IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2022, No. 3, pp. 303–340. DOI:10.46586/tosc.v2022.i3.303-340

Towards Tight Differential Bounds of Ascon

A Hybrid Usage of SMT and MILP

Rusydi H. Makarim and Raghvendra Rohit

Cryptography Research Centre, Technology Innovation Institute, Abu Dhabi, United Arab Emirates
firstname.lastname@tii.ae

Abstract. Being one of the winners of the CAESAR competition and a finalist of the ongoing NIST lightweight cryptography competition, the authenticated encryption with associated data algorithm Ascon has withstood extensive security evaluation. Despite the substantial cryptanalysis, the tightness on Ascon's differential bounds is still not well-understood until very recently, at ToSC 2022, Erlacher et al. have proven lower bounds (not tight) on the number of differential and linear active Sboxes for 4 and 6 rounds. However, a tight bound for the minimum number of active Sboxes for $4-6$ rounds is still not known.

In this paper, we take a step towards solving the above tightness problem by efficiently utilizing both Satisfiability Modulo Theories (SMT) and Mixed Integer Linear Programming (MILP) based automated tools. Our first major contribution (using SMT) is the set of all valid configurations of active Sboxes (for e.g., 1, 3 and 11 active Sboxes at round 0, 1 and 2, respectively) up to 22 active Sboxes and partial sets for 23 to 32 active Sboxes for 3-round differential trails. We then prove that the weight (differential probability) of any 3-round differential trail is at least 40 by finding the minimum weights (using MILP) corresponding to each configuration till 19 active Sboxes. As a second contribution, for 4 rounds, we provide several necessary conditions (by extending 3 round trails) which may result in a differential trail with at most 44 active Sboxes. We find 5 new configurations for 44 active Sboxes and show that in total there are 9289 cases to check for feasibility in order to obtain the actual lower bound for 4 rounds. We also provide an estimate of the time complexity to solve these cases. Our third main contribution is the improvement in the 7-year old upper bound on active Sboxes for 4 and 5 rounds from 44 to 43 and from 78 to 72, respectively. Moreover, as a direct application of our approach, we find new 4-round linear trails with 43 active Sboxes and also a 5-round linear trail with squared correlation 2^{-184} while the previous best known linear trail has squared correlation 2^{-186}. Finally, we provide the implementations of our SMT and MILP models, and actual trails to verify the correctness of results.

Keywords: Ascon · Active Sboxes · Differential trail · Satisfiability Modulo Theories (SMT) · Mixed Integer Linear Programming (MILP)

1 Introduction

Differential cryptanalysis, introduced by Biham and Shamir [BS90], is one of the most powerful cryptanalytic technique against symmetric key primitives. In a nutshell, the core idea of a differential attack is: (1) Select a pair of distinct inputs such that their XOR value (input difference) equals α and (2) Apply the primitive on both inputs, and XOR the outputs to obtain a output difference β. The goal then is to find a pair (α, β) which occurs with probability higher than $\min\{2^{-\text{blocksize}+1}, 2^{-\text{keysize}+1}\}$ for keyed ciphers

Received: 2022-03-01 Revised: 2022-06-01 Accepted: 2022-08-01 Published: 2022-09-09

or $2^{-\text{blocksize}+1}$ for public permutations. The pair (α, β) then can be exploited as a distinguisher and for key recovery attacks.

Finding such a pair (α, β) with maximum probability is not an easy task due to the large block size of a primitive. Accordingly, for a cipher with an iterative round function, one considers the propagation of differences round by round. More precisely, we have a r-round differential trail $\alpha_0, \cdots, \alpha_r$ such that the probability of $\alpha_i \to \alpha_{i+1}$ is nonzero for all $i = 0, \cdots, r-1$. Now, for an Sbox-based cipher, as a designer or an attacker, one typically approaches the differential analysis by asking the following three questions: (Q1) For any differential (α_0, α_r) what is the minimum number of differentially active Sboxes? This fundamental question is the core of the wide trail strategy proposed by the AES designers [DR02]; (Q2) What is the minimum weight (see Definition 4 and Definition 5 for weight) of a r-round differential trail $(\alpha_0, \cdots, \alpha_r)$? and (Q3) For a differential (α_0, α_r) what is the differential probability?

Investigating the above questions are crucial for understanding the security of any cipher. For example, knowing the exact value (say n) of Q1 and Sbox's differential probability (say p), a designer can lower bound the weight of a r-round differential trail by $n \cdot p$. However, this bound may not be tight as not all n active Sboxes can produce output differences with probability p [KS07, DPU$^+$16]. This brings us to the second question, i.e., what is the lower bound of weight for any r-round differential trail. By knowing the latter, we can estimate the differential probability of (α_0, α_r) by $\sum_{i=w} n(i) \cdot 2^{-i}$ where w is the minimum weight and $n(i)$ is the number of trails with weight i.

This work focuses on the differential analysis of Ascon, an authenticated encryption with associated data (AEAD) algorithm designed by Dobraunig, Eichlseder, Mendel, and Schläffer [DEMS16, DEMS21]. Being one of the winners of the CAESAR competition [CAE] and also a finalist of the ongoing NIST lightweight cryptography competition [Nat19], Ascon has received substantial cryptanalysis till date. A few distinguishing attacks on Ascon's underlying public permutation are differential/linear distinguishers [DEMS15, DEM15, BDKW19], limited-birthday distinguishers [GPT21], zero-sum distinguishing attacks [DEMS15, Tod15, GRW16, YLW$^+$19], and subspace trails [LTW18]. Moreover, there are numerous works which have analyzed the security of Ascon AEAD. Examples include provable security [JLM14], state recovery attacks [DKM$^+$17], differential-linear cryptanalysis [DEMS15, LLL21], forgery attacks [DEMS15, LZWW17, GPT21], cube attack and its variants [DEMS15, LDW17, LZWW17, RHSS21, RS21].

Despite all the aforementioned security evaluation in the last years, we noticed significant gaps in differential bounds [DEMS21] of the Ascon permutation (in particular, the Q1 and Q2 as discussed before). For completeness, we list them below.

- *Is the current 4-round upper bound of 44 active Sboxes tight? What are the configurations (see Definition 6) of active Sboxes which may give a trail with at most 44 active Sboxes? What is the time complexity to find a trail with the minimum number of active Sboxes?*
- *Is the current 5-round upper bound of 78 active Sboxes tight?*

Very recently, at ToSC 2022, Erlacher et al. [EME22] have proved that any 4-round differential trail must have at least 36 active Sboxes. This reduces our first problem to finding whether there exits a 4-round differential trail with the number of active Sboxes in between 36 and 43. In this work, we aim to answer these questions. In the following, we first briefly describe our approach and we then list our contributions.

1.1 Our Approach

Nowadays, Satisfiability Modulo Theories (SMT) [GD07, SNC09, Ste], Mixed Integer Linear Programming (MILP) [MWGP11, SHW$^+$14, ZSCH18, SWW21] and Constraint

Programming (CP) [SGL+17, GPT21] based automated tools[1] are widely utilized to model the differential behavior of a cipher and analyze relevant properties. Since each tool has its own advantage in solving a specific problem, for e.g., SMTs are highly efficient for (un)satisfiability problems while MILP performs well for optimization problems, they are often used independently in prior works.

Our approach here is slightly different as we use SMT and MILP in a hybrid manner. In particular, for small number of rounds, we study the differential behavior using SMT. We then extend those results to cover additional rounds using MILP. The reason is that using either SMT or MILP directly for higher rounds is too slow. To highlight the impact of our approach, we give one example here. The STP and Gurobi (when used independently) were unable to compute the minimum weight of a 3-round differential trail while using our hybrid approach we are able to prove that this weight equals 40. On a separate note, the same result was also obtained in [EME22] using SAT solvers.

1.2 Our Contributions

We report an in-depth differential analysis of Ascon and improve the state-of-the-art bounds. We also present new results on linear trails as a straightforward application of our technique. We emphasize that the goal here is to understand the differential bounds rather than finding an attack. Our contributions are summarized as follows.

1. Core 3-round differential trails: Let d_0, d_1, d_2 be the number of active Sboxes at round 0, 1 and 2, respectively, and let $n = d_0 + d_1 + d_2$. Using our SMT model of Ascon, we find all valid configurations (d_0, d_1, d_2) (see Definition 6) for $n = 15, \cdots, 22$ (see Table 3). It is noteworthy that there exists only one configuration $(1, 3, 11)$ satisfying $n = 15$ which is the minimum known value for 3 rounds. For $n = 23, \cdots, 32$, we apply a time-out strategy to find only those configurations for which the solver returns a trail or is infeasible within a time interval of 2 hrs. Furthermore, we prove that $d_0 + d_2 \geq 9$ for any 3-round differential trail.

2. Optimal weight of a 3-round differential trail: For each valid configuration (d_0, d_1, d_2), since the values of d_0, d_1 and d_2 are known, we are able to compute the minimum weight using the MILP model. For $n = 15, \cdots, 19$, we find that the minimum value equals 40 (see Table 4), this proves that the weight of any 3-round differential trail is at least 40. [2]

3. Exploring 4-round bound on the number of active Sboxes: We present a strategy to explore all 4-round trails with at most 44 active Sboxes. The central idea is to extend all 3-round core trails in forward/backward direction, check their feasibility with SMT and then give necessary conditions on active Sboxes at each round. We find several such conditions and further reduce the search space (possible configurations (d_0, d_1, d_2, d_3)) by using 3-round invalid configurations. In the end, we find 5 new configurations (6, 5, 9, 24), (5, 9, 7, 23), (6, 5, 10, 23), (10, 9, 6, 19) and (9, 4, 8, 23) for 44 active Sboxes while the one provided by designers is of the form (23, 3, 3, 15). Moreover, we show that there are only 9289 cases to check for feasibility in order to obtain the tight lower bound. We also give an estimate on the time complexity to solve these cases and provide comparisons with [EME22].

4. New 4-round and 5-round upper bound on the number of active Sboxes: We use the exact 3-round differential trails (obtained via SMT) as inputs to MILP and minimize the sum of active Sboxes in round 3 and round 4. Consequently, we find trails for 5-round with 72 and 75 active Sboxes while the previous upper bound (by designers)

[1] For example, Gurobi [Gur], STP [GD07], CryptoMiniSAT [SNC09] and CryptoSMT [Ste].

[2] A similar result has been proved in [EME22] but the approach is different.

was 78. The three trails are of the form (5, 9, 10, 23, 25), (10, 9, 5, 21, 30) and (29, 3, 3, 13, 30), respectively. Similarly, we also find a new trail for 4-round with 43 active Sboxes of the form (5, 9, 9, 20), while the previous upper bound was 44. Note that our 4- and 5-round bound of 43 and 72 active Sboxes may still not be tight, however, this improves the existing upper bound by 1 and 6 active Sboxes respectively.

5. New 4-round and 5-round linear trails: Using our combined approach of SMT and MILP, we find three new 4-round linear trails with 43 active Sboxes. The trails are of the form (23, 7, 6, 7), (17, 6, 9, 11) and (22, 8, 6, 7) while the one provided by the designers is of the form (15, 3, 3, 22). Moreover, we find a 5-round linear trail with 78 active Sboxes (21, 5, 9, 11, 30) having squared correlation 2^{-184}. The previous best known 5-round linear trail has 67 active Sboxes (15, 3, 3, 22, 24) and squared correlation 2^{-186} [DEM15].

All the differential and linear trails corresponding to the above mentioned configurations of active Sboxes are provided in Appendix B - Appendix F. Moreover, the source codes of our implementations are publicly available at `https://github.com/Crypto-TII/ascon_hybrid_milp_smt`.

1.3 Outline of the Paper

The rest of the paper is organized as follows. In Section 2, we give a brief overview of differential cryptanalysis, Ascon and our targeted problems. Section 3 presents our SMT and MILP based differential models of Ascon. In Section 4 and Section 5, we investigate the differential properties of 2 and 3 rounds, respectively. In Section 6, we explore the bounds on the number of differentially active Sboxes for 4 and 5 rounds. Section 7 presents our new results on linear trails. Finally, we conclude the paper in Section 8 with future research directions.

2 Preliminaries

In this section, we first give a brief overview of fundamental concepts in differential and linear cryptanalysis. Next, we present the specification of the Ascon permutation and then describe the problems which we address in this work.

2.1 Differential and Linear Cryptanalysis

Differential Cryptanalysis. Differential cryptanalysis [BS90] exploits a non-random behaviour of a cipher $F : \{0,1\}^n \mapsto \{0,1\}^n$ based on a difference in its input and output. More precisely, the aim is to find α and β such that for any input pair x, x' where $x' \oplus x = \alpha$, the output difference $F(x') \oplus F(x) = \beta$ occurs with high probability. For brevity, we consider F as a public permutation throughout the paper. We now state some relevant definitions adapted from [BS90, NK95].

Definition 1 (Differential Probability)**.** A *differential* on $F : \{0,1\}^n \mapsto \{0,1\}^n$ is a pair $(\alpha, \beta) \in \{0,1\}^n \times \{0,1\}^n$ and its probability is defined as $\Pr_{\mathbf{X}}[F(\mathbf{X}) \oplus F(\mathbf{X} \oplus \alpha) = \beta]$ where $\mathbf{X}$ is uniformly distributed in $\{0,1\}^n$, hence its equal to

$$\mathsf{DP}_F(\alpha, \beta) = 2^{-n} \cdot |\{x \in \{0,1\}^n \mid F(x) \oplus F(x \oplus \alpha) = \beta\}|.$$

For any differential (α, β) on F with nonzero probability, we say that F is *active* if $\alpha \neq 0$.

Definition 2 (Weight of a Differential)**.** For a differential (α, β) on F with probability $p \neq 0$, we define its *weight* as $\mathbf{w}(\alpha, \beta) = -\log_2(p)$.

