Distinguishers for Reduced Round Ascon, DryGASCON, and Shamash Permutations

Cihangir Tezcan

Informatics Institute, Department of Cyber Security, CyDeS Laboratory
Middle East Technical University, Ankara, Turkey

Abstract. Ascon, DryGASCON, and Shamash are submissions to NIST's lightweight cryptography standardization process and have similar designs. We analyze these algorithms against subspace trails, truncated differentials, and differential-linear distinguishers. We provide probability one 4-round subspace trails for DryGASCON-256, 3-round subspace trails for DryGASCON-128, and 2-round subspace trails for Shamash permutations. Moreover, we provide the first 3.5-round truncated differential and 5-round differential-linear distinguisher for DryGASCON-128. Finally, we improve the time and data complexity of the 4-round differential-linear attack on Ascon.

1 Introduction

The National Institute of Standards and Technology (NIST) is in the process of selecting one or more authenticated encryption and hashing schemes suitable for constrained environments. This competition-like process received 57 candidate algorithms in February 2019 and 56 of them were accepted as first-round candidates in April 2019. 32 candidate algorithms are selected for the second-round in August 2019. Ascon [8], DryGASCON [18], and Shamash [17] are submissions to NIST's Lightweight Cryptography Standardization Process. Ascon has been selected as the primary choice for lightweight authenticated encryption in the final portfolio of the CAESAR competition (2014-2019).

Since DryGASCON and Shamash have Ascon like designs, in this work we analyze them together and compare their security against subspace trails, truncated differentials, and differential-linear distinguishers. We first focus on probability one truncated differentials and subspace trails of these three candidate algoritms. We provide probability one 4-round subspace trails for DryGASCON-256, 3-round subspace trail for DryGASCON-128, and 2-round subspace trail for Shamash permutations. Moreover, we provide the first 3.5-round truncated differential. Finally, we combine our probability one truncated differentials with known linear approximations to provide the first 5-round differential-linear distinguisher for DryGASCON-128 and to reduce the time and data complexity of the 4-round differential-linear attack of [5] on Ascon.

This paper is organized as follows: in Sect. 2 we briefly define Ascon, DryGASCON, and Shamash algorithms, mention their differences and recall undis-

turbed bits. In Sect. 3 and Sect. 4 we provide probability one truncated differentials and subspace trails, respectively. In Sect. 5 we provide differential-linear distinguishers for DryGASCON and Ascon. Sect. 6 concludes the paper.

2 Preliminaries

2.1 Ascon

Ascon is a family of authenticated encryption and hashing algorithms that is currently competing in the NIST Lightweight Cryptography competition and selected as one of the 32 second round candidates. Ascon has been selected as the primary choice for lightweight authenticated encryption in the final portfolio of the CAESAR competition (2014-2019). It is a substitution-permutation network and it is based on a sponge-like construction with a state size of 320 bits. Ascon's mode of operation is based on MonkeyDuplex [4].

The initial design of Ascon, which is referred to as v1.0, supported two key lengths, 96 and 128 bits. 96-bit key support is removed in v1.1 and it is also not included in the current version v1.2. This tweaked version provides two recommended parameter sets referred to as Ascon-128 and Ascon-128a.

The encryption consists of four steps: Initialization, processing associated data, processing the plaintext, and finalization. The 320-bit state is represented with five 64-bit words $x_0, \ldots, x_4$. The scheme uses two permutations p^a and p^b which applies the round transformation p iteratively a and b times. These steps are illustrated in Figure 1.

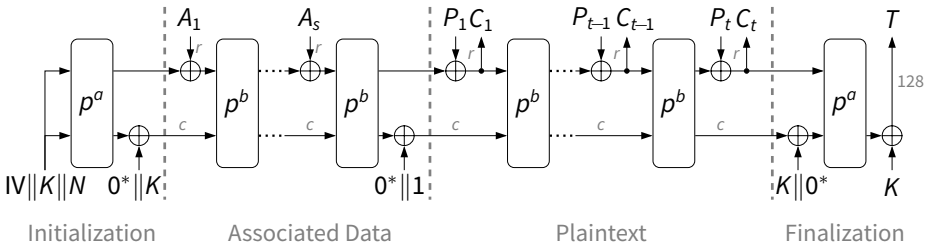

Fig. 1: The encryption of Ascon. Figure is taken from the cipher's official website *http://ascon.iaik.tugraz.at/*

For Ascon-128, we have $a = 12$ and $b = 6$. For Ascon-128a we have $a = 12$ and $b = 8$. Both versions use 128-bit key, nonce and tag. However, data block size is 64 for Ascon-128 and 128 for Ascon-128a.

