IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2021, No. 2, pp. 353–388. DOI:10.46586/tosc.v2021.i2.353-388

Provable Security of SP Networks with Partial Non-Linear Layers

Chun Guo[123], François-Xavier Standaert[4](✉), Weijia Wang[123](✉), Xiao Wang[5] and Yu Yu[6]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China chun.guo@sdu.edu.cn,fstandae@uclouvain.be,wjwang@sdu.edu.cn,wangxiao@northwestern.edu,yuyu@yuyu.hk
[2] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China
[3] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)
[4] ICTEAM/ELEN/Crypto Group, UCLouvain, Louvain-la-Neuve, Belgium
[5] Northwestern University, Evanston, Illinois, USA
[6] Shanghai Jiao Tong University, Shanghai, China

Abstract. Motivated by the recent trend towards low multiplicative complexity blockciphers (e.g., Zorro, CHES 2013; LowMC, EUROCRYPT 2015; HADES, EUROCRYPT 2020; MALICIOUS, CRYPTO 2020), we study their underlying structure *partial SPNs*, i.e., Substitution-Permutation Networks (SPNs) with parts of the substitution layer replaced by an identity mapping, and put forward the first provable security analysis for such partial SPNs built upon *dedicated linear layers*. For different instances of partial SPNs using MDS linear layers, we establish strong pseudorandom security as well as practical provable security against impossible differential attacks. By extending the well-established MDS code-based idea, we also propose the first principled design of linear layers that ensures optimal differential propagation. Our results formally confirm the conjecture that partial SPNs achieve the same security as normal SPNs while consuming less non-linearity, in a well-established framework.

Keywords: blockciphers · substitution-permutation networks · provable security · LowMC · low multiplicative complexity

1 Introduction

Blockciphers are one of the most prominently used cryptographic primitives. The classical approaches to the design of blockciphers include Feistel networks and substitution-permutation networks (SPNs), with DES and AES as well-known examples. A Feistel round applies a domain-preserving function (sometimes non-invertible, as in DES) on half of the data, and then executes XOR and swap operations, see Fig. 1 (a). This can be generalized along multiple axes, e.g., employing other group operations instead of XOR, employing contracting or expanding round functions, and employing more than 2 data chunks to constitute the so-called multi-line Type-II generalized Feistel networks (see Fig. 1 (b)). An SPN round, on the other hand, consists of parallel application of many instances of small S-box on the "full" data (divided equally into many chunks), composed with a (typically linear) transformation T, see Fig. 1 (c). In fact, as stated in [KL15, Chapter 6.2], the design of modern blockciphers is dominated by (generalized) Feistel networks (including the Lai-Massey structure of the cipher IDEA [LM91], which may be viewed as a sophisticated variant of Feistel [YPL11]), and SP networks.

Received: 2020-11-23 Revised: 2021-03-01 Accepted: 2021-05-01 Published: 2021-06-11

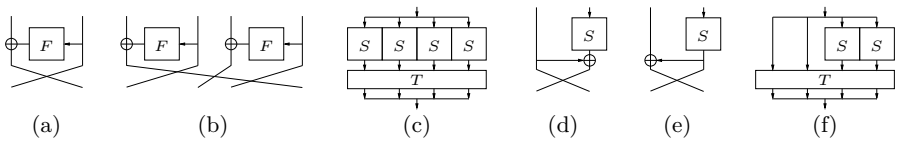

Figure 1: Different blockcipher structures. (a) Feistel network; (b) multi-line generalized Feistel, with 4 chunks; (c) the normal SPN; (d) Misty-L; (e) Misty-R; (f) partial SPN.

Despite the dominance of Feistel and SP networks, there remain a few important exceptions. At FSE 1997, Matsui introduced a blockcipher MISTY2 [Mat97] following a novel structure that somewhat resembles Feistel networks, but crucially relies on the invertibility of the round function (thus distinct from Feistel ciphers). The structure and its dual were later named Misty-L [GM02], see Fig. 1 (d), and Misty-R, see Fig. 1 (e), respectively.