Definition 3 (Differential Trail)**.** Let $F = F_{r-1} \circ F_{r-2} \circ \ldots \circ F_0$ be an r-round iterative permutation. A differential *trail* on F is a sequence $(\alpha_0, \cdots, \alpha_r)$ where each (α_i, α_{i+1}) is a differential on F_i (with $\mathsf{DP}_{F_i}(\alpha_i, \alpha_{i+1}) > 0$) and its probability (assuming independence of rounds) is defined as $\prod_{i=0}^{r-1} \mathsf{DP}_{F_i}(\alpha_i, \alpha_{i+1})$.

Definition 4 (Weight of a Trail)**.** For a differential trail $(\alpha_0, \cdots, \alpha_r)$ on an r-round permutation $F = F_{r-1} \circ F_{r-2} \circ \cdots \circ F_0$ with $\mathsf{DP}_{F_i}(\alpha_i, \alpha_{i+1}) = p_i$, we define the *weight* of the trail as $\sum_{i=0}^{r-1} \mathbf{w}(\alpha_i, \alpha_{i+1})$.

Definition 5 (Optimal Differential Trail)**.** An r-round differential trail $(\alpha_0, \cdots, \alpha_r)$ with weight w is *optimal* if all other r-round trails different from $(\alpha_0, \cdots, \alpha_r)$ have weight at least w.

Linear Cryptanalysis. The linear cryptanalysis method introduced by Matsui [MY92] is very much analogous to the differential cryptanalysis. For $F : \{0,1\}^n \mapsto \{0,1\}^n$, we consider input mask α and output mask β in $\{0,1\}^n$ and evaluate the bias $\epsilon = \Pr_{\mathbf{X}}[\alpha \cdot \mathbf{X} = \beta \cdot F(\mathbf{X})] - \frac{1}{2}$, or equivalently squared correlation $c^2 = 4\epsilon^2$. Here $\cdot$ denotes the scalar product. When F is an iterated cipher, the squared correlation of a linear trail can be computed by taking the product of the squared correlations of the active Sboxes.

2.2 Specification of Ascon Permutation

The Ascon permutation [DEMS16, DEMS21] is an Substitution Permutation Network (SPN) based iterative permutation. The core round function consists of three operations, namely constant addition p_C, the substitution layer p_S, and the linear diffusion layer p_L which are applied on a 320-bit state. In this work, we omit the constant addition since our focus is to analyse the differential property of the permutation. The 320-bit state of Ascon is viewed as a 5×64 binary matrix. The nonlinear function p_S applies identical 5-bit Sbox on all 64 columns of the matrix. The algebraic normal form of the Sbox is given by

$$\begin{aligned}
y_0 &= x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_1x_2 \oplus x_1x_4,\\
y_1 &= x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_1x_2 \oplus x_1x_3 \oplus x_2x_3,\\
y_2 &= x_1 \oplus x_2 \oplus x_4 \oplus x_3x_4 \oplus 1,\\
y_3 &= x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_0x_3 \oplus x_0x_4,\\
y_4 &= x_1 \oplus x_3 \oplus x_4 \oplus x_0x_1 \oplus x_1x_4.
\end{aligned}$$

The linear function p_L applies row-wise operation on each 64-bit word w_0, w_1, w_2, w_3, w_4 as follows

$$\begin{aligned}
w_0 &\leftarrow w_0 \oplus (w_0 \ggg 19) \oplus (w_0 \ggg 28),\\
w_1 &\leftarrow w_1 \oplus (w_1 \ggg 61) \oplus (w_1 \ggg 39),\\
w_2 &\leftarrow w_2 \oplus (w_2 \ggg 1) \oplus (w_2 \ggg 6),\\
w_3 &\leftarrow w_3 \oplus (w_3 \ggg 10) \oplus (w_3 \ggg 17),\\
w_4 &\leftarrow w_4 \oplus (w_4 \ggg 7) \oplus (w_4 \ggg 41),
\end{aligned}$$

where $w \ggg t$ denotes bit wise right rotation of the word w by t step (note that the rightmost bit is the least-significant bit).

The number of rounds r equals 6, 8 or 12 depending on Ascon's variant and its functionality.

2.3 The Targeted Problems

Before describing the targeted problems, we first define the notion of valid configuration of active Sboxes in Definition 6.

Definition 6 (Valid Configuration of Active Sboxes)**.** Let $r \geq 2$ be the number of rounds. We say a *configuration* $(d_0, \cdots, d_{r-1})$ is valid if there exists a r-round differential trail $(\alpha_0, \cdots, \alpha_r)$ with $d_0, \cdots, d_{r-1}$ active Sboxes at round $0, \cdots, r-1$, respectively.

We now list the problems which we address in this work.

1. Characterize (d_0, d_1, d_2) up to a specific number of active Sboxes. Find the minimum weight across all valid (d_0, d_1, d_2).
2. For a valid (d_0, d_1, d_2, d_3), is the $\sum_{i=0}^{3} d_i < 44$?
3. For a valid $(d_0, d_1, d_2, d_3, d_4)$, is the $\sum_{i=0}^{4} d_i < 78$?

2.4 Rotational Symmetry of Differential Trails

The differential trails of Ascon are rotational invariant, i.e., rotating each word of a trail by a fixed offset will result in another valid differential trail with the same number of active Sboxes and same probability. Thus, it is enough to consider one equivalent representative for each of these rotations.

Following the approach of [EME22], which is further inspired from [Mor72], we consider 2-ary necklaces of length 64 in this work. We say a 64-bead necklace given by $e = (e_0, e_1, \cdots, e_{63})$ has a weight n if the Hamming weight of e is n. For $n = 3, 4$ and 5, the number of such necklaces are 651, 9936 and 119133, respectively.

3 Automated Models for Differential Analysis of Ascon

In this section, we present our automated models for the differential propagation of Ascon. We first give the SMT modeling and then discuss the MILP models.

3.1 SMT Modeling

We utilize the SAT/SMT model as a tool to check the existence of a differential trail with nonzero probability on Ascon for a given configuration of active Sboxes. The SMT model represents the propagation of differentials through the linear and nonlinear layer of Ascon permutation. This is a natural approach since the problem of checking the existence of a differential trail with a specific configuration of active Sboxes is a satisfiability problem. The propagation of differential through the linear layer p_L is straightforward to express as SMT model, since it follows directly from the specification of the linear layer. The only non-trivial part is the Boolean formula representing the propagation of differential via the Sbox. On this part, the main result is given in Proposition 1.

Proposition 1. *For each differential* $((x_0, x_1, x_2, x_3, x_4), (y_0, y_1, y_2, y_3, y_4))$ *through the*

Sbox of Ascon*, where* $x_i, y_i \in \mathbb{F}_2^5$*, it holds that*

$$\begin{aligned}
(\neg x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge (y_4 \vee y_3 \vee y_2 \vee y_1 \vee y_0) &= 0\\
(x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge (\neg y_3 \vee \neg(y_0 \oplus y_4)) &= 0\\
(\neg x_0 \wedge x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge (\neg y_0 \vee \neg y_4) &= 0\\
(x_0 \wedge x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge (y_1 \vee \neg(y_0 \oplus y_4)) &= 0\\
(\neg x_0 \wedge \neg x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge (y_0 \vee \neg y_1 \vee \neg y_2) &= 0\\
(x_0 \wedge \neg x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge (\neg y_4 \vee \neg(y_0 \oplus y_2 \oplus y_3)) &= 0\\
(\neg x_0 \wedge x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge \neg y_0 &= 0\\
(x_0 \wedge x_1 \wedge x_2 \wedge \neg x_3 \wedge \neg x_4) \wedge (\neg y_1 \vee y_4) &= 0\\
(\neg x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4) \wedge (\neg y_1 \vee \neg y_2) &= 0\\
(x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4) \wedge \neg(y_0 \oplus y_2 \oplus y_3 \oplus y_4) &= 0\\
(\neg x_0 \wedge x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4) \wedge \neg(y_0 \oplus y_1 \oplus y_2) &= 0\\
(x_0 \wedge x_1 \wedge \neg x_2 \wedge x_3 \wedge \neg x_4) \wedge \neg y_1 &= 0\\
(\neg x_0 \wedge \neg x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4) \wedge (y_1 \vee y_2 \vee \neg(y_0 \oplus y_3 \oplus y_4)) &= 0\\
(x_0 \wedge \neg x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4) \wedge \neg(y_0 \oplus y_3 \oplus y_4) &= 0\\
(\neg x_0 \wedge x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4) \wedge (y_3 \vee \neg(y_0 \oplus y_1 \oplus y_2)) &= 0\\
(x_0 \wedge x_1 \wedge x_2 \wedge x_3 \wedge \neg x_4) \wedge (y_1 \vee \neg y_3) &= 0\\
(\neg x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \wedge (\neg y_3 \vee y_2 \vee \neg(y_0 \oplus y_4)) &= 0\\
(x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \wedge (\neg y_0 \vee y_3 \vee \neg y_4) &= 0\\
(\neg x_0 \wedge x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \wedge \neg(y_0 \oplus y_4) &= 0\\
(x_0 \wedge x_1 \wedge \neg x_2 \wedge \neg x_3 \wedge x_4) \wedge (y_0 \vee y_4 \vee \neg(y_1 \oplus y_2)) &= 0\\
(\neg x_0 \wedge \neg x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \wedge (\neg y_2 \vee y_4) &= 0\\
(x_0 \wedge \neg x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \wedge (\neg y_0 \vee \neg(y_2 \oplus y_3 \oplus y_4)) &= 0\\
(\neg x_0 \wedge x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \wedge \neg y_4 &= 0\\
(x_0 \wedge x_1 \wedge x_2 \wedge \neg x_3 \wedge x_4) \wedge (y_0 \vee \neg(y_1 \oplus y_2)) &= 0\\
(\neg x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4) \wedge \neg y_2 &= 0\\
(x_0 \wedge \neg x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4) \wedge \neg((y_1 \wedge (y_0 \oplus y_2)) \oplus ((y_3 \oplus y_4) \wedge \neg(y_0 \oplus y_1 \oplus y_2))) &= 0\\
(\neg x_0 \wedge x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4) \wedge \neg(y_0 \oplus y_1 \oplus y_3) &= 0\\
(x_0 \wedge x_1 \wedge \neg x_2 \wedge x_3 \wedge x_4) \wedge \neg(y_1 \oplus y_2) &= 0\\
(\neg x_0 \wedge \neg x_1 \wedge x_2 \wedge x_3 \wedge x_4) \wedge (y_2 \vee \neg(y_0 \oplus y_3 \oplus y_4)) &= 0\\
(x_0 \wedge \neg x_1 \wedge x_2 \wedge x_3 \wedge x_4) \wedge \neg((y_0 \wedge (y_1 \oplus y_2)) \oplus ((y_3 \oplus y_4) \wedge \neg(y_0 \oplus y_1 \oplus y_2))) &= 0\\
(\neg x_0 \wedge x_1 \wedge x_2 \wedge x_3 \wedge x_4) \wedge \neg y_3 &= 0\\
(x_0 \wedge x_1 \wedge x_2 \wedge x_3 \wedge x_4) \wedge (y_3 \vee \neg(y_2 \oplus y_1)) &= 0.
\end{aligned}$$

Note that Proposition 1 is a set of constraints that represent propagation of differentials through the S-Box with non-zero probability, and can be simply verified using the DDT. Moreover, our model ignores the probability of the differential, since we are only concerned in whether there is a trail corresponding to given configuration of active Sboxes. We use the SMT solver Stp [GD07] together with CryptoMiniSat [SNC09] as the underlying SAT solver.

3.2 MILP Modeling

We use two different MILP models for our analysis. The first one evaluates the number of active Sboxes while the second computes the weight of a differential trail.

3.2.1 Model for Counting Active Sboxes

Sbox Constraints. Let $(x_0, x_1, x_2, x_3, x_4)$ and $(y_0, y_1, y_2, y_3, y_4)$ be the input and output difference of the Sbox, respectively. Then the following inequalities are sufficient to model the differential propagation of Ascon's Sbox.

$$\begin{aligned} x_0 + x_1 + x_2 + x_3 + x_4 &\geq d \\ x_0 + x_1 + x_2 + x_3 + x_4 &\leq 5 \cdot d \\ y_0 + y_1 + y_2 + y_3 + y_4 &\geq d \\ y_0 + y_1 + y_2 + y_3 + y_4 &\leq 5 \cdot d \end{aligned} \tag{1}$$

$$\sum_{i=0}^{4} a_i^j x_i + \sum_{i=0}^{4} b_i^j y_i + c^j \geq 0, \text{ for } j = 0, \cdots, l-1$$

Here $d \in \{0, 1\}$ and it indicates whether the Sbox is active or not. For $l = 50$, the vectors $(a_0^j, \cdots, a_4^j)$ and $(b_0^j, \cdots, b_4^j)$ and the constant c^j capture all possible differential transitions through the Sbox. They are computed by following the convex hull H-representation technique [SHW+14] and given in Appendix A.1.

Linear Layer Constraints. Let $(y_0, \cdots, y_{319})$ and $(x_0, \cdots, x_{319})$ be the input and output difference of the linear layer, respectively. Then the following inequalities are sufficient to model the differential propagation of linear layer. For $0 \leq i \leq 63$ and $u_i \in \{0, 1, 2\}$, we have

$$\begin{aligned} y_i + y_{(64+i-19) \bmod 64} + y_{(64+i-28) \bmod 64} + x_i &= 2 \cdot u_i \\ y_{64+i} + y_{((64+i-61) \bmod 64)+64} + y_{((64+i-39) \bmod 64)+64} + x_{64+i} &= 2 \cdot u_{64+i} \\ y_{128+i} + y_{((64+i-1) \bmod 64)+128} + y_{((64+i-6) \bmod 64)+128} + x_{128+i} &= 2 \cdot u_{128+i} \\ y_{192+i} + y_{((64+i-10) \bmod 64)+192} + y_{((64+i-17) \bmod 64)+192} + x_{192+i} &= 2 \cdot u_{192+i} \\ y_{256+i} + y_{((64+i-7) \bmod 64)+256} + y_{((64+i-41) \bmod 64)+256} + x_{256+i} &= 2 \cdot u_{256+i} \end{aligned} \tag{2}$$

Note the multiplicative factor of two in Equation 2. This is because if the output bit difference equals 1 then the number of active bits in the input has to be odd. This means the sum of input and output bits is always even.