The round transformation of Ascon first adds a constant to x_2, applies a nonlinear substitution layer and then applies a linear layer. The substitution layer applies a 5-bit S-box 64 times in parallel. This S-box is affine equivalent to the Keccak [1] χ mapping and is provided in Table 1.

Table 1: Ascon's 5-bit s-box.

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

The linear layer is actually XOR of right rotations of the 64-bit words $x_0, \ldots, x_4$. The linear layer can be described as follows:

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

We can divide the attacks into two categories, forgery and key recovery. Forgery attacks focus on the finalization and key recovery attacks focus on the initialization phases of Ascon. When analyzing Ascon, we can target either the initialization in a nonce-respecting scenario, or the processing of the plaintext in a nonce-misuse scenario.

In case of an attack on the finalization of Ascon, suitable characteristics may contain differences in stateword x_0 at the input of the permutation. The rest of the statewords have to be free of differences. For the output of the finalization, the only requirement is that there is some fixed difference pattern in x_3 and x_4. Knowledge about the expected differences in x_0, x_1, and x_2 at the output of the permutation is not required. When we focus on the initialization, differences are allowed in the nonce x_3, x_4 and the output is observed only for x_0 (i.e. output difference should be at x_0).

The first analysis of Ascon is done by the designers in the CAESAR competition submission document [6]. They provided collision-producing differentials and 5-round impossible differential for the permutation. In [7], these observations are further improved to obtain 6-round cube-like, 5-round differential-linear key recovery attacks and 4-round differential forgery attack. They also provided linear and differential bounds and 12-round zero-sum distinguishers for the permutation that requires 2^{130} time complexity.

Moreover, Todo provided integral distinguishers for various numbers of rounds for the Ascon permutation [24].

Finally, Jovanovic et al. proved that Ascon's sponge mode is secure even for higher rates [11].

2.2 DryGASCON

DryGASCON combines the DrySponge construction with a generalized variant of Ascon. It is currently competing in the NIST Lightweight Cryptography

competition and selected as one of the 32 second round candidates. Unlike Ascon, DryGASCON supports two key lengths: 128 bits and 256 bits. They are referred to as DryGASCON-128 and DryGASCON-256, respectively.

DryGASCON-128 is very similar to Ascon with 320-bit state from five 64-bit words. It uses Ascon's 5×5 S-box but represents it in little endian. For DryGASCON-128, round number is reduced to 11 from 12. Thus, this version is referred to as $GASCON_{C5R11}$. The rotations of two rows are also changed, namely Σ_1 and Σ_4. Moreover, each 64 bit word is in bit interleaved representation in DryGASCON which makes the linear layer different than Ascon's. DryGASCON-256 has a state of 576 bits from nine 64-bit words and has 12 rounds. Since DryGASCON-256 has nine words, the S-box is replaced with a 9×9 one. The linear layer of DryGASCON-128 and DryGASCON-256 can be described as follows:

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

2.3 Shamash

Shamash is an Ascon like authenticated encryption algorithm and a submission to the NIST Lightweight Cryptography competition but it is not selected as one of the 32 second round candidates. It is stated in NIST's status report on the first round of the NIST LCW standardization process that although the security of Shamash is claimed to rely on the analysis of Ascon, the specification of Shamash did not sufficiently address the security implications of the differences between two designs.

Shamash uses a 5×5 S-box that is different than Ascon's and DryGASCON's and it is given in Table 2. It has less linear structures and undisturbed bits compared to Ascon's S-box.

Table 2: Shamash's 5-bit s-box.