This paper focuses on another notable exception. A recent trend initiated by Gérard et al. [GGNS13] is to base blockciphers on a variant of SP networks, in which parts of the S-box evaluations are replaced by an identity mapping. See Fig. 1 (f) for an illustration. This structure was named *SP network with partial non-linear layers* by Bar-On et al. [BDD+15], and we abbreviate it as P-SPN. In each round, the ratio between the number of S-box evaluations and w, the total number of data chunks, is henceforth referred to as its *rate*, and denoted r.

The motivation of Gérard et al. is that, to implement the cipher in a side-channel masked form, non-linear operations incur a higher performance penalty compared to linear ones. The structure P-SPN was thus proposed to reduce the amount of non-linearity (without harming security, hopefully) and produce low multiplicative complexity ciphers. For example, assuming wr S-box evaluations per round. If such a P-SPN with $\lambda' < \lambda/r$ rounds achieves the same (or comparable) security as a λ-round normal SPN, then the amount of non-linearity of the former is less than the latter. This is reflected by the comparison w.r.t. the total number of S-box evaluations, that is, $\lambda' wr < \lambda w$ (a similar example was also mentioned in [GGNS13, Sect. 3]). With these in mind, Gérard et al. "dropped" many S-boxes in the AES to obtain the P-SPN cipher Zorro, which was unfortunately broken and even its strategy of tweaking AES into P-SPN was shown flawed [BDD+15]. As compensation, the authors of [BDD+15] revitalized P-SPN by developing an algorithm for searching its characteristics and showing its potential to build blockciphers with reliable security against differential/linear cryptanalysis. Although Gérard et al.'s original scenario was intended for masking, the idea of reducing multiplicative complexity finds applications in other cryptographic settings, such as multi-party computation and zero-knowledge proofs. For example, the LowMC blockcipher [ARS+15], hash functions Starkad and Poseidon, and the recent HADES design [GKK+19, GLR+20]. In particular, thanks to the efficiency and low non-linearity of P-SPN, LowMC has been used in Picnic [ZCD+19] (a round-2 candidate in NIST's post-quantum cryptography standardization project) and the Dusk Network project [git19]. A recent more surprising design was the MALICIOUS framework of Peyrin and Wang [PW20], which leverages the features of partial SPNs to enable embedding backdoors into tweakable blockciphers.

As shown in Fig. 1, P-SPNs can be viewed as generalizations of both Misty (with smaller data chunks and stronger linear layers) and normal SPNs, unifying the two structures in some sense. This makes the study of P-SPNs theoretically interesting in its own right. This along with its additional popularity in real applications has motivated several works: besides the aforementioned searching tool [BDD+15], Dinur et al. formalized the equivalence relation between P-SPN ciphers [DKP+19], and the LowMC designers proved security against certain attacks for LowMC or P-SPNs using independent *random linear*

layers [ARS+15]. Though, theoretical analysis of P-SPNs with principled linear layers remain largely blank. This severely hinders its understanding. In particular, it remains an important open problem whether P-SPNs with less non-linearity can preserve the same security as the standard SPNs in a provable manner.

1.1 Our Contribution

We provide systematic analyses of partial SPNs, regarding strong pseudorandom permutation (SPRP) security, provable security against Impossible Differential (ID) and Zero-Correlation linear (ZC) attacks, and diffusion. Our results are as follows.

- In Sect. 3, we prove that a 5-round P-SPN with rate 1/2 is an SPRP, where the cost of $5w/2$ S-box calls is *less than* that of a normal (linear) SPN ($3w$ calls [DKS+17, CDK+18]). This P-SPN construction relies on an MDS linear layer that fulfill some additional requirements.

- In Sect. 4, we show that 4-round P-SPNs with rate at least 3/4 and *MDS linear layers* are secure against ID and ZC attacks. This *saves one round* compared to the AES-like structure, which needs 5 rounds for the same security [SLG+16].

- For P-SPNs with rate $r < 1/2$, $r^{-1} \in \mathbb{N}$, we propose the *first principled linear layers constructed from MDS codes*. Our proposal consists of $r^{-1}-1$ different transformations, and achieve a minimum security criteria, i.e., no r^{-1}-round differential with probability one. See Sect. 5 for details.

In all, our results (and the comparisons to existing results on AES-like SPNs) have justified the soundness of P-SPNs: as approaches to constructing efficient blockciphers, *P-SPNs could be comparable to, or even surpass the normal SPNs, in some well-defined sense*. Below we will elaborate in detail.