Constraints for Ascon. We add the above constraints for 64 Sboxes and for each linear layer in every round. We also add a constraint that the sum of input active bits is at least 1 in order to have a nonzero input difference.

Objective Function. Let $r \geq 2$ and for $0 \leq i \leq r-1$, $d_0^i, \cdots, d_{63}^i$ be the variables denoting the activity of 64 Sboxes at round i. Then, the objective function as given in Equation 3 is to minimize the number of active Sboxes.

$$\min \left(\sum_{i=0}^{r-1} \sum_{j=0}^{63} d_j^i \right) \tag{3}$$

The C++ code of the entire model is provided in our public repository at https://github.com/Crypto-TII/ascon_hybrid_milp_smt.

3.2.2 Model for Computing Weight

Sbox Constraints. Let $(x_0, x_1, x_2, x_3, x_4)$ and $(y_0, y_1, y_2, y_3, y_4)$ be the input and output difference of the Sbox, respectively. Since we are looking into the weight of a differential transition, the Sbox modeling is modified slightly compared to Equation 1. We use the approach from [AST+17, Appendix B] to include weights in differential transitions.

We first split the Difference Distribution Table (DDT) into multiple DDTs based on weight. Then, for each DDT we compute the minimized product-of-sum of Boolean functions, and then convert each Boolean function into a linear inequality. Accordingly, the following inequalities are sufficient to model the Sbox.

$$\begin{aligned} x_0 + x_1 + x_2 + x_3 + x_4 &\geq d \\ x_0 + x_1 + x_2 + x_3 + x_4 &\leq 5 \cdot d \\ y_0 + y_1 + y_2 + y_3 + y_4 &\geq d \\ y_0 + y_1 + y_2 + y_3 + y_4 &\leq 5 \cdot d \\ p + q + s &= d \end{aligned} \tag{4}$$

$$\begin{aligned} &\sum_{i=0}^{4} a_i^j x_i + \sum_{i=0}^{4} b_i^j y_i + c^j - 10 \cdot p \geq 0, \text{ for } j = 0, \cdots, l(p) - 1 \\ &\sum_{i=0}^{4} d_i^j x_i + \sum_{i=0}^{4} e_i^j y_i + f^j - 10 \cdot q \geq 0, \text{ for } j = 0, \cdots, l(q) - 1 \\ &\sum_{i=0}^{4} g_i^j x_i + \sum_{i=0}^{4} h_i^j y_i + k^j - 10 \cdot s \geq 0, \text{ for } j = 0, \cdots, l(s) - 1 \end{aligned}$$

Here $d, p, q, s \in \{0, 1\}$. Here p, q and s mean the difference via Sbox propagates with weight 2, 3 and 4, respectively. Thus, if the Sbox is active, i.e., $d = 1$, then either of p, q or s equals 1. Now, for instance, if $p = 1$, only then the inequalities corresponding to it are satisfied. For $l(p) = 22$, the vectors $(a_0^j, \cdots, a_4^j)$ and $(b_0^j, \cdots, b_4^j)$ and the constant c^j capture all possible differential transitions through the Sbox with weight 2. Similarly, for $l(q) = 50$ and $l(s) = 37$, we have $((d_0^j, \cdots, d_4^j), (e_0^j, \cdots, e_4^j), f^j)$ and $((g_0^j, \cdots, g_4^j), (h_0^j, \cdots, h_4^j), k^j)$ capturing the differential transitions with weight 3 and 4, respectively. More details on these vectors are given in Appendix A.2.

Linear Layer Constraints. This is exactly same as Equation 2.

Constraints for Ascon. We add the above constraints for 64 Sboxes and for each linear layer in every round. Furthermore, as before, we add a constraint that the sum of input active bits is at least 1 in order to have a nonzero input difference.

Objective Function. Let $r \geq 2$ and for $0 \leq i \leq r - 1$, $p_0^i, \cdots, p_{63}^i$, $q_0^i, \cdots, q_{63}^i$, $s_0^i, \cdots, s_{63}^i$ be the variables denoting the activity (along with weights) of 64 Sboxes at round i. Then, the objective function as given in Equation 5 is to minimize the weight of a r-round trail.

$$\min \left(\sum_{i=0}^{r-1} \sum_{j=0}^{63} 2 \cdot p_j^i + 3 \cdot q_j^i + 4 \cdot s_j^i \right) \tag{5}$$

The C++ code of the entire model is provided in our public repository at https://github.com/Crypto-TII/ascon_hybrid_milp_smt.

Remark 1. The second model can be easily adapted to count the number of active Sboxes by changing the objective function. However, it becomes slow compared to the first one due to more inequalities (arising from weights).

4 Differential Behavior of Ascon Linear Layer

We focus on Ascon's linear layer (p_L) to study the activity pattern of 2-round differential trails. More precisely, for a given number of active Sboxes d at the input of p_L, we compute the minimum and maximum number of active Sboxes after p_L. For $1 \leq d \leq 64$, we denote them by $N_{\text{min}}[d]$ and $N_{\text{max}}[d]$, respectively. Similarly, we denote $N_{\text{min}}^{-1}[d]$ and $N_{\text{max}}^{-1}[d]$ as the minimum and maximum number of active Sboxes after p_L^{-1}, respectively.

Since the above questions are optimization problems, we use an MILP model (see Subsection 3.2) to derive these bounds. In Table 1, we list these bounds for the linear layer.

Table 1: Activity pattern of Ascon's linear layer.

d	$N_{\text{min}}[d]$	$N_{\text{max}}[d]$	$N_{\text{min}}^{-1}[d]$	$N_{\text{max}}^{-1}[d]$	d	$N_{\text{min}}[d]$	$N_{\text{max}}[d]$	$N_{\text{min}}^{-1}[d]$	$N_{\text{max}}^{-1}[d]$
1	3	11	31	63	33	1	64	4	64
2	4	22	10	64	34	2	64	4	64
3	3	32	1	64	35	1	64	4	64
4	4	41	2	64	36	2	64	4	64
5	4	49	1	64	37	3	64	4	64
6	4	54	2	64	38	2	64	4	64
7	3	59	1	64	39	2	64	4	64
8	4	64	2	64	40	2	64	4	64
9	3	64	1	64	41	2	64	4	64
10	2	64	2	64	42	2	64	5	64
11	3	64	1	64	43	2	64	5	64
12	4	64	2	64	44	2	64	5	64
13	3	64	2	64	45	1	64	5	64
14	4	64	2	64	46	1	64	5	64
15	3	64	2	64	47	1	64	5	64
16	2	64	2	64	48	1	64	5	64
17	3	64	2	64	49	1	64	5	64
18	2	64	2	64	50	2	64	6	64
19	3	64	2	64	51	1	64	6	64
20	2	64	2	64	52	1	64	6	64
21	3	64	2	64	53	1	64	6	64
22	2	64	2	64	54	2	64	6	64
23	3	64	3	64	55	1	64	7	64
24	3	64	3	64	56	1	64	7	64
25	3	64	3	64	57	1	64	7	64
26	2	64	3	64	58	1	64	7	64
27	3	64	3	64	59	1	64	7	64
28	2	64	3	64	60	1	64	8	64
29	3	64	3	64	61	2	64	8	64
30	2	64	3	64	62	1	64	8	64
31	1	64	3	64	63	1	64	8	64
32	2	64	3	64	64	2	64	8	64

In the following, we consider the set of all possible transitions in Table 1 as the *valid 2-round pairs*. For instance, the configurations $(d_0, d_1) = (1, 3), (1, 11), (2, 4)$ result in valid 2-round differential trails while $(d_0, d_1) = (1, 2), (2, 3)$ are invalid configurations for 2 rounds. Here $(d_0, d_1) = (1, 2)$ is invalid meaning if there is one active Sbox at the input, then the output can not have 2 active Sboxes. Furthermore, an extension (forward or backward) of any 2-round invalid configuration to arbitrary number of rounds again results in an invalid configuration.

Invalid 2-round Configurations. We find that (3, 4), (10, 3), (16, 3) and (18, 3) are some of the invalid 2-round configurations.

5 Core 3-Round Trails of Ascon

Let $d_0, d_1, d_2 \in \{1, 2, \cdots, 64\}$ and $n = d_0 + d_1 + d_2$ be the number of active Sboxes for 3 rounds. In this section, we study the following problem: "*For a given n, what are the feasible triplets* (d_0, d_1, d_2)*, i.e., is there a differential trail with* d_0*,* d_1 *and* d_2 *active Sboxes in round 0, 1 and 2, respectively?*" We first present our search strategy. Next, we give results such as the minimum weight and relations among d_0, d_1 and d_2 that always hold for any 3-round trail.

5.1 Search Strategy for 3-Round Trails

For a given number of active Sboxes n, we define

$$\mathcal{I}_n^3 \coloneqq \{(d_0, d_1, d_2) \mid \sum_{i=0}^{2} d_i = n; (d_0, d_1) \text{ and } (d_1, d_2) \text{ are valid 2-round pairs}\}. \quad (6)$$

To find $\mathcal{I}_n^3$, we use the activity pattern of Ascon's linear layer (see Table 1). For instance, $d_0 = 1$ means $3 \leq d_1 \leq 11$, and if $d_1 = 3$ then $d_2 \geq 3$. Thus, for $n = 15$, we have $(1, 4, 11) \in \mathcal{I}_{15}^3$. However, this configuration of active Sboxes may not give a valid 3-round differential trail. Accordingly, to capture all configurations which result in valid 3-round trails, we define the following set.

$$\mathcal{S}_n^3 \coloneqq \{(d_0, d_1, d_2) \in \mathcal{I}_n^3 \mid \sum_{i=0}^{2} d_i = n; (d_0, d_1, d_2) \text{ is a valid 3-round triplet}\} \quad (7)$$

To obtain the set $\mathcal{S}_n^3$, we give $\mathcal{I}_n^3$ as an input to the SMT model (see Subsection 3.1) and check whether $(d_0, d_1, d_2) \in \mathcal{I}_n^3$ is feasible or not. Only if it is feasible, we add it to $\mathcal{S}_n^3$. This idea is also given in Algorithm 1.

Algorithm 1: Searching 3-round valid configurations

```
Input: $\mathcal{I}_n^3$, $\mathcal{S}_n^3 = \{\}$
Output: $\mathcal{S}_n^3$
for $(d_0, d_1, d_2) \in \mathcal{I}_n^3$ do
    if there is a differential trail with $d_0$, $d_1$ and $d_2$ active Sboxes in round 0, 1 and
      2, respectively then
        $\mathcal{S}_n^3 \leftarrow \mathcal{S}_n^3 \cup (d_0, d_1, d_2)$
    end
end
return $\mathcal{S}_n^3$
```

5.2 Examples of 3-Round Trails

We give explicit examples of $\mathcal{S}_n^3$ for $n = 15, \cdots, 30$. Note that the minimum number of active Sboxes for 3 rounds is 15, meaning $n \geq 15$. For $n = 15, \cdots, 22$, we provide the entire set $\mathcal{S}_n^3$ while for $n = 23, \cdots, 32$, we use a time-out (of 2 hrs) to search for the solutions.[3]

[3] There are some triplets for which checking the feasibility took more than 2 days. Hence, we aimed to find some solutions if not all.

In Table 2, we first compare the number of triplets which may belong to $\mathcal{S}_n^3$ with its actual number. Then, in Table 3, we list the entire set $\mathcal{S}_n^3$ for $n = 15, \cdots, 22$. For other values of n, the partial sets are given at `https://github.com/Crypto-TII/ascon_hybrid_milp_smt`. We also provide some of the corresponding differential trails in Appendix B and remaining trails in our public repository.

Table 2: Comparison of number of configurations for 3-round trails. Here $\mathcal{U}$ denotes the number of remaining cases left to solve for completing the search space for a given n.

n	$\lvert\mathcal{I}_n^3\rvert$	$\lvert\mathcal{S}_n^3\rvert$	$\mathcal{U}$	n	$\lvert\mathcal{I}_n^3\rvert$	$\lvert\mathcal{S}_n^3\rvert$	$\mathcal{U}$
15	37	1	0	24	156	≥ 43	35
16	47	2	0	25	174	≥ 55	38
17	56	2	0	26	195	≥ 62	47
18	66	3	0	27	215	≥ 73	67
19	77	4	0	28	236	≥ 85	77
20	90	8	0	29	257	≥ 88	98
21	104	21	0	30	279	≥ 95	114
22	121	22	0	31	303	≥ 118	111
23	137	≥ 35	21	32	328	≥ 136	117

Table 3: All possible configurations of active Sboxes for 3-round trails for $n = 15, \cdots, 22$.

n	$\mathcal{S}_n^3$
15	{(1, 3, 11)}
16	{(1, 3, 12), (2, 4, 10)}
17	{(1, 3, 13), (2, 4, 11)}
18	{(1, 3, 14), (2, 4, 12), (4, 4, 10)}
19	{(1, 3, 15), (2, 4, 13), (3, 3, 13), (4, 4, 11)}
20	{(1, 3, 16), (1, 5, 14), (2, 4, 14), (2, 5, 13), (3, 3, 14), (4, 4, 12), (6, 5, 9), (6, 6, 8)}
21	{(1, 3, 17), (1, 5, 15), (2, 4, 15), (2, 5, 14), (2, 6, 13), (3, 3, 15), (3, 5, 13), (3, 6, 12), (4, 4, 13), (4, 6, 11), (5, 4, 12), (5, 5, 11), (5, 6, 10), (5, 7, 9), (5, 9, 7), (6, 5, 10), (6, 6, 9), (7, 4, 10), (8, 4, 9), (9, 4, 8), (10, 2, 9)}
22	{(1, 3, 18), (1, 5, 16), (2, 4, 16), (2, 5, 15), (2, 6, 14), (3, 3, 16), (3, 5, 14), (3, 6, 13), (4, 4, 14), (4, 5, 13), (4, 6, 12), (5, 4, 13), (5, 5, 12), (5, 6, 11), (6, 4, 12), (6, 5, 11), (6, 6, 10), (7, 4, 11), (7, 5, 10), (8, 4, 10), (8, 5, 9), (10, 2, 10)}

5.3 Results on 3-Round Trails

We now present some new results on 3-round trails of Ascon. We first show in Theorem 1, that the minimum weight of a 3-round trail is at least 40. We then prove in Theorem 2 that the lower bound on the sum of active Sboxes at round 0 and round 2 is at least 9.