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

SHAMASH's row rotations are different than ASCON's and DRYGASCON's:

$$\begin{aligned}
\Sigma_0(x_0) &= x_0 \oplus (x_0 \ggg 43) \oplus (x_0 \ggg 62) \\
\Sigma_1(x_1) &= x_1 \oplus (x_1 \ggg 21) \oplus (x_1 \ggg 46) \\
\Sigma_2(x_2) &= x_2 \oplus (x_2 \ggg 58) \oplus (x_2 \ggg 61) \\
\Sigma_3(x_3) &= x_3 \oplus (x_3 \ggg 57) \oplus (x_3 \ggg 63) \\
\Sigma_4(x_4) &= x_4 \oplus (x_4 \ggg 3) \oplus (x_4 \ggg 26)
\end{aligned}$$

Moreover, diffusion layer of SHAMASH has further steps. In order to provide diffusion vertically, each column of the state is multiplied by a 5×5 matrix over $\mathbb{F}_2$ with differential and linear branch number equal to 4. The matrix is

$$\begin{bmatrix}
1 & 0 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 \\
1 & 1 & 1 & 1 & 0
\end{bmatrix}$$

In terms of words, it is given in [17] as

$$\begin{aligned}
x_i &= x_i \oplus x_3 \oplus x_4, \qquad i = 0, 1, 2 \\
x_i &= x_i \oplus x_0 \oplus x_1 \oplus x_2, \; i = 3, 4
\end{aligned}$$

Finally, SHAMASH has a final rotation of words, x_i is rotated $2i + 1$ bytes to the right, $i = 0, 1, 2, 3$, while x_4 is left fixed. SHAMASH permutation consists of 9 rounds.

2.4 Undisturbed Bits

Undisturbed bits, which are probability one truncated differentials for S-boxes, are introduced in [22] as follows.

Definition 1 (Undisturbed Bits [22]). *For a specific input difference of an S-box, if some bits of the output difference remain invariant, then we call such bits* undisturbed.

It was shown in [16] that undisturbed bits are actually linear structures in coordinate functions of an S-box.

Definition 2 (Linear Structures [9]). *An $n \times m$ S-Box S is said to have a* linear structure *if there exists a nonzero vector $\overline{\alpha} \in \mathbb{F}_2^n$ together with a nonzero vector $\overline{b} \in \mathbb{F}_2^m$ such that $\overline{b} \cdot S(\overline{x}) \oplus \overline{b} \cdot S(\overline{x} \oplus \overline{\alpha})$ takes the same value $c \in \mathbb{F}_2$ for all $\overline{x} \in \mathbb{F}_2^n$.*

ASCON's 5×5 S-box has 91 linear structures and 35 of them corresponds to coordinate functions, thus they are undisturbed bits in the forward direction and they are provided in Table 3. Moreover, ASCON has 2 undisturbed bits for the inverse S-box, namely 00010 →???1? and 01000 →?1???. Although the inverse S-box is not used in the encryption or decryption process, its undisturbed bits

Table 3: Undisturbed Bits of Ascon's and DryGASCON's S-box

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

can be used when constructing impossible differentials via the miss-in-the-middle technique.

These undisturbed bits are used in [23] to provide 5-round truncated, impossible and improbable differential distinguishers for Ascon. Similar analysis performed by the designer of DryGASCON in [18] to obtain 3-round and 3.5-round probability one truncated differentials for DryGASCON-128 and DryGASCON-256.

Shamash's 5×5 S-box has 31 linear structures and only 5 of them corresponds to coordinate functions, thus they are undisturbed bits in the forward direction and they are provided in Table 4. The inverse of this S-box has no undisturbed bits.

Table 4: Undisturbed Bits of Shamash's S-box

Input Difference	Output Difference
00001	???1?
00010	??1??
00100	?1???
01000	1????
10000	????1

The 9×9 S-box of DryGASCON-256 has 7459 linear structures and 1143 undisturbed bits in the forward direction. Moreover, it has 4 undisturbed bits in the backward direction.

Although undisturbed bits are useful for finding longer or better distinguishers, they are also used in [20] to show that full PRESENT is secure against related-key differential crypranalysis.