1.1.1 Small-box cryptography, and SPRP security with rate 1/2

With a model recently put forward by Dodis et al. [DKS+17, CDK+18], i.e., modeling the S-boxes as small ideal primitives and the linear layers as efficient functions, it turns possible to study the security of P-SPNs from a theoretical point of view. The S-boxes act as the only source of cryptographic hardness. This methodology was termed "small-box cryptography" by Dodis [Dod18], to highlight the deviation from the classical practice-oriented provable security based on large-domain primitives (e.g., based on the AES). Actually, in the past decades, various structures, including the standard SPNs [IK01, MV15, DSSL16] and the multi-line generalized Feistel networks (GFNs) [ZMI90, IK01, MV00, SM10, HR10, BFMT16], have been studied in this model, enabling comparisons.

In light of this, assuming that each round calls a *public random n-bit permutation* as the S-box and a strong linear layer, we prove that a 5-round rate 1/2 P-SPN is a strong pseudorandom permutation (SPRP), up to $2^{n/2}$ queries the classical birthday security (like the Luby-Rackoff result [LR88]). To ensure this result, the linear layer shall achieve stronger diffusion than a general MDS transformation. This indeed matches intuitions.

Our SPRP results on P-SPNs not only provide support for its reliability—as reliable as the more common SPNs and GFNs, but also enable comparisons. For clarity, we list known wide SPRP constructions in Table 1. Here we focus on the so-called "linear structures" of Nandi [Nan15], in which block functions/S-boxes constitute the only source of non-linearity. It is easy to make a fair comparison between linear structures: relative multiplicative complexity (MC) is reflected by the total number of S-boxes, while relative AND Depth is reflected by the maximum number of S-boxes on any path from an input data chunk to

Table 1: Comparison to existing wide SPRP structures. The *Rounds* column presents the number of rounds sufficient for birthday-bound security, where $\lambda(w) = \lceil \log_2 1.44w \rceil$. For Type-II GFN (i.e., GFNs with $w/2$ block functions per round, see Fig. 1 (b)), note that $2\lambda(w) = 2\lceil \log_2 1.44w \rceil \geq 6$ when $w \geq 4$. Parameters in the *MC* and *AND Depth* columns are relative w.r.t. the S-box. The mode XLS [RR07] is not included due to attacks [Nan14, Nan15].

Structure	Rounds	MC	AND Depth	Reference
Optimal Type-II GFN	$2\lambda(w)$	$w\lambda(w)$	$2\lambda(w)$	[SM10, DFLM19]
Extended Type-II GFN	10	$5w$	10	[BFMT16, Theorems 7,8]
Linear SPN	3	$3w$	3	[DKS+17]
CMC	-	$2w$	$2w$	[HR03]
EME & EME*	-	$2w + 1$	3	[HR04, Hal04]
Rate 1/2 P-SPN	**5**	$\mathbf{2.5}w$	**5**	Theorem 1

an output chunk, see Table 1.[1] Note that classical blockcipher structures GFNs and linear SPN are all linear structures. On the other hand, the structures CMC, EME and EME* were designed as *wide SPRP encryption modes* rather than blockcipher structures—indeed, CMC is sequential, as indicated by its huge AND Depth. Regarding classical blockcipher structures, the relative MC $5w/2$ of rate 1/2 P-SPNs is less than that of the normal linear SPN (which is $3w$), and this confirms the conjecture of less non-linearity. Also, rate 1/2 P-SPNs outperform the best GFNs definitively.

Implications for small block size. With the "small-box cryptography" methodology, provable security is limited by the domain of the small ideal S-boxes, to e.g. at most 8-bit security for the AES parameter. Admittedly, this restriction renders the proved security meaningless for any concrete P-SPN blockciphers. For example, LowMC uses 3-bit small S-boxes, and thus our $n/2$-bit bounds indicate security up to $2^{1.5}$ queries. However, we stress that new blockcipher structures are typically accomplished by such small-box provable security justifications, and we refer to Zheng et al.'s proof for their proposal of multi-line GFNs [ZMI90], Iwata and Kurosawa's proof for Serpent-like SPNs [IK01], Suzaki and Minematsu's proof for their proposal of GFNs with optimal shuffles [SM10], and Berger et al.'s proof for their proposal of extended GFNs [BFMT16] as examples. By these, while the terminology was new [Dod18], the methodology has been proposed decades ago and *recognized* as an important sanity check—particularly for the soundness of *new structures*. With P-SPNs popularized in these years, the lack of such a justification has thus been an important gap.