Theorem 1 (Minimum weight of a 3-round trail)**.** *Let $n \geq 15$. Then for any $(d_0, d_1, d_2) \in \mathcal{S}_n^3$, the weight of a differential trial is at least 40.*

Proof. To start, note that for any input difference $\alpha \in \mathbb{F}_2^5$, the output difference (via Ascon's Sbox) $\beta \in \mathbb{F}_2^5$ has weight at least 2. This means for $n \geq 20$, since there are at least 20 active Sboxes, the weight of a trail is at least $20 \times 2 = 40$. Thus, to proof the theorem, it is enough to restrict n in the range $[15, 19]$ and show that there does not exist a trail with weight less than 40.

Now, as seen from Table 3, there are exactly 12 such possibilities which may attribute to weight less than 40. Thus, we check the minimum weight corresponding to each of the possible cases. To do this, we add the constraints, for instance, corresponding to configuration $(1, 3, 11)$, we set the number of active Sboxes as 1, 3 and 11 at round 0, 1, and 2, respectively. We then minimize the weight for 3 rounds. Table 4 lists these weights. From the same table, we observe that the minimum weight is 40 which corresponds to trails having 1, 3 and 11 active Sboxes at round 0, 1 and 2, respectively. This proves the theorem.

Table 4: Minimum weights for 3-round differential trails corresponding to specific configuration of active Sboxes.

(d_0, d_1, d_2)	Minimum weight	(d_0, d_1, d_2)	Minimum weight
(1, 3, 11)	**40**	(1, 3, 12)	46
(2, 4, 10)	43	(1, 3, 13)	44
(2, 4, 11)	46	(1, 3, 14)	44
(2, 4, 12)	46	(4, 4, 10)	≥ 43 [not tight]
(1, 3, 15)	49	(2, 4, 13)	49
(3, 3, 13)	45	(4, 4, 11)	≥ 41 [not tight]
(1, 3, 16)	49	(1, 5, 14)	55
(2, 4, 14)	50	(2, 5, 13)	55
(3, 3, 14)	49		

□

Theorem 2 (Sum of active Sboxes at round 0 and round 2)**.** *Let $n \geq 15$. Then for any $(d_0, d_1, d_2) \in \mathcal{S}_n^3$, the following holds: $d_0 + d_2 \geq 9$.*

Proof. We prove this theorem in 3 steps.

- Step 1: For each $d_0 \in \{1, 2, 3\}$, minimize the value of d_2. For $d_0 = 1, 2$ and 3, the minimum values of d_2 are 11, 10 and 12, respectively. This step took seconds using MILP.
- Step 2: For $d_0 = 4$ and 5, we first list all 64-bead necklaces with weight 4 and 5, respectively. We then minimize the value of d_2 corresponding to each necklace. The minimum values are 10 and 7 for $d_0 = 4$ and 5, respectively. This step took ≈ 3.5 days on a single CPU core (on 2.4 GHz 8-Core Intel Core i9 processor) using SMT model.
- Step 3: For $d_2 = 1$ and 2, $d_0 \geq 13$ and $d_0 \geq 10$, respectively. Here, the lower bounds on d_0 are not tight, but good enough considering the proof.

Steps $1 - 3$ mean that $d_0 + d_2 \geq 9$. This proves the theorem. □

Remark 2. The bound in Theorem 2 is certainly not tight. We believe the tight bound is 12. To prove this, we need to show that the following 3-round configurations $(6, \star, 3), (6, \star, 4), (6, \star, 5), (7, \star, 3), (7, \star, 4)$ and $(8, \star, 3)$ are invalid. We tried to solve these cases, but were unable to finish because of the limited resources.

Remark 3. As noted in Step 2 above, for $d_0 = 5$, we have $d_2 \geq 7$. In fact, we find that there is only one 64-bead necklace with weight 5 (Sboxes at positions 32, 37, 38, 41, 63 are active at round 0) which gives this result. For other necklaces, we have $d_2 \geq 9$.

6 New Trails for 4 and 5 Rounds Ascon

The current upper bounds on the number of active Sboxes for 4 and 5 rounds differential trails of Ascon are 44 and 78, respectively [DEMS15, DEMS21]. In this section, we aim to answer the following: "*Are these upper bounds for 4 and 5 rounds tight and what are the configurations of active Sboxes which can improve these bounds?*"

We start this section by discussing our search strategy for 4 and 5 rounds trails. Next, we present new trails for 4 rounds with 44 active Sboxes. We then answer that 4- and 5-round upper bounds are not tight by providing explicit trails with 43 and 72 active Sboxes, respectively.

6.1 Extending 3-Round Trails

Recall from Subsection 5.2, we know some feasible configurations of active Sboxes for 3 rounds. We extend them to one and two rounds forward (backward) to obtain 4 and 5 round trails, respectively. For the forward (resp. backward) extension we use the activity pattern of p_L (resp. p_L^{-1}) as given in Table 1.

We now define the sets which capture all possible configurations of active Sboxes for 4 and 5 rounds with at most 44 and 78 active Sboxes, respectively.

Forward Extension. Let n be the number of active Sboxes in 3 rounds. We first consider all 4-round trails configurations that have n active Sboxes in the first 3 rounds and in total at most 44 active Sboxes in 4 rounds. To do so, we look at $\mathcal{I}_n^3$ (see Equation 6). For each $(d_0, d_1, d_2) \in \mathcal{I}_n^3$, we find d_3 such that (d_2, d_3) is a valid pair for 2 rounds. Next, for a valid (d_2, d_3), we check if there is differential trail for 4 rounds having d_0, d_1, d_2 and d_3 active Sboxes in round 0, 1, 2 and 3, respectively. The above idea is captured by sets $\mathcal{I}_n^4[f]$ and $\mathcal{S}_n^4[f]$ which are defined in Equation 8.

$$\begin{aligned}\mathcal{I}_n^4[f] &\coloneqq \{(d_0, d_1, d_2, d_3) \mid n + d_3 \leq 44;\ (d_0, d_1, d_2) \in \mathcal{I}_n^3;\\ &\qquad (d_2, d_3) \text{ is a valid 2-round pair}\}\\ \mathcal{S}_n^4[f] &\coloneqq \{(d_0, d_1, d_2, d_3) \in \mathcal{I}_n^4[f] \mid (d_0, d_1, d_2, d_3) \text{ is a valid 4-round configuration}\}\end{aligned} \tag{8}$$

To be more explicit about these sets, we give Example 1.

Example 1. For $n = 15$, $(1, 3, 11) \in \mathcal{I}_{15}^3$. Since $d_2 = 11$, then from Table 1, we know $d_3 \geq 3$. Also, $d_3 \leq 29$ as $1 + 3 + 11 + d_3 \leq 44$. Thus, we have $(1, 3, 11, d_3) \in \mathcal{I}_{15}^4[f]$ for $3 \leq d_3 \leq 29$. However, we find that for all $3 \leq d_3 \leq 29$, $(1, 3, 11, d_3) \notin \mathcal{S}_{15}^4[f]$.

In simple words, this example says that for any 4-round trail with at most 44 active Sboxes, the first 3 rounds can never have 15 active Sboxes.

Remark 4. In Equation 8, we use $\mathcal{I}_n^3$ rather than $\mathcal{S}_n^3$. This is because, as seen from Table 2 the set $\mathcal{S}_n^3$ for $n \geq 22$ is partial.

Now, similarly to 4 rounds, we define sets $\mathcal{I}_n^5[f]$ and $\mathcal{S}_n^5[f]$ for 5 rounds (considering 78 Sboxes) in Equation 9.

$$\begin{aligned}\mathcal{I}_n^5[f] &\coloneqq \{(d_0, \ldots, d_4) \mid n + d_3 + d_4 \leq 78;\ (d_0, d_1, d_2) \in \mathcal{I}_n^3;\\ &\qquad (d_2, d_3), (d_3, d_4) \text{ are valid 2-round pairs}\}\\ \mathcal{S}_n^5[f] &\coloneqq \{(d_0, \ldots, d_4) \in \mathcal{I}_n^5[f] \mid (d_0, \ldots, d_4) \text{ is a valid 5-round configuration}\}\end{aligned} \tag{9}$$

Backward Extension. The idea of backward extension is analogous to the forward extension. The only differences are: (1) For 4 (resp. 5) rounds, we use a 3-round configuration in $\mathcal{I}_n^3$ starting at round 1 (resp. round 2); and (2) we use the behavior of p_L^{-1}

instead of p_L. Accordingly, we have the following sets for backward extension as defined in Equation 10 and Equation 11.

$$\begin{aligned}\mathcal{I}_n^4[b] &:= \{(d_0, d_1, d_2, d_3) \mid d_0 + n \leq 44;\ (d_1, d_2, d_3) \in \mathcal{I}_n^3;\\ &\qquad (d_0, d_1) \text{ is a valid 2-round pair}\} \\ \mathcal{S}_n^4[b] &:= \{(d_0, d_1, d_2, d_3) \in \mathcal{I}_n^4[b] \mid (d_0, d_1, d_2, d_3) \text{ is a valid 4-round configuration}\}\end{aligned} \tag{10}$$

$$\begin{aligned}\mathcal{I}_n^5[b] &:= \{(d_0, \ldots, d_4) \mid d_0 + d_1 + n \leq 78;\ (d_2, d_3, d_4) \in \mathcal{I}_n^3;\\ &\qquad (d_0, d_1), (d_1, d_2) \text{ are valid 2-round pairs}\} \\ \mathcal{S}_n^5[b] &:= \{(d_0, \ldots, d_4) \in \mathcal{I}_n^5[b] \mid (d_0, \ldots, d_4) \text{ is a valid 5-round configuration}\}\end{aligned} \tag{11}$$

6.2 Results on 4-Round Trails

Here we give multiple results (in Lemmas 1-4) on what could be the elements of $\mathcal{S}_n^4[f]$ and $\mathcal{S}_n^4[b]$. We also give new paths (apart from designer's one) for 4 rounds with 44 and 43 active Sboxes. In the end, we discuss the number of cases which needs to be solved to find the tight lower bound.

6.2.1 Properties of 4-Round Trails

Lemma 1. *$(1, d_1, d_2, d_3), (d_0, 1, d_2, d_3)$ and $(d_0, d_1, 1, d_3) \notin \mathcal{S}_n^4[f] \cup \mathcal{S}_n^4[b]$.*

Proof. For each case, we minimize the sum using MILP. We find that: (1) $1 + d_1 + d_2 + d_3 \geq 47$, (2) $d_0 + 1 + d_2 + d_3 \geq 53$ and (3) $d_0 + d_1 + 1 + d_3 \geq 47$. Thus, the sum is always greater than 44 and the proof follows. □

Lemma 2 (Bounds on d_0 with backward extension)**.** *For any $(d_0, d_1, d_2, d_3) \in \mathcal{S}_n^4[b]$, the following holds: $5 \leq d_0 \leq 23$. Furthermore, the upper bound is tight as $(23, 3, 3, 15) \in \mathcal{S}_{21}^4[b]$ is the only solution for $d_0 = 23$.*

Proof. We prove the lemma by considering $d_0 = 1, 2, 3, 4, 24, \cdots, 29$. We discard $d_0 = 1$ by Lemma 1. To discard other values, we first note that $n = \sum_{i=1}^3 d_i \geq 15$ and $\sum_{i=0}^3 d_i \leq 44$. Moreover, if $n = 15$, then $(d_1, d_2, d_3) = (1, 3, 11)$ is the only solution. Thus, again by Lemma 1, we remove all configurations of type $(d_0, 1, d_2, d_3)$. The latter also eliminates the case of $d_0 = 29$. We now look at other cases individually as follows.

- $\underline{d_0 = 28}$: Here $n = 16$ and $(28, 2, 4, 10)$ is the only choice.
- $\underline{d_0 = 27}$: Here $n \in \{16, 17\}$, and $d_0 = 27$ means $d_1 \geq 3$. But there is no configuration which starts with $d_1 = 3$ and gives $n = 16, 17$ (see Table 3).
- $\underline{d_0 = 26}$: Here $n \in \{16, 17, 18\}$ and the possible choices are (26, 2, 4, 10), (26, 2, 4, 11), (26, 4, 4, 10) and (26, 2, 4, 12).
- $\underline{d_0 = 25}$: Here $n \in \{16, 17, 18, 19\}$, and $d_0 = 25$ means $d_1 \geq 3$. Thus, we have the following possibilities: (25, 3, 3, 13), (25, 4, 4, 10) and (25, 4, 4, 11).
- $\underline{d_0 = 24}$: Here $n \in \{16, 17, 18, 19, 20\}$, and $d_0 = 24$ means $d_1 \geq 3$. In total, there are 7 possibilities: (24, 3, 3, 13), (24, 4, 4, 10), (24, 4, 4, 11), (24, 3, 3, 14), (24, 4, 4, 12), (24, 6, 5, 9) and (24, 6, 6, 8).
- $\underline{d_0 = 23}$: Here $n \in \{16, 17, 18, 19, 20, 21\}$, and $d_0 = 23$ means $d_1 \geq 3$. In total, there are 23 possibilities: (23, 4, 4, 10), (23, 3, 3, 13), (23, 4, 4, 11), (23, 3, 3, 14), (23, 4, 4, 12), (23, 6, 5, 9), (23, 6, 6, 8), **(23, 3, 3, 15)**, (23, 3, 5, 13), (23, 3, 6, 12), (23, 4, 4, 13), (23, 4, 6, 11), (23, 5, 4, 12), (23, 5, 5, 11), (23, 5, 6, 10), (23, 5, 7, 9), (23, 5, 9, 7), (23, 6, 5, 10), (23, 6, 6, 9), (23, 7, 4, 10), (23, 8, 4, 9), (23, 9, 4, 8), (23, 10, 2, 9).