3 Truncated Differentials

Truncated [12], impossible [2], and improbable differential [21] distinguishers for ASCON is provided in [23]. The 3.5-round truncated differential with probability one of [23] extensively uses undisturbed bits. Due to the changes in the linear layer of DryGASCON, namely the two rotations, it is claimed in [18] that it is not possible to obtain 3.5-round truncated differentials for DRYGASCON128 with probability one. Moreover, they provide 3-round and 3.5-round truncated differentials with probability one for DRYGASON-128 and DRYGASCON-256, respectively.

As mentioned in Sec. 4, although the subspace search tool of [15] provided 4-round subspace trails for ASCON with dimension 313, we could not get a 4-round subspace trail for DRYGASCON-128 with dimension less than 320. However, as explained in [15], a differential with full dimension can still provide a truncated differential with probability one and may be used for constructing impossible differentials via the miss-in-the-middle-technique because we may deduce some parts of the output has non-zero difference. For instance, we obtained a 3.5-round truncated differential with probability one for DRYGASCON-128 where we observe that two S-boxes are active after 3.5 rounds (i.e. they have non-zero output difference). We provide this differential in Table 5.

For SHAMASH has a more complicated diffusion layer and its S-box has no zero undisturbed bits, by a similar analysis the longest probability one truncated differentials we can get for SHAMASH are of 1.5 rounds.

4 Subspace Trails

Subspace trail cryptanalysis is introduced in [10] as a generalization of invariant subspace cryptanalysis [14]. However, it is showed in [15] that subspace trails are in fact a special case of truncated differentials and efficient algorithms are provided in [15] to find probability one subspace trails.

We recall the definition of a subspace trail next. For this, let F denote a round function of a key-alternating block cipher, and let $U \oplus a$ denote a coset of a vector space U. By U^c we denote the complementary subspace of U.

Definition 3 (Subspace Trails [10]). *Let $(U_1, U_2, \ldots, U_{r+1})$ denote a set of $r+1$ subspaces with $\dim(U_i) \leqslant \dim(U_{i+1})$. If for each $i = 1, \ldots, r$ and for each a_i, there exists (unique) $a_{i+1} \in U_{i+1}^c$ such that*

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

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

If all the previous relations hold with equality, the trail is called a constant-dimensional subspace trail.

Table 5: Truncated differential Δ_1 with probability one for DryGASCON128 that covers 3.5 rounds of p in binary notation. Substitution and permutation layers are denoted by S and P, respectively.

	3.5-Round Truncated Differential Δ_1
	1000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
I	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	1000000000000000000000000000000000000000000000000000000000000000
S_1	0000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?000000000000000000000000000000000000000000000000000000000000000
	?00000000000000000?00000000000000000000000000000000000?000000000
	1000000000000100000000000000000001000000000000000000000000000000
P_1	0000000000000000000000000000000000000000000000000000000000000000
	?00000000000000000000000000?000000000000000000000000000?00000000
	?00000000000?00000000000000000000000000000000000000000000000?000
	?00000000000??0000?00000000?00000?00000000000000000000??0000?000
	?00000000000??0000?00000000?00000?00000000000000000000??0000?000
S_2	?00000000000?1000000000000000?00000100000000000000000000?0000?000
	?00000000000?10000?00000000?00000100000000000000000000??0000?000
	?00000000000??0000?00000000?00000?00000000000000000000??0000?000
	?000?0000000???000??0000?00?00??0???0000??0000?00?0?00??0000?000
	?00?0000?000??0000?00000????00??0?0??0000?000??0000?00??0000?000
P_2	?10000000?10?1000000000??00???0001000000000?10000000?00?0??0?01?
	?000000?10000???00?0?0?0010?0000010?10000?0000000??000??0000?000
	?000000?0000??0000???000??0?00?00???0000??000??0000000??0000?000
	??0??00????0????00???0??????????0????000??0????00????0??0??0?0??
	??0??00????0????00???0??????????0????000??0????00????0??0??0?0??
S_3	?10?000???10????00???0??????????0????000??0?1??00????0??0??0?01?
	?10??00???10????00???0??????????0????000??0?1??00????0??0??0?01?
	?00??00??000????00???0?0????00??0????000??000??000??00??0000?000
	???????????????????????????????????????0????????????????0???????
	??0???
P_3	??
	???????????????0???????????????????????1????????????????1???????
	?????????0???????0???0?0????00???????000????0???????????0???????
	???????????????????????????????????????x????????????????y???????
	???????????????????????????????????????x????????????????y???????
S_4	???????????????????????????????????????x????????????????y???????
	???????????????????????????????????????x????????????????y???????
	???????????????????????????????????????x????????????????y???????