Meanwhile, with various structures studied in the same model [IK01, MV15, DSSL16, IK01, MV00, SM10, HR10, BFMT16], our results enable fair comparisons, which again justifies the soundness of P-SPNs: as approaches to constructing efficient blockciphers, *P-SPNs could be comparable to, or even surpass the normal SPNs, in some well-defined sense.*

1.1.2 Provable security of P-SPN structures against truncated IDs

Given the theoretical SPRP results we have, a first question is whether they lead to tight design guidelines (for the selection of the linear layer and the number of rounds). To this end, we also examine practical provable security of P-SPNs against two important classes of attacks, namely Impossible Differential (ID) and Zero-Correlation linear (ZC) attacks, and show the plausibility to trade the complexity of linear layers for less rounds.

[1] On the other hand, comparison turns difficult for SPRPs using field multiplications (e.g., [NR99]) or tweakable blockciphers (e.g., [BLN18]).

In detail, ID attacks were introduced in the 1990s [BBS99], and exhibited differentials with probability 0 to distinguish the cipher from random. ZC attacks were introduced in 2011 [BR14, BW12], and leveraged linear hulls with correlation zero for distinguishing. Both have become major cryptanalysis techniques. For a dedicated iterated blockcipher, there always exist IDs and ZCs for any rounds with some keys. Though, being effective for only a small set of weak keys, such distinguishers are useless. To remedy this and to retain generality, we follow [SLR+15, SLG+16] and concentrate on truncated IDs and ZCs on *P-SPN structures* $\mathcal{E}_{\text{P-SPN}}$. Such models capture *IDs and ZCs that are independent of the secret keys as well as the concrete S-boxes*, and we refer to Sect. 2.4 for formal definitions.

As results, we prove that for P-SPN structures $\mathcal{E}_{\text{P-SPN}}$ with MDS linear layers and *rate at least 3/4, there do not exist 4-round truncated ID distinguishers*. In other words, no 4-round impossible differential exists in such P-SPNs*unless the details of the S-boxes are taken into account*. As complement, we also show that 3-round IDs always exist as long as the rate is less than 1, thus 4-round is optimal. By the links between cryptanalytic techniques, security against ZC attacks is also established. These demonstrate insights to the longest possible ID and ZC distinguishers on P-SPNs.

In [BDD+15, Sect. 6.2], it was conjectured that trading the amount of non-linearity for stronger linear layers mitigates "structural attacks", which in that particular context refers to ID, zero-correlation linear, and integral attacks. *This is confirmed by our results, since 4-round AES-like structures do admit ID distinguishers*. For AES-like structures, provable security against generic IDs is only achieved with ≥ 5 rounds [SLG+16], which is one more round than rate 3/4 MDS-based P-SPNs.

On the other hand, we stress that this does not mean P-SPNs are stronger than SPNs in general. Indeed, AES-like SPNs are using composed linear layers that are much weaker than huge MDS transformations, and if the latter are adopted, [SLG+16, Theorem 2] implies that even 3 rounds are already sufficient for generic ID security. Though, it could indeed be beneficial to *use stronger linear layers and less S-boxes*.

We also attempted for better provable bounds against differential and linear attacks. Yet, our conclusions are mostly negative, admitting the difficulty to establish them by pencil and paper. This is in accordance with [BDD+15], in which an automated searching tool was developed for provable differential bounds. For the sake of space, we include these results in Appendix D (we don't view this as our main results).

