlock, Simeck, and SERPENT,*

[HuCu24] Kai Hu: *Improved Conditional Cube Attacks on Ascon AEADs in Nonce-Respecting Settings – with a Break-Fix Strategy,* eprint.iacr.org/2024/743, May 2024.

[LiIsMeYa21] Fukang Liu, Takanori Isobe, Willi Meier & Zhonghao Yang: *Algebraic Attacks on Round-Reduced Keccak,* In ACISP 2021, Springer LNCS 13083, pp. 91110.

[LMCFW23] Zhenyu Lu, Sihem Mesnager, Tingting Cui, Yanhong Fan, Meiqin Wang, *An STP-based model toward designing S-boxes,* eprint.iacr.org/2023/1023.pdf

[MaTe14] Rusydi H. Makarim1 and Cihangir Tezcan: *Relating Undisturbed Bits to Other Properties of Substitution Boxes,* eprint.iacr.org/2014/855

[MeBi19] Lauren De Meyer, Begül Bilgin: *Classification of Balanced Quadratic Functions,* In TOSC 2019 vol 2, pp. 169192, June 2019.

[QSMG17] Kexin Qiao, Ling Song, Meicheng Liu, and Jian Guo: *New Collision Attacks on Round-Reduced Keccak,* eprint.iacr.org/2017/128.pdf, April 2017. Minor revision w.r.t. Eurocrypt 2017, pp 216243, LNCS 10212.

[LatRa22] Shahram Rasoolzadeh: *Low-Latency Boolean Functions and Bijective S-boxes,* In TOSC 2022, No 3, pp: 403-447, Sept. 2022.

[TeDi19] Cihangir Tezcan: *Distinguishers for Reduced Round Ascon, DryGASCON, and Shamash Permutations,* In NIST Lightweight Cryptography Workshop, 2019. https://www.nist.gov/news-events/events/2019/11/lightweight-cryptography-workshop-2019

[TeAs16] Cihangir Tezcan: Truncated, Impossible, and Improbable Differential Analysis of ASCON, International Conference on Information Systems Security and Privacy, December 2016

[wikiMI] Wikipedia article: *Mutual Information*, en.wikipedia.org/wiki/Mutual_information, consulted 3 May 2024.

A More Translation Invariance with 961 Pairs in LAT

In this paper we have seen that one major weakness of Ascon S-box was the fact that the A_{11} property does not exist in isolation, but is stable by arbitrary translations. This is our **first holographic property** cf. Thm. 3. For example, an attacker is trying to manipulate the state of one S-box in order to make sure it will be one of the 11 values. Then we have an applications of a secret constant such as a cryptographic key, or a public constant such as the round constant in Ascon equal to 0x4 at one S-box. In spite of this, we obtain a related set with a similar property. Finally we will maybe even obtain the exact same configuration after a few rounds in some [hypothetic] periodic invariant attack. Now and again, with Thm. 3 this property is less exceptional than it seems, and it actually holds for all LSS properties of any size, and for all quadratic S-boxes.

Another interesting set of translation similarities was studied in Section 4 and in Table 5. We saw that in 336+40 cases and in all cases without exception which are unbalanced, i.e. not of type 8+8, two pairs of sets are equivalent by [just one] translation constant. This is our **second holographic property**. We have also seen that this did not happen **at all** for Thakor. We are going to see that such undesirable properties happen for all small size quadratic S-boxes used in cryptography (but not for larger sizes). Following Section 4 we recall the main motivation of this exercise:

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?

This leads to different ways of partitioning of 32 elements into 2+2 disjoint sets like 6+10+6+10 or similar. It would also be interesting to see how many entries of different type we see, which is essentially about relative frequencies of different entries in the LAT table. We show some further detailed results of this type in Table 15 below.