Using SMT, we checked the feasibility of each of these configurations. We found that only $(23, 3, 3, 15)$ is feasible.

- $\underline{d_0 = 2}$: With MILP, we find that $d_0 + d_1 + d_2 + d_3 \geq 45$.
- $\underline{d_0 = 3}$: Using SMT, we checked if there is 64-bead necklace with weight 3 for which there exists a trail with at most 44 active Sboxes. In around 5 hours of run-time (on a single core), we find that all necklaces are infeasible.
- $\underline{d_0 = 4}$: Again with SMT, we checked if there is 64-bead necklace with weight 4 for which there exists a trail with at most 44 active Sboxes. In around 83 hours of run-time (on a single core), we find that all necklaces are infeasible.

□

Lemma 3 (Bounds on d_3 with forward extension)**.** *For any* $(d_0, d_1, d_2, d_3) \in \mathcal{S}_n^4[f]$*, the following holds:* $1 \leq d_3 \leq 24$*. Furthermore, the upper bound is tight as* $(6, 5, 9, 24) \in \mathcal{S}_{20}^4[f]$ *is the only solution for* $d_3 = 24$*.*

Proof. The proof idea is exactly similar to Lemma 2. Since we are interested in $n = \sum_{i=0}^{2} d_i \geq 15$ and $\sum_{i=0}^{3} d_i \leq 44$, d_3 has to be at most 28. To discard $d_3 = 28, \cdots, 24$, we first enumerate all possible choices corresponding to these values of d_3 .

- $\underline{d_3 = 28}$: Here $n = 16$ and only choice is (2, 4, 10, 28).
- $\underline{d_3 = 27}$: Here $n \in \{16, 17\}$. The choices are (2, 4, 10, 27) and (2, 4, 11, 27).
- $\underline{d_3 = 26}$: Here $n \in \{16, 17, 18\}$. The choices are (2, 4, 10, 26), (2, 4, 11, 26), (2, 4, 12, 26) and (4, 4, 10, 26).
- $\underline{d_3 = 25}$: Here $n \in \{16, 17, 18, 19\}$. We have 7 possibilities: (2, 4, 10, 25), (2, 4, 11, 25), (2, 4, 12, 25), (4, 4, 10, 25), (2, 4, 13, 25), (3, 3, 13, 25), (4, 4, 11, 25).
- $\underline{d_3 = 24}$: Here $n \in \{16, 17, 18, 19, 20\}$ and there are 13 possible configurations: (2, 4, 10, 24), (2, 4, 11, 24), (2, 4, 12, 24), (4, 4, 10, 24), (2, 4, 13, 24), (3, 3, 13, 24), (4, 4, 11, 24), (2, 4, 14, 24), (2, 5, 13, 24), (3, 3, 14, 24), (4, 4, 12, 24), **(6, 5, 9, 24)**, (6, 6, 8, 24).

We checked the feasibility of above configurations of active Sboxes with SMT. We found that only $(6, 5, 9, 24)$ is the feasible choice. Since we have covered the entire sets $\mathcal{S}_n^3$ for $n = 16, \cdots, 20$, the bound on $d_3 = 24$ is tight with $(6, 5, 9, 24)$ as the only solution. This proves the lemma.

□

Lemma 4. *Let* $(d_0, d_1, d_2, d_3) \in \mathcal{S}_n^4[f] \cup \mathcal{S}_n^4[b]$*. Then*

1. $d_1 = 3 \iff$ *the Sboxes at positions 35, 44, 63 in round 1 are active,*
2. $d_1 = 4 \iff$ *the Sboxes at positions 30, 37, 60, 63 in round 1 are active.*

Proof. We checked the feasibility (using SMT) of all 64-bead necklaces with weights 3 and 4 at round 1. We find that all necklaces are infeasible except the two aforementioned positions. The corresponding trails are $(23, 3, 3, 15)$ and $(9, 4, 8, 23)$. Considering the time, it took around 1 CPU day to solve all cases. □

6.2.2 Trails with 44 and 43 Active Sboxes

For 44 active Sboxes, (23, 3, 3, 15) is the only known configuration till now which was provided by Ascon's designers. We found the same trail with our backward extension. Furthermore, our approach (forward extension) gives five new configurations: (6, 5, 9, 24), (5, 9, 7, 23), (6, 5, 10, 23), (10, 9, 6, 19) and (9, 4, 8, 23). We also find a trail with 43 active Sboxes of the form (5, 9, 9, 20) which improves the current upper bound from 44 to 43. All these differential trails along with their corresponding weights are provided in Appendix C.

6.2.3 Configurations with at most 42 Active Sboxes

In the previous section, we have shown that there exists a differential trail for 4 rounds with 43 active Sboxes. *Thus, to find the exact lower bound it is enough to investigate the configurations with at most 42 active Sboxes.* Before checking all these configurations with SMT and MILP, we first filter out some invalid candidates using the properties of 2, 3 and 4 round trails. More precisely, we discard invalid candidates using a three step approach as follows.

Step 1: If (d_0, d_1, d_2, d_3) does not satisfy Lemmas 1-4, discard it.

Step 2: Discard (d_0, d_1, d_2, d_3) if either of the following condition holds.

(a) $(d_0, d_1, d_2, d_3) = (\star, \star, 3, \star)$

(b) $(d_0, d_1, d_2, d_3) = (\star, \star, \star, 3)$

(c) $(d_0, d_1, d_2, d_3) = (5, 5, \star, \star)$

(d) $(d_0, d_1, d_2, d_3) = (6, 5, \star, \star)$

(e) $(d_0, d_1, d_2, d_3) = (\star, \star, 4, \star)$ and $d_1 = 5, \cdots, 9, 11$

(f) $(d_0, d_1, d_2, d_3) = (\star, \star, \star, 4)$ and $d_2 = 5, \cdots, 9, 11$

Finding these relations (a) to (f) took ≈ 8 CPU days.

Step 3: Discard (d_0, d_1, d_2, d_3) using 3-round properties, i.e., if either of the following condition holds.

(a) $d_0 + d_1 + d_2 \leq 15$ or $d_1 + d_2 + d_3 \leq 15$

(b) (d_0, d_1, d_2) or (d_1, d_2, d_3) is an infeasible 3-round configuration. Note that we already know some infeasible cases after computing Table 2 (also given at https://github.com/Crypto-TII/ascon_hybrid_milp_smt).

Using a simple Python script we find that there are only 11496 cases to check for feasibility. Moreover, if we assume that the number of active Sboxes is at least 36 (result from [EME22]) then this number reduces to 9793. Consequently, we need to solve these 9793 cases to find the minimum number of active Sboxes for 4 rounds.

6.2.4 Discussion on the Time Complexity and Reducing Cases

We now discuss the time it would take to solve 9793 cases. We give the expected time complexities based on our experimental results. In our experiments, we used 2.4 GHz 8-Core Intel Core i9 processor MAC laptop.

Time Complexity to solve 9793 cases. First, note that all these cases are not the same. We did some experiments for the run-time. There are easy configurations which returns False within $2-20$ minutes while there are some which require even 2 hours or more. Next, assuming the worst case, i.e., each case require 1 CPU day to solve, we can find the exact lower bound in 9793 CPU days. Although these cases are perfectly parallelizable, currently we do not have enough computational resources to do the same.

We now present some strategies to solve these cases in an efficient way. For instance, out of the 9793 cases, there are 954 cases where $d_0 = 5$. The worst case requires 954 CPU days. However, we can solve them in roughly 207 CPU days. The reasoning is as follows. We find that a necklace with weight 5 at round 0 on average require 2.5 minutes to return True or False (checked with around 105 necklaces). So, the total time can be estimated as

$$\underbrace{119133}_{\#\text{ necklaces}} \times \underbrace{2.5}_{\text{solving time per necklace}} \text{ minutes } \approx 207 \text{ days.}$$

We can further reduce another 504 cases by considering necklaces with weight 5 at round 1. Note that, in this case, the average run-time per necklace is 8 seconds. We were able to solve 13136 necklaces in 29 hours. They all returned output as False. This means the remaining necklaces require another 10 days to complete the search. However, we find a better approach which reduced the run time to 5 days (from 10 days). The idea is as follows. By Remark 3, we need to consider configurations of the form $(d_0, 5, d_2, d_3)$ where $d_3 \geq 9$, meaning $d_0 + 5 + d_2 \leq 33$ (except one configuration[4] where $d_3 = 7$). Accordingly, for a given necklace, we first check whether there is a valid configuration for 3 rounds satisfying $d_0 + 5 + d_2 \leq 33$. Only if a valid configuration exists, then we proceed to check if there is a 4-round configuration with at most 42 active Sboxes. We were able to solve all 119133 necklaces in 5 days and could not find any 4-round trail of the form $(d_0, 5, d_2, d_3)$ such that $d_0 + 5 + d_2 + d_3 \leq 42$. *Consequently, the number of remaining cases is* $9793 - 504 = 9289$.

Remark 5. We emphasize that it is still difficult to estimate the time to prove the tight bound. However, the rate at which we are able to filter out the cases (32825 to 10665 to 9289) is much faster compared to the worst run time.

Proving other Lower Bounds. It is worth noting that to prove the lower bound of 40 active Sboxes, we only need to solve 3898 cases (requiring $\approx$ 3898 CPU days). On the other hand, the approach of [EME22, Section 5.4] requires 6688 CPU days. Furthermore, to prove the lower bound of 36, we initially needed to solve 3578 cases compared to 2^{26} in [EME22]. Note that if solved one by one, we were able to solve around 100 cases in a day on a single core. However, applying Lemma 3 and Lemma 4, we reduced these cases to 1813 in around 5 days of computational time on a single CPU core. These were further reduced to 952 in another 30 days. The latter took longer time as we found some cases which took 2 to 3 days. Currently, we are left with 952 cases to prove the bound of 36 active Sboxes, and we estimate to solve this in around 60 CPU days. We estimated this time based on the solving time of $861(1813 - 952)$ cases.

Note on Run-time and Solvers. The above mentioned timings are obtained using CryptoMiniSAT as the underlying SAT solver. Thus, it is possible that these timings could be improved by using other SAT solvers, for instance Kissat [Kis]. We plan to investigate different SAT solvers in future to improve the results and to provide refined comparisons with that of [EME22].

[4] We checked the only configuration $(d_0, 5, d_2, 7)$ and did not find a trail with less than 42 active Sboxes.

6.3 New Upper Bound for 5-Round Trails

We now show that the best known upper bound (which is 78) of active Sboxes for 5 rounds is not tight. Till date, the only known solution is $(29, 3, 3, 13, 30)$ which was provided by the designers. We use the forward extension approach (see Equation 9) to investigate the tightness of this bound. However, we find the following initial challenges.

1. Setting (d_0, d_1, d_2) to a fixed value as given by $\mathcal{S}_n^3$ for $n = 15, \cdots, 30$, and then minimizing $d_3 + d_4$ using MILP is usually computationally expensive.

2. For $(d_0, d_1, d_2, d_3, d_4) \in \mathcal{I}_n^5[f]$ (see Equation 9), checking its feasibility with SMT is again computationally expensive.

Alternative Approach. In order to tackle the run-time of solvers, we give another efficient approach which is good enough to understand the tightness. Our main idea is to work with the exact differential trails corresponding to each $(d_0, d_1, d_2) \in \mathcal{S}_n^3$ for $n = 15, \cdots, 30$. For a given trail with exact values of differences in the state, finding the minimum value of $d_3 + d_4$ (with MILP) or checking the feasibility (with SMT) is highly efficient. The reason is that on restricting the first three rounds difference values to some constants, the solution space for next 2 rounds is reduced a lot. We can further improve the efficiency by only using the difference values of round 2 and then minimizing the sum of active Sboxes in the next two rounds.

We use the above approach and find configurations with 75 and 72 active Sboxes. The configurations are of the form (10, 9, 5, 21, 30) and (5, 9, 10, 23, 25). The exact differential trails are given in Figure 9 and Figure 10 in Appendix D.

Further Remarks on Tightness. We could not find any other trail with less than 72 active Sboxes for 5 rounds. Thus, currently we are not sure whether this is a tight bound. Also, our solution sets for 3 rounds with more than 22 active Sboxes are partial, and hence, the possibility of multiple configurations with 72 active Sboxes for 5 rounds can not be ignored.

7 New Results on Linear Trails

In this section, we present some results on the linear trails of Ascon. The results are obtained by following a similar approach as of differentials. The only difference is that we replace the DDT modeling with that of LAT (linear approximation table), and slightly modified the linear layer modeling to incorporate the behavior of masks. Since linear analysis is analogous to differentials, we include the complete SMT and MILP models in the Supplementary Material and only provide the initial results here.

No 3-round Trail with 14 Active Sboxes. We checked the feasibility of all possible 3-round configurations with 14 active Sboxes. We find that all these configurations are infeasible.

4-round Trails with 43 Active Sboxes. We extend the 3-round linear trails and found 3 new configurations with 43 active Sboxes. The trails are of the form (23, 7, 6, 7), (17, 6, 9, 11) and (22, 8, 6, 7) while the one provided by the designers is of the form (15, 3, 3, 22). The newly found linear trails are given in Appendix F.

5-round Trail with Improved Squared Correlation. We find a 5-round linear trail with 78 active Sboxes (21, 5, 9, 11, 30) having squared correlation 2^{-184}. The previous best known 5-round linear trail [DEM15] has 67 active Sboxes (15, 3, 3, 22, 24) and squared correlation 2^{-186}. The linear trail is given in Figure 11 in Appendix E.

8 Conclusion

In this work, we have presented an in-depth analysis of differential properties of Ascon by adopting a hybrid usage of SMT and MILP based automated tools. With our approach, we found several results on Ascon which were not known before or were infeasible to prove due to the usage of these tools in an independent manner in prior works. We completely characterized the behavior of 3-round differential trails up to 22 active Sboxes, further investigated 3-round trails with 22 to 30 active Sboxes, and proved that the weight of any 3 round trail is at least 40. For 4 rounds, we identified five new configurations with 44 active Sboxes and presented several necessary conditions to understand the tightness of this bound. We also improved the 7-year old upper bound on active Sboxes for 4 and 5 rounds from 44 to 43 and from 78 to 72, respectively. Finally, we presented new linear trails for 4 rounds, and found a 5-round linear trail with the best squared correlation of 2^{-184} till date.