1.1.3 Linear layers for small rate P-SPNs

Another important question is whether the P-SPN approach could be pushed towards low rates and what would be the corresponding design guideline for the linear layer(s). Typically, the design principle of linear layers is to ensure *a maximum number of active S-boxes in differential/linear characteristics*. It has been known that an MDS transformation M achieve this in normal SPNs: the idea is to connect $\{x\|M \cdot x\}_{x\in\{0,1\}^{wn},x\neq 0}$ with a set of MDS codewords. Though, this idea can only ensure properties within the differences in two consecutive rounds. For a P-SPN with rate r, $r^{-1} \in \mathbb{N}$, this appears insufficient: it has been noticed that for $r^{-1}-1$ rounds, there always exist differential paths with probability 1 [BDD+15]. By this, the very least requirement for a good linear layer is to ensure that *no r^{-1}-round probability-1 differential path exist*. But this requires to address dependencies between differences in consecutive r^{-1} rounds, which seems quite intricate. Moreover, classical blockciphers typically employ *the same* linear layer in all rounds, and it is extremely difficult to identify a linear layer that ensures complicated properties as mentioned. Due to this gap, LowMC employed "independent random linear layers" to simplify the security analysis, and the designers have left dedicated linear layers with solid theory foundation as an open problem [ARS+15, Conclusion].

We address this question. Our idea is a natural extension of the above MDS idea: for rate r, we construct $r^{-1}-1$ linear transformations $T_{M1},\ldots,T_{Mr^{-1}-1}$, so that $\{x\|T_{M1}\cdot$

$x\| \dots \|(\prod_{i=r^{-1}-1}^{1} T_{Mi}) \cdot x\}_{x \in \{0,1\}^{wn}, x \neq 0}$ is linked to a long MDS code. The MDS property ensures at least $(r^{-1}-1)w+1$ active chunks in $x\| \dots \|(\prod_{i=r^{-1}-1}^{1} T_{Mi}) \cdot x$, which implies at least 1 active S-box in r^{-1} rounds.

Of course, the above proposals need refinements as well as more validations before being used in real blockciphers. Though, it is important to make this first step. In addition, this shows *instead of using independent linear layers to simplify the situation, we can indeed use dependent ones and leverage the dependence for the security arguments.* Further improved designs probably require optimized searching algorithms or heavy coding theory tools.

1.2 Related Work

A concurrent and independent work of Grassi, Rechberger, and Schofnegger (GRS) [GRS20] exhibited conditions on P-SPN linear layers that are sufficient and necessary for the existence of iterative subspace trails with probability 1. These in particular include truncated differential trails, which creates strong resemblance between GRS and our linear layers. While both results imply the non-existence of "obvious" differential attacks on infinite rounds, we remark that regarding differential trails *with no active S-boxes*, our linear layers ensure *stronger security* than GRS, since

$$\begin{aligned} & \underbrace{\text{non-existence of } r^{-1}\text{-round probability-1 differential path}}_{\text{Our security goal}} \\ \implies & \text{non-existence of infinite probability-1 differential path} \\ \implies & \underbrace{\text{non-existence of iterative probability-1 differential path}}_{\text{One of GRS's goals}} \end{aligned}$$

Actually we identify sufficient conditions for *the best possible differential security within $1/r$ rounds*, which might be the first step towards lower bounds on the number of active S-boxes. In addition, we also provide a *solid approach* towards constructing *a series of linear layers* with desirable properties.

The advantages of GRS's work are as follows.

- First, GRS's proposal uses only a single linear permutation $T \in \mathbb{F}^{w \times w}$ that provides full diffusion after a finite number of rounds. This is simpler than our $r^{-1}-1$ transformations. In particular, they showed that the MDS property is not needed for their goals.[2]
- Second, GRS also studied preventing iterative truncated differentials *with active S-boxes*, which is an important issue not addressed by us.

In summary, the results of GRS and ours are somewhat incompatible and complementary. We are currently unable to extend our treatment to (the more practical case with) more than r^{-1} rounds, while GRS result does not ensure lower bounds on the number of active S-boxes. Both results could be starting points for future works.

1.3 Organization

We establish notations and models in Sect. 2. Then in Sect. 3, we study the SPRP security of rate 1/2 P-SPNs; in Sect. 4, we study the security of P-SPNs against generic IDs and ZCs; in Sect. 5, we present our extended MDS code-based linear layers. We finally conclude in Sect. 6.

[2] Our proposal relies on MDS since we aim at stronger security.

2 Preliminaries

For any positive integer m, we write $\mathcal{P}(m)$ for the set of permutations of $\{0,1\}^m$. We view n as a cryptographic security parameter and let $\mathbb{F} := \mathrm{GF}(2^n)$, which is identified with $\{0,1\}^n$. The zero entry of $\mathbb{F}$ is denoted by $\mathsf{0}$ (the sans serif typestyle).