When searching for truncated differentials or subspace trails, cryptanalysts intuitively give difference to a single S-box to obtain the longest differential or subspace trail. For SPN ciphers, it is proven in [15] that this approach is correct for subspace trail search only when the S-boxes of the cipher do not contain any linear structures. When the cipher has linear structures, the Algorithm 3 of [15] provides the longest subspace trail that starts from the linear layer with r_e rounds and it is proven that the longest subspace trail for this cipher can be at most $r_e + 1$. Thus, it provides an upper bound for the longest probability one subspace trail and lower bound for its dimension.

For instance, Algorithm 3 of [15] obtains a 3-round subspace trail for Ascon with dimension 298, showing that the longest subspace trail for this cipher can be at most 4 rounds with dimension greater than or equal to 298. And using

this algorithm from the substitution layer shows that there actually is a 4-round subpsace trail for Ascon with dimension 313. Actually this subspace trail is used as a truncated differential in [23] but it is obtained via undisturbed bits [22] and for this reason it stops at 3.5 rounds, with dimension 315, because the attacker cannot follow the differences after the final linear layer.

We used the Algorithm 3 of [15] which starts from the linear layer to obtain an upper bound for the longest probability one subspace trails for Ascon, DryAscon-128, DryAscon-256, and Shamash. Results that are provided in Table 6 show that theoretically the longest subspace trails can be achieved except for DryAscon-128.

Table 6: Obtained longest probability one subspace trails both for forward r_e and backward r_d directions and their dimensions d with theoretical upper bounds for Ascon, DryGASCON and Shamash

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

The best 4-round subspace trails we obtained for DryAscon-256 has dimension 558. We could not find a 4-round subspace trail for DryAscon-128 with dimension less than 320. However, a 3.5-round truncated differential with dimension 320 is provided in the previous section.

Although all three algorithms are inverse free, in order to find the subspace trails in the backward direction or to apply techniques like miss-in-the-middle or meet-in-the-middle, we require the inverses of the permutations. For the rotations of the rows, [19] shows that these operations are invertible since they consist of XOR of odd number of values. Moreover, the inverses can also be represented as XOR of t rotations. The values of the t are $31, 33, 33, 33, 35$ for Ascon, $31, 37, 33, 33, 27, 31, 35, 37, 37$ for DryGASCON, and $37, 37, 43, 37, 37$ for Shamash.

5 Differential-Linear Distinguishers

In 1994, Langford and Hellman combined differential cryptanalysis with linear cryptanalysis and introduced differential-linear cryptanalysis [13]. They suggested using a truncated differential with probability one and concatenating a linear approximation with bias q (i.e. probability $1/2+q$) where the output difference of the differential should contain zero differences in the places where input bits masked in the linear approximation. This way one can construct differential-linear distinguishers and the data complexity of the distinguisher is $O(q^{-4})$ cho-

sen plaintexts. The exact number depends on the success probability and the number of possible subkeys.

Moreover, Biham, Dunkelman and Keller showed that it is possible to construct a differential-linear distinguisher where the differential holds with probability $p < 1$ and introduced enhanced differential-linear cryptanalysis [3]. They also showed that the attack is still applicable if the XOR of the masked bits of the differential is 1. In the enhanced method, the bias becomes $2pq^2$ and the data complexity becomes $O(p^{-2}q^{-4})$ chosen plaintexts.