Although we have presented new bounds here, the exact lower bounds on active Sboxes and weight for 4 and 5 rounds differential trails are still not known. We believe that further study of 3-round trails, solving the remaining cases for 4 rounds, new techniques on hybrid usage of SMT and MILP, and investigating different SAT and MILP solvers will play a crucial role in finding the tight lower bounds for differential and linear trails.

Acknowledgments

We would like to thank the reviewers of ToSC 2022 and Florian Mendel for providing us with insightful comments to improve the quality of the paper. We would also like to thank Emanuele Bellini, Joan Daemen and Silvia Mella for their fruitful discussions on this work.

References

[AST^{+}17] Ahmed Abdelkhalek, Yu Sasaki, Yosuke Todo, Mohamed Tolba, and Amr M. Youssef. MILP modeling for (large) s-boxes to optimize probability of differential characteristics. *IACR Trans. Symmetric Cryptol.*, 2017(4):99–129, 2017.

[BDKW19] Achiya Bar-On, Orr Dunkelman, Nathan Keller, and Ariel Weizman. DLCT: A new tool for differential-linear cryptanalysis. In *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part I*, pages 313–342, 2019.

[BS90] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

[CAE] CAESAR: Call for Submissions. https://competitions.cr.yp.to/caesar-call.html.

[DEM15] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. Heuristic tool for linear cryptanalysis with applications to CAESAR candidates. In *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*, pages 490–509, 2015.

[DEMS15] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Cryptanalysis of ascon. In Kaisa Nyberg, editor, *Topics in Cryptology - CT-RSA 2015, The Cryptographer's Track at the RSA Conference 2015, San Francisco, CA, USA, April 20-24, 2015. Proceedings*, volume 9048 of *Lecture Notes in Computer Science*, pages 371–387. Springer, 2015.

[DEMS16] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2. *Candidate for the CAESAR Competition. See also*, 2016. http://ascon.iaik.tugraz.at.

[DEMS21] Christoph Dobraunig, Maria Eichlseder, Florian Mendel, and Martin Schläffer. Ascon v1.2: Lightweight authenticated encryption and hashing. *J. Cryptol.*, 34(3):33, 2021.

[DKM+17] Ashutosh Dhar Dwivedi, Milos Kloucek, Pawel Morawiecki, Ivica Nikolic, Josef Pieprzyk, and Sebastian Wójtowicz. SAT-based cryptanalysis of authenticated ciphers from the CAESAR competition. In *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications (ICETE 2017) - Volume 4: SECRYPT, Madrid, Spain, July 24-26, 2017*, pages 237–246, 2017.

[DPU+16] Daniel Dinu, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, Johann Großschädl, and Alex Biryukov. Design strategies for ARX with provable bounds: Sparx and LAX. In Jung Hee Cheon and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part I*, volume 10031 of *Lecture Notes in Computer Science*, pages 484–513, 2016.

[DR02] Joan Daemen and Vincent Rijmen. AES and the wide trail design strategy. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 108–109. Springer, 2002.

[EME22] Johannes Erlacher, Florian Mendel, and Maria Eichlseder. Bounds for the security of ascon against differential and linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2022(1):64–87, 2022.

[GD07] Vijay Ganesh and David L. Dill. A decision procedure for bit-vectors and arrays. In Werner Damm and Holger Hermanns, editors, *Computer Aided Verification, 19th International Conference, CAV 2007, Berlin, Germany, July 3-7, 2007, Proceedings*, volume 4590 of *Lecture Notes in Computer Science*, pages 519–531. Springer, 2007.

[GPT21] David Gérault, Thomas Peyrin, and Quan Quan Tan. Exploring differential-based distinguishers and forgeries for ASCON. *IACR Trans. Symmetric Cryptol.*, 2021(3):102–136, 2021.

[GRW16] Faruk Göloglu, Vincent Rijmen, and Qingju Wang. On the division property of S-boxes. *IACR Cryptol. ePrint Arch.*, 2016:188, 2016.

[Gur] Gurobi. https://www.gurobi.com/.

[JLM14] Philipp Jovanovic, Atul Luykx, and Bart Mennink. Beyond $2^{c/2}$ security in Sponge-based authenticated encryption modes. In *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*, pages 85–104, 2014.

[Kis] The Kissat SAT Solver. https://github.com/arminbiere/kissat.

[KS07] Liam Keliher and Jiayuan Sui. Exact maximum expected differential and linear probability for two-round advanced encryption standard. *IET Inf. Secur.*, 1(2):53–57, 2007.

[LDW17] Zheng Li, Xiaoyang Dong, and Xiaoyun Wang. Conditional cube attack on round-reduced ASCON. *IACR Trans. Symmetric Cryptol.*, 2017(1):175–202, 2017.

[LLL21] Meicheng Liu, Xiaojuan Lu, and Dongdai Lin. Differential-linear cryptanalysis from an algebraic perspective. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part III*, volume 12827 of *Lecture Notes in Computer Science*, pages 247–277. Springer, 2021.

[LTW18] Gregor Leander, Cihangir Tezcan, and Friedrich Wiemer. Searching for subspace trails and truncated differentials. *IACR Trans. Symmetric Cryptol.*, 2018(1):74–100, 2018.

[LZWW17] Yanbin Li, Guoyan Zhang, Wei Wang, and Meiqin Wang. Cryptanalysis of round-reduced ASCON. *Sci. China Inf. Sci.*, 60(3):38102, 2017.

[Mor72] Charles Moreau. On distinct circular permutations. 2nd series, 11:309–314, 1872.

[MWGP11] Nicky Mouha, Qingju Wang, Dawu Gu, and Bart Preneel. Differential and linear cryptanalysis using mixed-integer linear programming. In Chuankun Wu, Moti Yung, and Dongdai Lin, editors, *Information Security and Cryptology - 7th International Conference, Inscrypt 2011, Beijing, China, November 30 - December 3, 2011. Revised Selected Papers*, volume 7537 of *Lecture Notes in Computer Science*, pages 57–76. Springer, 2011.

[MY92] Mitsuru Matsui and Atsuhiro Yamagishi. A new method for known plaintext attack of FEAL cipher. In Rainer A. Rueppel, editor, *Advances in Cryptology - EUROCRYPT '92, Workshop on the Theory and Application of of Cryptographic Techniques, Balatonfüred, Hungary, May 24-28, 1992, Proceedings*, volume 658 of *Lecture Notes in Computer Science*, pages 81–91. Springer, 1992.

[Nat19] National Institute of Standards and Technology. Lightweight Cryptography (LWC) Standardization project, 2019. https://csrc.nist.gov/projects/lightweight-cryptography.

[NK95] Kaisa Nyberg and Lars R. Knudsen. Provable security against a differential attack. *J. Cryptol.*, 8(1):27–37, 1995.

[RHSS21] Raghvendra Rohit, Kai Hu, Sumanta Sarkar, and Siwei Sun. Misuse-free key-recovery and distinguishing attacks on 7-round ascon. *IACR Trans. Symmetric Cryptol.*, 2021(1):130–155, 2021.

[RS21] Raghvendra Rohit and Santanu Sarkar. Diving deep into the weak keys of round reduced ascon. *IACR Trans. Symmetric Cryptol.*, 2021(4):74–99, 2021.

[SGL$^+$17] Siwei Sun, David Gérault, Pascal Lafourcade, Qianqian Yang, Yosuke Todo, Kexin Qiao, and Lei Hu. Analysis of aes, skinny, and others with constraint programming. *IACR Trans. Symmetric Cryptol.*, 2017(1):281–306, 2017.

[SHW$^+$14] Siwei Sun, Lei Hu, Peng Wang, Kexin Qiao, Xiaoshuang Ma, and Ling Song. Automatic security evaluation and (related-key) differential characteristic search: Application to simon, present, lblock, DES(L) and other bit-oriented block ciphers. In Palash Sarkar and Tetsu Iwata, editors, *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*, volume 8873 of *Lecture Notes in Computer Science*, pages 158–178. Springer, 2014.

[SNC09] Mate Soos, Karsten Nohl, and Claude Castelluccia. Extending SAT solvers to cryptographic problems. In Oliver Kullmann, editor, *Theory and Applications of Satisfiability Testing - SAT 2009, 12th International Conference, SAT 2009, Swansea, UK, June 30 - July 3, 2009. Proceedings*, volume 5584 of *Lecture Notes in Computer Science*, pages 244–257. Springer, 2009.

[Ste] Stefan Kölbl. CryptoSMT: An easy to use tool for cryptanalysis of symmetric primitives. https://github.com/kste/cryptosmt.

[SWW21] Ling Sun, Wei Wang, and Meiqin Wang. Accelerating the search of differential and linear characteristics with the SAT method. *IACR Trans. Symmetric Cryptol.*, 2021(1):269–315, 2021.

[Tod15] Yosuke Todo. Structural evaluation by generalized integral property. In Elisabeth Oswald and Marc Fischlin, editors, *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*, volume 9056 of *Lecture Notes in Computer Science*, pages 287–314. Springer, 2015.

[YLW$^+$19] Hailun Yan, Xuejia Lai, Lei Wang, Yu Yu, and Yiran Xing. New zero-sum distinguishers on full 24-round Keccak-f using the division property. *IET Inf. Secur.*, 13(5):469–478, 2019.

[ZSCH18] Yingjie Zhang, Siwei Sun, Jiahao Cai, and Lei Hu. Speeding up MILP aided differential characteristic search with matsui's strategy. In Liqun Chen, Mark Manulis, and Steve A. Schneider, editors, *Information Security - 21st International Conference, ISC 2018, Guildford, UK, September 9-12, 2018, Proceedings*, volume 11060 of *Lecture Notes in Computer Science*, pages 101–115. Springer, 2018.

A MILP models for Ascon

A.1 Sbox Inequalities

X = [(4, 9, 3, 9, 5, -2, 2, -1, 0, -6, 0), (-2, 3, 0, 4, -2, 1, 1, 2, 0, 3, 0), (13, 7, -5, -5, 8, -1, -2, 4, 4, 13, 0), (-1, 3, 1, -3, -2, -1, 0, 0, -1, -2, 7), (3, 5, 5, -2, 1, 3, 0, -2, -2, 3, 0), (1, -1, 3, 5, 4, -2, 2, 6, -1, -2, 0), (2, -2, -3, 2, 4, 0, -1, -4, 1, -1, 7), (-1, -1, -1, -3, -2, 0, 2, 3, 3, 0, 5), (-3, -2, -3, -4, -6, -1, -3, -3, -3, -1, 23), (-3, 3, 2, 4, -2, 1, -2, -1, 0, 1, 4), (-5, -4, -2, -3, -2, 1, 5, -7, -7, -3, 26), (2, -1, -1, -2, -2, 0, 2, 0, 1, 0, 4), (2, -2, -4, 3, 1, 4, -4, 1, -1, -4, 10), (-3, -1, 2, -2, -3, -1, -2, 5, 5, -2, 9), (-2, -1, -5, 5, -1, -4, -4, -3, 2, 6, 14), (-2, 2, -2, -1, 1, 2, 0, 1, 1, 0, 3), (4, 4, -3, 2, -2, 5, 1, 0, 3, 1, 0), (-1, -2, -9, 7, 3, -7, 6, -4, 1, -5, 19), (1, -2, 2, 1, 2, 0, 0, 1, 1, 1, 0), (-3, -3, -4, -1, 2, 1, 4, -2, -2, 1, 11), (-2, 9, 10, 8, -4, -3, 10, -1, -2, 12, 0), (4, -3, -4, -1, 2, -1, -4, 0, -2, 1, 11), (2, -3, 2, -1, 1, -1, -1, -3, 3, -3, 9), (0, 2, -1, 2, 1, -1, -1, 1, 0, -1, 2), (1, -1, -2, 3, -1, 4, 4, 2, 0, 4, 0), (2, 2, -2, -3, -4, -4, 1, -1, -1, -1, 12), (0, -1, 0, -1, 1, 0, 1, 1, -1, -1, 3), (-1, -3, 2, 2, 1, -1, -1, 3, -1, 2, 4), (-1, -3, -1, 2, -1, 3, -3, 1, -1, -2, 9), (2, 1, 1, -3, 1, 2, 0, 2, 2, 2, 0), (-2, 2, 3, 1, -1, -1, -3, -1, 0, -1, 6), (-1, -2, 2, -2, 1, 0, -2, -1, -2, 2, 8), (-2, -2, 1, 1, -1, 1, -1, 3, 2, -3, 6), (-1, -1, 0, -1, 1, 0, 1, 0, 1, 1, 2), (-1, 1, -1, -2, -2, 0, 0, 1, 1, -1, 5), (1, -2, 2, -1, -1, -1, -1, 1, 2, 1, 4), (-1, 1, -1, -1, 0, 1, 0, -1, -1, 0, 4), (0, 0, 1, 1, -1, 1, 1, -1, 0, -1, 2), (1, 0, 2, 1, -1, 2, -2, -2, 1, 2, 3), (2, -4, -4, 2, 3, -1, -1, -1, -2, 1, 9), (-1, -2, 0, 2, -1, -2, 2, 1, -1, -1, 6), (2, -2, -1, -1, 1, 0, -1, 1, -1, -1, 5), (-1, 2, 1, -2, -1, -1, 0, 0, 0, -1, 4), (-1, 1, 2, 2, -2, -1, 2, -2, 1, 3, 3), (2, 5, 1, -3, -5, -4, 1, -1, -4, -1, 13), (2, -2, -2, 2, 3, 1, -1, -3, 2, -1, 5), (0, 0, 1, 1, -1, -1, -1, -1, 0, -1, 4), (0, -1, 1, -1, 1, 0, -1, -1, 1, -1, 4), (-1, 1, -2, 1, 2, 1, -1, 2, 0, -1, 3), (2, -1, -1, -1, 1, 0, 0, -2, -2, 2, 5)]

We add one inequality corresponding to each vector in X. For example, we have

$$4x_0 + 9x_1 + 3x_2 + 9x_3 + 5x_4 - 2y_0 + 2y_1 - 1y_2 + 0y_3 - 6y_4 + 0 \geq 0$$

corresponding to the vector $(4, 9, 3, 9, 5, -2, 2, -1, 0, -6, 0)$.