Following the cryptographic convention, a wn-bit string $x \in \{0,1\}^{wn}$ is also viewed as a *column vector* in $\mathbb{F}^w$. Hence, x^T is a row vector obtained by transposing x. Indeed, bit strings and column vectors are just two sides of the same coin. Throughout the remaining, depending on the context, the same notation, e.g., x, may refer to both a bit string and a column vector, *without additional highlight*. In the same vein, the concatenation $x\|y$ is also "semantically equivalent" to the column vector

$$\begin{pmatrix} x \\ y \end{pmatrix}.$$

In this respect, for $x \in \mathbb{F}^w$, we denote the j th entry of x (for $j \in \{1,\ldots,w\}$) by $x[j]$, and define $x[a..b] := (x[a],\ldots,x[b])$ for any integers $1 \le a < b \le w$. Given an n-bit permutation S, for any positive integer m and any vector $x \in \mathbb{F}^m$, we define $\overline{S}(x) := \big(S(x[1]),\ldots,S(x[m])\big)$; we write $\mathsf{0}^m$ for the all-zero vector in $\mathbb{F}^m$, which also represents the all-zero string of length mn by our convention. For integers $1 \le b \le a$, we write $(a)_b := a(a-1)\ldots(a-b+1)$ and $(a)_0 := 1$ by convention.

MDS transformations. For any (column) vector $x \in \mathbb{F}^w$, the *Hamming weight* of x is defined as the number of non-zero entries of x, i.e.,

$$\mathsf{wt}(x) := \big|\{i | x[i] \neq \mathsf{0}, i = 1,\ldots,w\}\big|.$$

Let $T \in \mathbb{F}^{w\times w}$, then the *branch number* of T (from the viewpoint of differential cryptanalysis) is defined as $\min_{x\in\mathbb{F}^w, x\neq\mathsf{0}}\{\mathsf{wt}(x) + \mathsf{wt}(T\cdot x)\}$. A matrix $T \in \mathbb{F}^{w\times w}$ reaching $w+1$, the upper bound on such branch numbers, is called *Maximum Distance Separable* (MDS). MDS matrices have been widely used in modern blockciphers including the AES, since the ensured lower bounds on weights typically transform into bounds on the number of active S-boxes (i.e., S-boxes with non-zero input differences).

2.1 P-SPN: SP Networks with Partial Non-linear Layers

To ease a comparison, we first recall the standard *Substitution-Permutation Networks (SPNs)*. An SPN defines a keyed permutation via repeated invocation of three transformations:[3] addition of a round key, blockwise computation of a public, cryptographic permutation called an "S-box", and application of a linear permutation. Formally, a λ-round SPN taking inputs of length wn where $w \in \mathbb{N}$ is the *width* of the network, is defined by a distribution $\mathcal{K}$ over $K_0 \times \ldots \times K_\lambda$, λ permutations $\mathcal{S} = \{S_i : \{0,1\}^n \to \{0,1\}^n\}_{i=1}^{\lambda}$,[4] and $\lambda - 1$ linear permutations $\{T_i \in \mathbb{F}^{w\times w}\}_{i=1}^{\lambda-1}$. This is close to the practice of key-alternating ciphers such as the AES. Given round keys $k_0,\ldots,k_\lambda \in K_0 \times \ldots \times K_\lambda$ and input $x \in \{0,1\}^{wn}$, the computation of the SPN is described in Fig. 2 (left). One may also see Fig. 3 (left) for an illustration.

A partial SP-network P-SPN is very similar to an SPN, except that its S-box layer contains less than w S-box evaluations, as shown in Fig. 2 (right). We call the proportion of S-box evaluations its *rate*. E.g., if each round consists of $w/2$ S-box evaluations, then the rate is $r = 1/2$. If $S_1,\ldots,S_\lambda$ are efficiently invertible and each T_i is efficiently invertible, then both computations in Fig. 2 are reversible given the round keys $k_0,\ldots,k_\lambda$. Also see Fig. 3 (right) for illustration.

[3] SPNs also yield *keyless cryptographic permutations*. Though, this paper focuses on keyed SPNs.

[4] Using different S-boxes in different rounds follows [CDK+18, Sect. 4.2]. Though, earlier work [DKS+17] assumed the same S-box in every round.