5.1 Ascon

Differential-linear attacks are applied to 4 and 5 rounds of Ascon in [7] for key recovery. Such an attack should focus on the initialization part where the input difference can be given to the nonce, namely the words x_3 and x_4. Moreover, the linear active bits have to be observable and therefore must be in x_0. For instance, a 2-round differential characteristic with probability 2^{-5} is combined with a 2-round linear approximation with bias 2^{-8} in [7]. Thus, the bias of the generated differential-linear characteristic becomes $2pq^2 = 2^{-20}$. In practice this theoretically obtained bias can be higher.

However, these attacks can be improved when the used differential characteristic is replaced with a truncated differential that has probability one. In this work we show that a similar 4-round attack can be performed with a 2-round probability one truncated differential. Namely we combine the probability one 2-round truncated differential Δ_2 of Table 7 and the 2-round linear approximation with bias 2^{-8} of [5] which is also provided in Table 8. Thus, our differential-linear characteristic has a bias of $2pq^2 = 2^{-15}$, contrary to 2^{-20} of [7]. Therefore, the attack can be performed with way less time and data complexity.

5.2 DryGASCON

In a similar manner, we provide a 5-round differential-linear distinguisher by combining the 2-round truncated differential Δ_3 of Table 9 and the 3-round linear approximation of [18] which is also provided in Table 10. Note that this linear approximation does not take into account the $Mix128$ function which is a unique feature of DryGASCON. Hence, it is referred to as an *unconstrained* linear approximation. Otherwise the characteristics should be limited to the lower half of each 64 bit word.

Our 5-round differential-linear characteristic for DryGASCON-128 has a bias of $2pq^2 = 2^{-29}$. Note that this distinguisher for the DryGASCON-128 permutation has input difference in the word x_0 and thus cannot be directly used in a key recovery attack. Such distinguishers are referred as Type-I in [5]. To the best of our knowledge, this is the first 5-round distinguisher for $GASCON_{C5R11}$.

Table 7: Truncated differential Δ_2 with probability one for Ascon that covers 2 rounds of p in binary notation. Substitution and permutation layers are denoted by S and P, respectively.

	2-Round Truncated Differential Δ_3
I	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	0000000001000000000000000000000000000000000000000000000000000000
	0000000001000000000000000000000000000000000000000000000000000000
S_1	000000000?000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000000000000000000000000000000000000000
	000000000?000000000000000000000000000000000000000000000000000000
P_1	000000000?000000000000000000?00000000?0000000000000000000000000
	000000?00?000000000000000000000000000000000000?0000000000000000
	000000000??0000?000000000000000000000000000000000000000000000000
	0000000000000000000000000000000000000000000000000000000000000000
	000000000?000000?000000000000000000000000000000?0000000000000000
S_2	000000?00??0000??000000000000?00000000?000000000?0?0000000000000
	000000?00??0000??000000000000?00000000?000000000?0?0000000000000
	000000?00??0000??000000000000000000000000000000?0?0000000000000
	000000?00??0000??000000000000?00000000?000000000?0?0000000000000
	000000?00?000000?000000000000?00000000?000000000?0?0000000000000
P_2	0?0?0??00??0?0???00000000?00??0000??0??0000??00??0?00000?0000000
	000?00??0??0??0?000000?0?00?00000?00?0000000?0????000??00000000
	000000??0????00???000??000000000000000000000000????00?0?0000000
	0?0?00?00??0000??00??00?0????000??000??000000?0??0?000?000?0?000
	00000??00?000??0?000000?0?0??000000?0?000000?00??0?0000?0?0000000

Table 8: Type-II linear characteristic for 2 rounds of the Ascon-128 permutation with bias 2^{-8} in hexadecimal notation

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

6 Conclusion

In this work we provided probability one subspace trails for DryGASCON-128, DryGASCON-256, and Shamash and a 3.5-round truncated differential and a 5-round differential-linear distinguisher for DryGASCON-128, for the first time. We also showed that the time and the data complexity of the 4-round differential-linear attack on Ascon can be improved by replacing the differential characteristic with a probability one truncated differential. Although our results do not contradict the security claims of these three candidates, our results improve the previously known ones.

Table 9: Truncated differential Δ_2 with probability one for DryGASCON128 that covers 2 rounds of p in binary notation. Substitution and permutation layers are denoted by S and P, respectively.