S-box	all	8+8	7+9	6+10	5+11	4+12	0+16	DMI
28	961	702	0	192	0	**128**	0	2.16
inp-shifted		474	0	192	0	**128**	0	
unrelated		228	0	0	0	0	0	
47	961	552	0	384	0	48	0	1.97
inp-shifted		174	0	384	0	48	0	
unrelated		378	0	0	0	0	0	
60	961	648	0	256	0	56	0	2.34
inp-shifted		366	0	256	0	56	0	
unrelated		282	0	0	0	0	0	
68,Ascon	961	585	0	336	0	40	0	1.91
inp-shifted		240	0	336	0	40	0	
unrelated		345	0	0	0	0	0	
70,69,71	961	585	0	336	0	40	0	1.88,
inp-shifted		240	0	336	0	40	0	1.72,
unrelated		345	0	0	0	0	0	1.69
67,66	961	585	0	336	0	40	0	1.56
inp-shifted		240	0	336	0	40	0	
unrelated		345	0	0	0	0	0	
72	961	525	0	416	0	40	0	1.59
inp-shifted		120	0	**416**	0	40	0	
unrelated		405	0	0	0	0	0	
73	961	501	0	448	0	24	0	1.41
inp-shifted		72	0	**448**	0	4	0	
unrelated		429	0	0	0	0	0	
74,75,Fides	961	465	0	496	0	0	0	1.12
inp-shifted		0	0	**496**	0	0	0	
unrelated		465	0	0	0	0	0	
Icepole	961	435	220	240	36	30	0	1.82
inp-shifted		120	10	160	6	20	0	
unrelated		315	210	80	30	10	0	
Thakor	961	270	420	196	60	15	0	1.59
inp-shifted		0	0	0	0	0	0	
unrelated		**270**	**420**	**196**	**60**	**15**	0	

Table 15. Pairs of spaces of the same size which happen to be equivalent by translation [vs. just unrelated sets of the same size] in several S-boxes and their affine equivalents.

B Focus on Stronger S-boxes - Not Quadratic

In Table 7 in [MeBi19] we find a list of 17 particularly strong quartic (degree 4) permutations on 5 bits. Here below we analyze their vulnerability to translation self-similarity properties with pairs of hyperplanes, as studied above and in Section 4. We recall some of the strongest S-boxes in this set and to avoid confusion with previous class numbers, we pre-pend 4- to the numbers used in Table 7 in [MeBi19].

sbox	specification
4-11	0,1,2,3,4,6,8,12,5,11,16,24,22,26,9,19,7,23,10,13,31,18,20,29,27,30,28,15,14,17,21,25
4-12	0,1,2,3,4,6,8,12,5,13,16,23,17,18,24,11,7,29,21,27,25,9,22,10,31,14,15,20,19,30,28,26
4-13	0,1,2,3,4,6,8,12,5,14,16,26,10,27,23,31,7,24,11,28,20,17,9,18,25,21,13,30,15,22,29,19
4-14	0,1,2,3,4,6,8,12,5,16,13,23,25,21,26,14,7,17,20,28,29,19,11,9,15,10,31,24,27,18,30,22
4-15	0,1,2,3,4,6,8,12,5,16,21,26,31,22,18,10,7,24,17,13,30,14,19,27,20,9,23,25,11,29,15,28
4-16	0,1,2,3,4,6,8,16,5,10,20,29,7,31,27,13,9,25,15,18,19,14,22,26,21,17,11,12,30,28,23,24
4-17	0,1,2,4,3,6,8,16,5,10,15,27,19,29,31,20,7,18,25,21,12,14,24,28,26,11,23,13,30,9,17,22
Fides	1,0,25,26,17,29,21,27,20,5,4,23,14,18,2,28,15,8,6,3,13,7,24,16,30,9,31,10,22,12,11,19

Table 16. The top or the strongest quartic S-boxes according to Table 7 in [MeBi19].