$\mathbf{SPN}^{\mathcal{S}}_{\mathbf{k}}(x)$
// $\mathcal{S} = \{S_1, \ldots, S_\lambda\}$
$u_1 := k_0 \oplus x$
for $i = 1, \ldots, \lambda - 1$ **do**
  $v_i := \overline{S_i}(u_i)$
  $u_{i+1} := k_i \oplus T_i \cdot v_i$
end for
$v_\lambda := \overline{S_\lambda}(u_\lambda)$
$u_{\lambda+1} := k_\lambda \oplus v_\lambda$
Outputs $u_{\lambda+1}$.

$\mathbf{P\text{-}SPN}^{\mathcal{S}}_{\mathbf{k}}(x)$ // $\mathcal{S} = \{S_1, \ldots, S_\lambda\}$
$u_1 := k_0 \oplus x$
for $i = 1, \ldots, \lambda - 1$ **do**
  $v_i := \mathsf{PS}^{S_i}(u_i, r)$, where
    $\mathsf{PS}^{S_i}(x_i, r) := x_i[1..w(1-r)] \,\|\, \overline{S_i}\big(x_i[w(1-r)+1..w]\big)$
  $u_{i+1} := k_i \oplus T_i \cdot v_i$
end for
$v_\lambda := \mathsf{PS}^{S_\lambda}(u_\lambda, r)$
$u_{\lambda+1} := k_\lambda \oplus v_\lambda$
Outputs $u_{\lambda+1}$.

Figure 2: The computation flows in λ-round SPN and P-SPN upon input x.

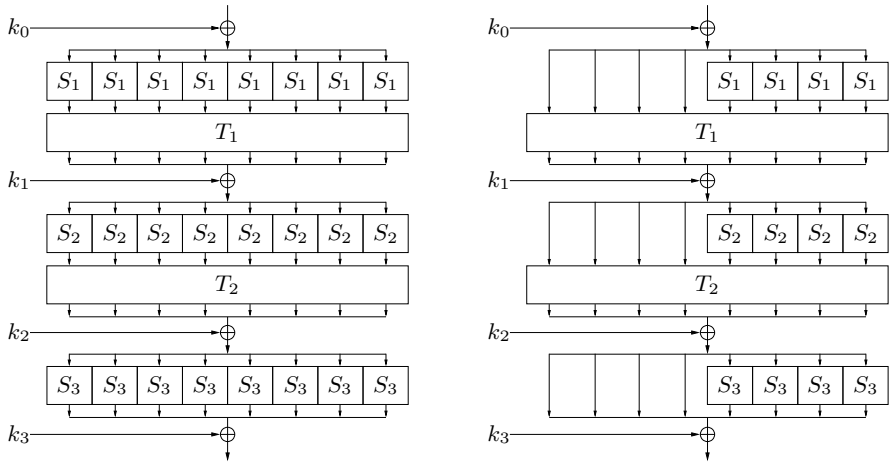

Figure 3: SP and partial SP networks, with $w = 8$. (Left) the 3-round linear SPN proved secure in [DKS+17] (the proof in [DKS+17] assumed identical S-box, i.e., $S_1 = S_2 = S_3$); (Right) a 3-round linear P-SPN with rate 1/2, which will be broken in Sect. A.

Dodis et al. presented a more general model for SPNs [CDK+18], which essentially allows for non-linear permutations instead of the linear $T_1, ..., T_{\lambda-1}$. In this paper we only consider the above specific models using linear permutations, both for simplicity and for consistency with the very motivation of using P-SPNs (i.e., to *reduce* the amount of non-linearity). We refer to [CDK+18] for a complete discussion on the models.