A.2 Sbox Inequalities with Weights

Weight 2 transitions. W$_2$ = [(1, 0, 1, 0, 0, 0, 0, 0, 0, 0), (0, 0, 0, -1, 0, 0, 0, 0, 0, -1),(0, 1, -1, 0, 0, 0, 0, 1, 0, 0), (0, 0, -1, 0, -1, 0, 0, 0, 0, 0), (0, -1, 1, 0, 0, 0, 0, 0, 0, 0), (0, 0, -1, 0, 0, 0, 0, -1, 1, 0), (-1, 0, -1, 0, 0, 0, 0, 0, 0, 0), (0, 0, 0, -1, 1, 0, 0, 0, 0, 0), (0, -1, 0, 0, 0, 0, 0, 0, -1, 0), (0, 0, 1, 0, 1, 0, 0, -1, 0, 0), (0, 0, 0, -1, 0, 0, 0, 1, 1, 0), (0, 0, 0, -1, 0, 0, 0, -1, -1, 0), (0, 0, 1, 1, 0, 1, 0, 0, 0, 1), (0, 0, -1, 0, 0, 0, 0, 0, -1, -1), (0, 0, 0, 0, -1, -1, 0, 0, 0, 1), (0, 0, 1, 0, 1, 0, 1, 0, 0, 0), (0, 0, 0, 0, -1, 1, 0, 0, 0, -1), (0, 0, 1, 0, 0, -1, -1, 0, 0, -1), (0, -1, 0, 0, 0, -1, -1, 0, 0, 1), (0, -1, 0, 0, 0, 1, 1, 0, 0, 1), (0, 0, -1, 0, 0, 1, -1, 0, 0, -1), (0, 0, 0, 0, 1, -1, 1, 0, 0, -1)]

We add one inequality corresponding to each vector in W$_2$. For example, we have

$$-x_3 - y_4 + 11 - 10p \geq 0$$

corresponding to the vector $(0, 0, 0, -1, 0, 0, 0, 0, 0, -1)$. The constant value 11 equals the sum of 9 and number of times -1 occurs.

Weight 3 transitions. W$_3$ = [(-1, 0, 0, -1, 1, 0, 0, 0, 0, 0), (0, -1, 1, -1, 0, 0, 0, 0, 0, 0), (1, -1, 0, 0, -1, 0, 1, 0, 0, 0), (-1, 1, 1, 0, 0, 0, 0, 0, 0, 0), (0, 1, 0, 1, 1, -1, 0, 0, 0, 0), (1, -1, 0, 1, -1, 0, 0, 0, 0, 0), (0, 1, 1, 0, 0, 1, 0, 0, 0, 1), (-1, 0, 1, 0, 1, 0, 0, 0, 0, 0), (1, 0, -1, 1, 0, 1, 0, 0, 0, 0), (1, 0, 0, 1, 1, 0, 0, 1, 0, 0), (0, -1, 0, 1, 0, 0, 0, -1, 1, 1), (0, 1, 0, 1, 0, 0, 1, 1, 0, 1), (1, 1, -1, -1, 0, 0, 0, 0, 1, 0), (-1, 1, 0, 1, -1, 0, 0, 0, 0, 1), (0, -1, 0, 0, 1, 0, 0, -1, 1, -1), (-1, -1, 0, -1, 0, 0, -1, 0, 0, 0), (0, 1, 1, 0, 1, 1, 0, 0, 0, 0), (-1, 1, 0, -1, 0, 0, 0, 0, 0, -1), (0, -1, -1, 1, 1, 0, 0, -1, 0, 0), (0, -1, 0, 0, -1, 0, 0, -1, -1, -1), (0, -1, 0, -1, 0, 0, -1, 0, -1, 0), (0, 1, 1, 0, -1, -1, 0, 0, 0, -1), (0, 1, -1, -1, 1, 0, 0, 0, 0, 0), (1, 0, 0, -1, -1, -1, 0, 0, -1, 0), (0, 1, 0, 1, 0, 1, 1, 1, 0, 0), (0, -1, 0, 1, -1, 0, 0, 1, -1, 1), (0, -1, -1, 1, 0, -1, 1, 0, 0, -1), (0, -1, -1, 1, 0, 1, 1, 0, 0, 1), (0, -1, 0, 1, 0, 1, -1, 1, 0, -1), (0, 0, -1, 1, 0, -1, -1, -1, 0, 1), (0, 1, 1, 1, 0, 0, 1, 0, 0, 0), (0, -1, 0, 0, -1, 0, 1, 1, 1, -1), (-1, 0, 0, -1, 0, 0, 0, -1, -1, 0),

(-1, 0, 0, -1, 0, 0, 0, 1, 1, 0), (0, 0, -1, -1, 1, 0, -1, 0, 0, 0), (0, 0, 1, -1, 1, 0, 0, 0, 0, 1), (0, 0, 1, 0, -1, -1, 1, 0, -1, 0), (-1, 0, 0, 0, -1, -1, -1, 1, 1, 0), (0, 0, -1, 1, -1, 1, -1, -1, 0, -1), (0, 1, 0, 0, -1, -1, -1, 1, 0, -1), (0, 1, 0, 1, 0, -1, 1, -1, 0, -1), (0, 0, 1, 1, 0, 1, 1, 0, 1, 0), (0, 1, 0, 0, 1, 1, 0, 1, 0, 0), (0, 0, 1, -1, 0, 1, 0, 0, -1, 0), (0, 0, 0, 0, 1, -1, -1, 1, 0, 1), (1, -1, 0, 0, 0, 0, 0, 1, -1, -1), (0, 0, 0, -1, 1, 0, 0, -1, -1, 1), (0, 0, -1, -1, 0, 0, 1, 1, 1, 1), (-1, 0, 1, 0, 0, -1, -1, 0, 1, 0), (-1, 0, 1, 0, 0, 1, -1, 0, -1, 0)]

We add one inequality corresponding to each vector in W_3. For example, we have

$$-x_0 - x_3 + x_4 + 11 - 10q \geq 0$$

corresponding to the vector $(-1, 0, 0, -1, 1, 0, 0, 0, 0, 0)$.

Weight 4 transitions. $\mathsf{W}_4 =$ [(0, 0, -1, 0, 0, 1, 1, 0, 0, 1), (0, 0, 0, 1, 0, 1, 1, 1, 0, 1), (0, 0, 0, 1, 0, 1, -1, 1, 0, -1), (0, 0, 0, 1, 0, -1, 1, 1, 0, -1), (0, 1, 0, 1, 0, 0, 0, 0, 0, 0), (0, 0, 0, 1, 0, -1, -1, 1, 0, 1), (0, 1, 0, 0, -1, 0, 0, 0, 0, 0), (-1, 1, -1, 0, 0, 1, 0, 0, 0, 0), (-1, 0, 0, 1, -1, 0, 0, 0, 0, 0), (1, 1, 1, 0, 0, 0, 0, 0, 0, 0), (0, 1, 0, 0, 0, 1, 0, 0, 0, 1), (1, 0, 0, 1, 1, 0, 0, 0, 0, 0), (1, 0, 0, -1, -1, 0, 0, 0, 1, 0), (0, 1, 1, 0, 0, -1, 0, 0, 0, -1), (-1, 0, 0, 0, -1, 0, 0, -1, -1, 0), (-1, -1, 0, -1, 1, 0, 1, 0, 1, 1), (1, 0, 0, 0, 1, 0, 0, -1, -1, 1), (1, -1, -1, -1, 0, 0, 0, 0, 0, 0), (0, 0, -1, -1, -1, 0, 0, 0, 0, 0), (0, -1, -1, 0, 1, 0, 1, 0, 0, 0), (0, 0, 0, 1, 1, 0, 0, 1, 0, 0), (0, 0, -1, 1, 1, 0, 0, 0, 0, 0), (0, 0, 0, -1, -1, 0, 0, 1, 1, 0), (1, 0, 1, 0, 1, 0, 0, -1, 1, -1), (1, 0, 1, 0, 1, 0, 0, 1, -1, -1), (-1, -1, 1, -1, 1, 0, -1, 0, 1, -1), (1, 0, 0, 0, 1, 0, 0, 1, 1, 1), (-1, -1, 0, -1, 1, 0, 1, 0, -1, -1), (-1, -1, 1, -1, 1, 0, -1, 0, -1, 1), (1, 0, -1, 0, 1, 0, 0, 0, 0, 1), (0, 0, 1, 1, -1, -1, -1, -1, 0, -1), (0, 0, 1, 1, -1, 1, 1, -1, 0, -1), (0, 0, 1, 1, -1, 1, -1, -1, 0, 1), (0, 0, 1, 1, -1, -1, 1, -1, 0, 1), (0, 0, -1, 0, -1, 1, -1, 0, 0, -1), (0, 0, -1, 0, -1, -1, 1, 0, 0, -1), (0, 0, -1, 0, -1, -1, -1, 0, 0, 1)]

We add one inequality corresponding to each vector in W_4. For example, we have

$$-x_0 - x_1 - x_3 + x_4 + y_1 + y_3 + y_4 + 12 - 10s \geq 0$$

corresponding to the vector $(-1, -1, 0, -1, 1, 0, 1, 0, 1, 1)$.

B Examples of 3-Round Trails

```
................................................................
1...............................................................
1...............................................................
................................................................
................................................................
----------------------------------------------------------------   p_S
1...............................................................
................................................................
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_L
1..................1........1...................................
................................................................
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_S
1..................1........1...................................
1..................1........1...................................
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_L
1.....................................1.................1.......
1..1............1..1.....1..1..........1..................1..1..
................................................................
................................................................
................................................................
```

Figure 1: 3-round trail with 15 [1, 3, 11] active Sboxes and weight 40 [2, 6, 32].

```
................................................................
..........................................1.....................
..........................................1.....................
................................................................
................................................................
----------------------------------------------------------------   p_S
..........................................1.....................
................................................................
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_L
......1...................................1..................1..
................................................................
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_S
......1...................................1..................1..
......1...................................1..................1..
................................................................
......1.........................................................
................................................................
----------------------------------------------------------------   p_L
................1.................1.......1.....................
...1..1..........1..................1..1..1..1............1..1..
................................................................
......1.........1......1........................................
................................................................
```

Figure 2: 3-round trail with 16 [1, 3, 12] active Sboxes and weight 46 [2, 6, 38].

```
.......................................................1........
.1..............................................................
.1..............................................................
.......................................................1........
.......................................................1........
----------------------------------------------------------------   p_S
................................................................
................................................................
................................................................
.......................................................1........
.1..............................................................
----------------------------------------------------------------   p_L
................................................................
................................................................
................................................................
.1......1..............................................1........
.1......1.................................1.....................
----------------------------------------------------------------   p_S
.......................................................1........
..........................................1.....................
................................................................
................................................................
.1......1.................................1............1........
----------------------------------------------------------------   p_L
..........1........1...................................1........
.................1.....................1..1.....................
................................................................
................................................................
.1.............1...1............1......................1......1.
```

Figure 3: 3-round trail with 16 [2, 4, 10] active Sboxes and weight 43 [4, 12, 27].

C Trails for 4 Rounds with 43 and 44 Active Sboxes

```
..........................1..................1........1.........
..........................1.........1......1....................
..........................1.........1......1....................
..........................1..................1........1.........
..........................1..................1........1.........
----------------------------------------------------------------   p_S
..........................1.........1......1....................
................................................................
................................................................
..........................1..................1........1.........
................................................................
----------------------------------------------------------------   p_L
1......1..................1.........1......1.1........11......1.
................................................................
................................................................
1......1..................1.........1......1.1........11......1.
................................................................
----------------------------------------------------------------   p_S
1......1..................1.........1......1.1........11......1.
................................................................
................................................................
1.........................1.....................................
................................................................
----------------------------------------------------------------   p_L
1.........1......11.......1.1......11......1....................
................................................................
................................................................
1.........1......1........1.........1......1....................
................................................................
----------------------------------------------------------------   p_S
1................1........1........11......1....................
..................1.........1......1............................
................................................................
................................................................
..........1.......1.........1...................................
----------------------------------------------------------------   p_L
.......1.........1.1......1.1......1.......1...........1......11
...1......1....1..1......1..1...1..1.....................1......
................................................................
................................................................
.....1....1......11......1..1......1...............1.......1....
```

Figure 4: 4-round trail with 43 [5, 9, 9, 20] active Sboxes and weight 132 [11, 36, 30, 55].

```
...1..1...........................................1.........1...
................1...1.............................1.............
................1...1.............................1.............
...1..1...........................................1.........1...
...1..1...........................................1.........1...
----------------------------------------------------------------   p_S
................................................................
................................................................
................................................................
...1..1...........................................1.........1...
................1...1.............................1.............
----------------------------------------------------------------   p_L
................................................................
................................................................
................................................................
................1...1..1..........................1.............
................1...1..1..........................1..........1..
----------------------------------------------------------------   p_S
.............................................................1..
.............................................................1..
................................................................
................................................................
................1...1..1..........................1.............
----------------------------------------------------------------   p_L
................1........1...................................1..
....................................1.....................1..1..
................................................................
................................................................
1...............1...1.........1...................1..........1..
----------------------------------------------------------------   p_S
................1........1...................................1..
1...................1....1....1...................1.............
................1...................1.....................1.....
....................1...............1.....................1.....
1...............1...1.........1...................1.............
----------------------------------------------------------------   p_L
...................................1.................1.......1..
.....1...........1..1.1....1..1........1.......1..1........1.1..
1...............11....1.............11....1...............11....
....1......1........1.........1.....11........1......1....1.....
1...............1...1..1......1......1...1........1..........1..
```