	2-Round Truncated Differential Δ_3
I	00000000000000000000000000000000000000000000000000000000000000000000000000000000
	00000000000000000000000000010000000000000000000000000000000000000000000000000000
	00000000000000000000000000010000000000000000000000000000000000000000000000000000
	00000000000000000000000000000000000000000000000000000000000000000000000000000000
	00000000000000000000000000000000000000000000000000000000000000000000000000000000
S_1	000000000000000000000000?000000000000000000000000000000000000000000000000000000
	000000000000000000000000?000000000000000000000000000000000000000000000000000000
	00000000000000000000000000000000000000000000000000000000000000000000000000000000
	00000000000000000000000000000000000000000000000000000000000000000000000000000000
	000000000000?000000000000?000000000000000000000?000000000000000
P_1	0000000?000000000000000?000000000000000000000000000000000000?0000
	00000000000000000000000000000000000000000000000000000000000000000000000000000000
	00000000000000000000000000000000000000000000000000000000000000000000000000000000
	000000?000000000000000000?000000000000000000000000000?000000000
S_2	000000??0000?000000000000?000000000000000000000?00000?0000?0000
	000000??0000?000000000000?000000000000000000000?00000?0000?0000
	000000??0000?000000000000?000000000000000000000000?0000?0000
	000000??0000?000000000000?000000000000000000000?00000?0000?0000
	000000??0000?000000000000?000000000000000000000?00000?0000?0000
P_2	000000??0000??0000?00000???000?000?00000?0000?00?00000?0000???00
	000000??0000?00000???000???00?00000?000??0000?00?00000?0000?0?00
	000??0??000000000000000??00??000000000??000000000000?00?0??0?0000
	0??000???000?0?0000?0?0000?00000000?0000000?0000??0000?0000?0??0
	000000??0000??0000??0000?0?00000000??000??0000000?00000?0000??000

Table 10: Type-I $GASCON_{C5R11}$ unconstrained linear characteristic for 3 rounds with bias 2^{-15} in hexadecimal notation

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

Acknowledgements

I would like to thank the designers of DryGASCON and Shamash for their helpful comments.

References

1. Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: The Keccak SHA-3 submission. Submission to NIST (Round 3) (2011), http://keccak.noekeon.org/Keccak-submission-3.pdf
2. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. J. Cryptology 18(4), 291–311 (2005), https://doi.org/10.1007/s00145-005-0129-3

3. Biham, E., Dunkelman, O., Keller, N.: Enhancing differential-linear cryptanalysis. In: Zheng, Y. (ed.) Advances in Cryptology - ASIACRYPT 2002, 8th International Conference on the Theory and Application of Cryptology and Information Security, Queenstown, New Zealand, December 1-5, 2002, Proceedings. Lecture Notes in Computer Science, vol. 2501, pp. 254–266. Springer (2002), https://doi.org/10.1007/3-540-36178-2_16
4. Daemen, J.: Permutation-based encryption, authentication and authenticated encryption. DIAC - Directions in Authenticated Ciphers (2012)
5. Dobraunig, C., Eichlseder, M., Mendel, F.: Heuristic tool for linear cryptanalysis with applications to CAESAR candidates. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II. Lecture Notes in Computer Science, vol. 9453, pp. 490–509. Springer (2015), https://doi.org/10.1007/978-3-662-48800-3_20
6. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: ASCON v1, submission to the CAESAR competition (2014)
7. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Cryptanalysis of ascon. In: Nyberg, K. (ed.) Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings. Lecture Notes in Computer Science, vol. 9048, pp. 371–387. Springer (2015), https://doi.org/10.1007/978-3-319-16715-2_20
8. Dobraunig, C., Eichlseder, M., Mendel, F., Schläffer, M.: Ascon v1.2. In: Lightweight Cryptography Standardization Process round 1 submission. NIST (2019)
9. Evertse, J.H.: Linear Structures in Blockciphers. In: Chaum, D., Price, W.L. (eds.) EUROCRYPT. Lecture Notes in Computer Science, vol. 304, pp. 249–266. Springer (1987)
10. Grassi, L., Rechberger, C., Rønjom, S.: Subspace trail cryptanalysis and its applications to AES. IACR Trans. Symmetric Cryptol. 2016(2), 192–225 (2016), https://doi.org/10.13154/tosc.v2016.i2.192-225
11. Jovanovic, P., Luykx, A., Mennink, B.: Beyond 2 c/2 security in sponge-based authenticated encryption modes. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I. Lecture Notes in Computer Science, vol. 8873, pp. 85–104. Springer (2014), http://dx.doi.org/10.1007/978-3-662-45611-8_5
12. Knudsen, L.R.: Truncated and higher order differentials. In: Preneel, B. (ed.) Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings. Lecture Notes in Computer Science, vol. 1008, pp. 196–211. Springer (1994), https://doi.org/10.1007/3-540-60590-8_16
13. Langford, S.K., Hellman, M.E.: Differential-linear cryptanalysis. In: Desmedt, Y. (ed.) Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings. Lecture Notes in Computer Science, vol. 839, pp. 17–25. Springer (1994), https://doi.org/10.1007/3-540-48658-5_3
14. Leander, G., Abdelraheem, M.A., AlKhzaimi, H., Zenner, E.: A cryptanalysis of printcipher: The invariant subspace attack. In: Rogaway, P. (ed.) Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6841, pp. 206–221. Springer (2011), https://doi.org/10.1007/978-3-642-22792-9_12