More Translation Properties - 8li8 and 8ci8. In Table 17 below, we introduce and study new types of translation properties, which will sometimes denote by a shorthand notation **8li8** and **8ci8** and which exist only in size 8, and which are different than 8+8 similarity studied so far. In essence, the 8+8 property was to see how many times for different pairs of hyperplanes out of 961, we get two sets in one diagonal inside Def. 11, like for example:

$S^{-1}[L^o] \cap L^i$

$$co - S^{-1}[L^o] \cap co - L^i$$

which are related by a translation and were studied in Thm. 1 page 12. In contrast, the 8li8 property occurs when two sets in the 1st column are related by a translation, which sets are exactly:

$S^{-1}[L^o] \cap L^i$

$co - S^{-1}[L^o] \cap L^i$

Furthermore we denote by 8ci8 the number of pairs of hyperplanes out of 961 when this happens in the 2nd column of our table of Def. 11.

Note. These events 8li8 and 8ci8 happen only for balanced partitions where the sizes of all 8 sets are the same. We do not report when it happens that two sets in the same line are related by translation. This happens less frequently in general, and this information can be entirely deduced from 8+8 and 8ci8 and 8co8 values displayed below.

B.1 Translation Similarity with Larger S-boxes

We have examined all top 8 or the so-called "strong" 6-bit quadratic permutations listed in Table 15 in [MeBi19]. They all have the same characteristics with $DMI = 2.06$ and max $DDT()$ size of 8. All these permutations give the same

S-box	best LSS	8ci8	8li8	8+8	7+9	6+10	5+11	4+12	0+16	DMI
28	13	702	702	702	0	**192**	0	**128**	0	2.16
inp-shifted		**702**	**702**	**474**	0	**192**	0	**128**	0	
unrelated		0	0	228	0	0	0	0	0	
68,Ascon	11	585	585	585	0	336	0	40	0	1.91
inp-shifted		585	585	240	0	336	0	40	0	
unrelated		0	0	345	0	0	0	0	0	
73	8	501	501	501	0	448	0	24	0	1.41
inp-shifted		501	501	**72**	0	448	0	4	0	
unrelated		0	0	448	449	0	0	0	0	
74,75,Fides	7	465	465	465	0	496	0	0	0	1.12
inp-shifted		465	465	**0**	0	**496**	0	0	0	
unrelated		0	0	465	0	0	0	0	0	
Icepole	11	435	435	435	220	240	36	30	0	1.82
inp-shifted		435	315	120	10	160	6	20	0	
unrelated		0	120	315	210	80	30	10	0	
Thakor	11	270	270	270	420	196	60	15	0	1.59
inp-shifted		61	62	0	0	0	0	0	0	
unrelated		209	208	270	420	**196**	**60**	**15**	0	
4-13	9	245	245	245	410	236	140	0	0	1.36
inp-shifted		29	31	0	0	**16**	0	0	0	
unrelated		216	214	245	410	220	**140**	0	0	
4-11	10	215	215	215	435	250	122	0	0	1.30
inp-shifted		12	13	0	0	0	0	0	0	
unrelated		203	202	215	435	250	122	0	0	
4-15	9	215	215	215	435	250	122	0	0	1.30
inp-shifted		16	19	0	0	0	0	0	0	
unrelated		199	196	215	435	250	122	0	0	
4-16	8	205	205	205	430	276	100	0	0	1.24
inp-shifted		29	31	0	0	**16**	0	0	0	
unrelated		176	174	205	430	260	100	0	0	
4-17	**9**	155	155	155	465	310	62	0	0	1.12
inp-shifted		**0**	**0**	0	0	0	0	0	0	
unrelated		**155**	**155**	**155**	**465**	310	**62**	0	0	

Table 17. New quartic S-boxes compared to some 5-bit S-boxes previously studied.

results: we either have 16+16 situation with 3024/3969 cases of translation similarity, or 12+20 situation with guaranteed translation similarity in 1008 cases out of 1008. These are the only two types of partitioning which actually happen.

AES S-box. We have finally also looked at what happens with the AES S-box. We found that there is a great variety of 65025 pairs of hyperplanes, and yet translation similarities between pairs of sets of the same size NEVER happen at all for the AES S-box.