Figure 5: 4-round trail with 44 [6, 5, 9, 24] active Sboxes and weight 126 [13, 15, 25, 73].

```
..1.....................1..1....................................
............................1....1..............................
............................1....1..............................
..1.....................1..1....................................
..1.....................1..1....................................
----------------------------------------------------------------   p_S
................................................................
...........................11....1..............................
..1.....................1..1....................................
................................................................
................................................................
----------------------------------------------------------------   p_L
................................................................
..11....1...............11.11.1..1..............................
..11....1...............11.11.1..1..............................
................................................................
................................................................
----------------------------------------------------------------   p_S
................................................................
..11....1...............11.11.1..1..............................
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_L
................................................................
.....................11.....1....1.......11....1................
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_S
................................................................
................................................................
.....................11.....1....1.......11....1................
.....................11.....1....1.......11....1................
................................................................
----------------------------------------------------------------   p_L
................................................................
................................................................
.....................1.1...1.1...1.....1.1.1.........1..........
1....................11.....1..111.....1.111.1.1..111....111....
................................................................
```

Figure 6: 4-round trail with 44 [5, 9, 7, 23] active Sboxes and weight 119 [10, 18, 21, 70].

```
....................1.........1......1..1.......................
....................1.............................1...1.........
....................1.............................1...1.........
....................1.........1......1..1.......................
....................1.........1......1..1.......................
----------------------------------------------------------------   pS
................................................................
................................................................
................................................................
....................1.........1......1..1.......................
....................1.............................1...1.........
----------------------------------------------------------------   pL
................................................................
................................................................
................................................................
....................1.............................1...1..1......
....................1..........1..................1...1..1......
----------------------------------------------------------------   pS
...............................1.........................1......
...............................1................................
................................................................
................................................................
....................1.............................1...1.........
----------------------------------------------------------------   pL
............1........1.........1..................1......1.1....
......1.....................1..1................................
................................................................
................................................................
....................1..........1..................1...1..1......
----------------------------------------------------------------   pS
............1........1.........1..................1......1.1....
............1.......11................................1....1....
......1.....................1...................................
......1..............1......1...................................
....................1.............................1...1..1......
----------------------------------------------------------------   pL
.....1.................1.........................1.......1......
.........1..1....11.11.......1....1...................1.1...1...
......11....1...............11....1.............................
......1.........1....1.1....1..1.............1..................
1...................1..........1..1...............1...1.........
```

Figure 7: 4-round trail with 44 [6, 5, 10, 23] active Sboxes and weight 123 [13, 15, 25, 70].

```
...................................1.....1.............1..1.....
................1.........1......1....1.........1..1............
................1.........1......1....1.........1..1............
...................................1.....1.............1........
...................................1.....1.............1........
----------------------------------------------------------------   p_S
................................................................
................1.........1......1....1..1......1..1...1..1.....
................................................................
...................................1.....1.............1........
..........................................................1.....
----------------------------------------------------------------   p_L
................................................................
.1......1..........................1.....1...1.....11..1..1.....
................................................................
.1......1..........................1.....1...1.....11..1..1.....
.1.................................1......................1.....
----------------------------------------------------------------   p_S
.........................................1......................
................................................................
................................................................
.1......1..........................1.....1...1.....11..1..1.....
................................................................
----------------------------------------------------------------   p_L
.....1...................................1..................1...
................................................................
................................................................
.....1...................1.........1.....1...................1..
................................................................
----------------------------------------------------------------   p_S
.....1...................1.........1.....1..................11..
............................................................1...
................................................................
................................................................
.........................1.........1.........................1..
----------------------------------------------------------------   p_L
...............11................1.1.....1..1........11......1.1
...................................1.....................1..1...
................................................................
................................................................
..1.1.......1............1......1..1..1...1..................1..
```

Figure 8: 4-round trail with 44 [10, 9, 6, 19] active Sboxes and weight 123 [20, 36, 19, 48].

D Trails for 5 Rounds with 75 and 72 Active Sboxes

```
................1.....1.............1...........................
.......1......1....1.........1..1......1.....................1..
.......1......1....1.........1..1......1.....................1..
................1.....1.............1...........................
................1.....1.............1...........................
----------------------------------------------------------------   p_S
................................................................
.......1......1....1..1......1..1...1..1.....................1..
................................................................
................1.....1.............1...........................
................................................................
----------------------------------------------------------------   p_L
................................................................
................1.....1...1.....11..1..1......1......1..........
................................................................
................1.....1...1.....11..1..1......1......1..........
................................................................
----------------------------------------------------------------   p_S
................................................................
................................................................
................................................................
................1.....1...1.....11..1..1......1......1..........
................................................................
----------------------------------------------------------------   p_L
................................................................
................................................................
................................................................
......1.........1.....1...................1.......1.............
................................................................
----------------------------------------------------------------   p_S
......1.........1.....1...................1.......1.............
......................1...........................1.............
................................................................
......1.........................................................
......1.........1.....1...................1.......1.............
----------------------------------------------------------------   p_L
.....1........1.1.....1..1........11.....11.1................1..
...................1..1..1.....................1..1..........1..
................................................................
......1.........1......1........................................
......1......1..1..1..11...1.1............1....1.11............1
----------------------------------------------------------------   p_S
......1......1.........1.1.1......1......11......1..............
.....1.......11.1.....1....1.1....11.....1..1..1.11............1
.........................1.......................1...........1..
................1..............................................1
.....1........1....1.........1.....1......1.1..................1
----------------------------------------------------------------   p_L
....11.................1...1....1...........1.1..1.1...1....111.
....11...1.1..1..........111.1.11.11........1.1..11.11.1....11.1
...1.....................11....1.................11....1.....11.
.........1................1......1.............................1
.....1........1...........1..1.....11...1...1.1..1.1...1....1..1
```

Figure 9: 5-round trail with 75 [10, 9, 5, 21, 30] active Sboxes and weight 223 [20, 36, 15, 60, 92].

```
................................................................
1......1...............................1.1...................1..
1......1...............................1.1...................1..
................................................................
................................................................
----------------------------------------------------------------  p_S
................................................................
.......1.................................1......................
................................................................
................................................................
1......................................1.....................1..
----------------------------------------------------------------  p_L
................................................................
....1..1........1.....................1..1....1.................
................................................................
................................................................
1...1..1........1.....................11.1....1..............1..
----------------------------------------------------------------  p_S
................................................................
1......................................1.....................1..
................................................................
................................................................
1...1..1........1.....................11.1....1..............1..
----------------------------------------------------------------  p_L
................................................................
1.............1...........................................1.....
................................................................
................................................................
1..........1..11..1....................1.............1...1...1..
----------------------------------------------------------------  p_S
.......................................1.............1...1...1..
1..........1..11..1....................1.............1...1...1..
...............1..........................................1.....
1..........1...1.........................................11.....
...........1...1..1.............................................
----------------------------------------------------------------  p_L
...1....1...1...11...1...1.............1.............1...11..1..
1.......1...1.....1.........1...1.........................1.....
1..............11....1....................................11....
1..11..........1.1...1...1..1...1........................11.....
...........1...1......1..1..........................1...1..1....
----------------------------------------------------------------  p_S
...11...1...1....1...1.................1.............1...111.1..
...........1....1.....1..1..1..........1............11..1.11.1..
...1....1..11..11.1..1..............................1.....1.....
1...1...1......1.11..1...1..1...1........................1......
....1......1...1..1...1.............................1...1.......
----------------------------------------------------------------  p_L
....1........11.1........1.1....1......1.....1...1...1...1.1.1..
1..1....1..1.11.1..1.......1...1.11....1.........1..1......1....
1..11...1..1.111...1....1..1........................11.....1....
1..11...1.....11.........1.1...1..1..........1...1.......1......
....1..........1.........1.......1...........1..................
```

Figure 10: 5-round trail with 72 [5, 9, 10, 23, 25] active Sboxes and weight 225 [10, 33, 32, 74, 76].

E 5 Round Linear Trail with Squared Correlation 2^{-184}

```
..1......1......1............11.1....1............1...1..1..1..1
.........11.......................................1.1.1.1...1...
......................................................1..1.....1
.11......11.....1.1..........11.1..1..1.....11....1.1.1.1...1...
.1........1.......1................1.11.....11......1...11.....1
----------------------------------------------------------------   p_S
.1........1.......1................1.11.....11........1..1.....1
................................................................
................................................................
................................................................
..1......1......1............11.1....1............1.1...11..1..1
----------------------------------------------------------------   p_L
.........1...................1.......1...................1.....1
................................................................
................................................................
................................................................
.........1...................1.......1...................1.....1
----------------------------------------------------------------   p_S
................................................................
.........1...................1.......1...................1.....1
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_L
................................................................
..................1....1..1..........1..1.......1........1..1.1.
................................................................
................................................................
................................................................
----------------------------------------------------------------   p_S
................................................................
..................1....1..1..........1..1.......1........1..1.1.
................................................................
..................1....1..1..........1..1.......1........1..1.1.
................................................................
----------------------------------------------------------------   p_L
................................................................
.......................1.............1...................1......
................................................................
.1......1.........1.....................1..1...1..1......1..1...
................................................................
----------------------------------------------------------------   p_S
.1......1............................1...................1......
..................1....1.............1.....1.............1..1...
.....................................1..1..1...1..1......1..1...
.1......1.........1....1.............1..1..1...1..1.........1...
.1......1.........1....1.............1..1......1..1......1..1...
----------------------------------------------------------------   p_L
1........1........11.......1.1.......11................1.1......
.....................................1..1................1....1.
...........................................1..1.1..11.1...111...
..................1.....................1......1............1...
1.1.1..11....1....1.1....1.1.........11....1.1.11...1......1....
```

Figure 11: 5-round linear trail with 78 [21, 5, 9, 11, 30] active Sboxes and correlation 92 [21, 5, 18, 18, 30].

F New 4 Round Linear Trails with 43 Active Sboxes

```
....1..1..1..1....11.11......1........1....11....1..1..........1
...11.......11...1.1.11....................11...11.......1.....1
...11..1....1....1....1..................1.11...1........1.....1
1...1..1...........1.1............1.............................
1...1..1..1..1....1..1.......1....1...1....11....1..1...........
----------------------------------------------------------------  p_S
.............1........1..................1......................
....1..1..1.......11.11......1........1..1.11....1..1..........1
...11.......11...1.1.......................1....11.......1.....1
................................................................
1.................................1......1......................
----------------------------------------------------------------  p_L
.........................................1......................
....1.............11..................1..........1..............
....1.............11.............................1.............1
................................................................
.........................................1......................
----------------------------------------------------------------  p_S
................................................................
......................................1..1.....................1
................................................................
....1.............11..................1..........1.............1
................................................................
----------------------------------------------------------------  p_L
................................................................
......................................1.........................
................................................................
..1......1.........1.1......1.........1.........................
................................................................
----------------------------------------------------------------  p_S
..1................1........1.........1.........................
................................................................
.........1.........1.1..........................................
..1......1.........1.1......1.........1.........................
................................................................
----------------------------------------------------------------  p_L
..1............................................1................
................................................................
...............1....11..........................................
...................1..................1.........................
................................................................
```

Figure 12: 4-round linear trail with 43 [23, 7, 6, 7] active Sboxes and correlation 56 [30 9 10 7].

```
.............1..1............1.......11.....11.1..1.1.1.11.....1
.............................1.......1......1.........1..1......
.....................................11.....11..................
.1........1..1..1.1..........1........1......1.1..1.1.1.1......1
.1........1.......1......................................1......
----------------------------------------------------------------  p_S
.1........1.......1..................11......1........1..1......
................................................................
................................................................
.....................................1......1.........1.........
.............1..1............1.................1..1.1.1.11.....1
----------------------------------------------------------------  p_L
.........1...................1.......1...................1......
................................................................
................................................................
......................................................1.........
.............................1........................1..1.....1
----------------------------------------------------------------  p_S
.........1...........................1................1........1
.........1...................1.......1...................1.....1
................................................................
................................................................
................................................................
----------------------------------------------------------------  p_L
..................1..................1..........................
..................1....1..1..........1..1.......1........1..1.1.
................................................................
................................................................
................................................................
----------------------------------------------------------------  p_S
................................................................
..................1....1..1..........1..1.......1........1..1.1.
................................................................
..................1....1..1..........1..1.......1........1..1.1.
................................................................
----------------------------------------------------------------  p_L
................................................................
.......................1.............1...................1......
................................................................
.1......1.........1.....................1..1...1..1......1..1...
................................................................
```

Figure 13: 4-round linear trail with 43 [17, 6, 9, 11] active Sboxes and correlation 57 [19 9 18 11].

```
1...1..1..1.....1.....1......1...................1..1.1.........
1..1...1....11.....1..1...........1........1....1.....11.1.....1
...1...1....1.........1..................1.1....1.....1..1......
....1.......11....11..1...........1......1.......1....11.......1
1...1.....1..1..1.11.........1....1..............1..1..1.......1
----------------------------------------------------------------   p_S
1............1....11..1..................1............11.......1
....1..1..1..1..1............1...........1.......1..1..........1
...11..1....11.............................1....11.......1.....1
................................................................
1.................................1......1......................
----------------------------------------------------------------   p_L
..................11.....................1......................
....1........1........................1..........1..............
....1........1...................................1.............1
................................................................
.........................................1......................
----------------------------------------------------------------   p_S
................................................................
......................................1..1.....................1
.............1....11............................................
....1.............11..................1..........1.............1
................................................................
----------------------------------------------------------------   p_L
................................................................
......................................1.........................
...................1............................................
..1......1.........1.1......1.........1.........................
................................................................
----------------------------------------------------------------   p_S
..1................1........1.........1.........................
................................................................
.........1.........1.1..........................................
..1......1.........1.1......1.........1.........................
................................................................
----------------------------------------------------------------   p_L
..1............................................1................
................................................................
...............1....11..........................................
...................1..................1.........................
................................................................
```

Figure 14: 4-round linear trail with 43 [22, 8, 6, 7] active Sboxes and correlation 54 [27 10 10 7].