15. Leander, G., Tezcan, C., Wiemer, F.: Searching for subspace trails and truncated differentials. IACR Trans. Symmetric Cryptol. 2018(1), 74–100 (2018), https://doi.org/10.13154/tosc.v2018.i1.74-100
16. Makarim, R.H., Tezcan, C.: Relating undisturbed bits to other properties of substitution boxes. In: Eisenbarth, T., Öztürk, E. (eds.) Lightweight Cryptography for Security and Privacy - Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014, Revised Selected Papers. Lecture Notes in Computer Science, vol. 8898, pp. 109–125. Springer (2014), https://doi.org/10.1007/978-3-319-16363-5_7
17. Penazzi, D., Montes, M.: Shamash (and shamashash) (version 1). In: Lightweight Cryptography Standardization Process round 1 submission. NIST (2019)
18. Riour, S.: Drygascon. In: Lightweight Cryptography Standardization Process round 1 submission. NIST (2019)
19. Rivest, R.L.: The invertibility of the XOR of rotations of a binary word. Int. J. Comput. Math. 88(2), 281–284 (2011), http://dx.doi.org/10.1080/00207161003596708
20. Sun, S., Hu, L., Wang, P., Qiao, K., Ma, X., Song, L.: Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers. In: Sarkar, P., Iwata, T. (eds.) Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, R.O.C., December 7-11, 2014. Proceedings, Part I. Lecture Notes in Computer Science, vol. 8873, pp. 158–178. Springer (2014), https://doi.org/10.1007/978-3-662-45611-8_9
21. Tezcan, C.: The improbable differential attack: Cryptanalysis of reduced round CLEFIA. In: Gong, G., Gupta, K.C. (eds.) Progress in Cryptology - INDOCRYPT 2010 - 11th International Conference on Cryptology in India, Hyderabad, India, December 12-15, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6498, pp. 197–209. Springer (2010), https://doi.org/10.1007/978-3-642-17401-8_15
22. Tezcan, C.: Improbable differential attacks on present using undisturbed bits. J. Computational Applied Mathematics 259, 503–511 (2014), https://doi.org/10.1016/j.cam.2013.06.023
23. Tezcan, C.: Truncated, impossible, and improbable differential analysis of ASCON. In: Camp, O., Furnell, S., Mori, P. (eds.) Proceedings of the 2nd International Conference on Information Systems Security and Privacy, ICISSP 2016, Rome, Italy, February 19-21, 2016. pp. 325–332. SciTePress (2016), https://doi.org/10.5220/0005689903250332
24. Todo, Y.: Structural evaluation by generalized integral property. In: Oswald, E., Fischlin, M. (eds.) Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I. Lecture Notes in Computer Science, vol. 9056, pp. 287–314. Springer (2015), http://dx.doi.org/10.1007/978-3-662-46800-5_12