2.2 SPRP Security of P-SPNs, and the H-coefficient Technique

Following [DKS+17, CDK+18], we consider P-SPN constructions that are defined by linear permutations $\{T_i \in \mathbb{F}^{w \times w}\}_{i=1}^{\lambda-1}$ and a distribution $\mathcal{K}$, and that take *oracle* access to λ public, random permutations $\mathcal{S} = \{S_i : \{0,1\}^n \to \{0,1\}^n\}_{i=0}^{\lambda}$; we write this as $\text{P-SPN}^{\mathcal{S}}_{\mathbf{k}}$, where $\mathbf{k} = (k_0, \ldots, k_\lambda)$. We then analyze security of the construction against unbounded-time attackers making a bounded number of queries to the construction and to $\mathcal{S}$. Formally, we consider the ability of an adversary D to distinguish two worlds: the "real world", in which it is given oracle access to $\mathcal{S}$ and $\text{P-SPN}^{\mathcal{S}}_{\mathbf{k}}$ (for unknown keys $\mathbf{k}$ sampled according to $\mathcal{K}$), and an "ideal world" in which it has access to $\mathcal{S}$ and a random permutation $P : \{0,1\}^{wn} \to \{0,1\}^{wn}$. By default, we always allow D to make forward and inverse queries to all its oracles (though we do not write this explicitly). With these, for a distinguisher D, we define its *strong-PRP advantage* against the construction $\mathcal{C}$ as

$$\mathsf{Adv}^{\mathsf{sprp}}_{\mathcal{C}}(D) := \Big| \Pr\left[\mathbf{k} \leftarrow \mathcal{K} : D^{\mathcal{C}^{\mathcal{S}}_{\mathbf{k}}, \mathcal{S}} = 1\right] - \Pr\left[P \xleftarrow{\$} \mathcal{P}(wn) : D^{P, \mathcal{S}} = 1\right] \Big|,$$

where $\mathcal{S} = (S_1, \ldots, S_\lambda)$ are λ independent, uniform permutations on $\{0,1\}^n$. The *strong-PRP (SPRP) security* of $\mathcal{C}$, is

$$\mathsf{Adv}^{\mathsf{sprp}}_{\mathcal{C}}(q_C, q_S) := \max_D \left\{\mathsf{Adv}^{\mathsf{sprp}}_{\mathcal{C}}(D)\right\},$$

where the maximum is taken over all distinguishers that make at most q_C queries to their left oracle and q_S queries to their right oracles.

We use Patarin's H-coefficient technique [Pat09] to prove SPRP security of P-SPNs. We provide a quick overview of its main ingredients here. Our presentation borrows heavily from that of [CS14]. Fix a distinguisher D that makes at most q queries to its oracles. As in the security definition presented above, D's aim is to distinguish between two worlds: a "real world" and an "ideal world". Assume wlog that D is deterministic. The execution of D defines a *transcript* that includes the sequence of queries and answers received from its oracles; D's output is a deterministic function of its transcript. Thus, if μ, ν denote the probability distributions on transcripts induced by the real and ideal worlds, respectively, then D's distinguishing advantage is upper bounded by the statistical distance

$$\mathsf{Dist}(\mu, \nu) := \frac{1}{2}\sum_\tau \big|\mu(\tau) - \nu(\tau)\big|, \tag{1}$$

where the sum is taken over all possible transcripts τ.

Let $\mathcal{T}$ denote the set of all transcripts such that $\nu(\tau) > 0$ for all $\tau \in \mathcal{T}$. We look for a partition of $\mathcal{T}$ into two sets $\mathcal{T}_1$ and $\mathcal{T}_2$ of "good" and "bad" transcripts, respectively, along with a constant $\epsilon_1 \in [0, 1)$ such that

$$\tau \in \mathcal{T}_1 \Longrightarrow \mu(\tau)/\nu(\tau) \geq 1 - \epsilon_1. \tag{2}$$

It is then possible to show (see [CS14] for details) that

$$\mathsf{Dist}(\mu, \nu) \leq \epsilon_1 + \Pr[\nu \in \mathcal{T}_2] \tag{3}$$

is an upper bound on the distinguisher's advantage.

2.3 Impossible Differential and Zero-Correlation Linear Cryptanalysis

Let $\Delta_1 \in \mathbb{F}^w$ and $\Delta_2 \in \mathbb{F}^w$. The differential probability of $\Delta_1 \to \Delta_2$ is defined as

$$\Pr\left(\Delta_1 \xrightarrow{G} \Delta_2\right) := \frac{\left|\{x \in \mathbb{F}^w \mid G(x) \oplus G(x \oplus \Delta_1) = \Delta_2\}\right|}{2^{wn}}.$$

Following [BBS99], if $\Pr(\Delta_1 \xrightarrow{G} \Delta_2) = 0$, then $\Delta_1 \to \Delta_2$ is called an *Impossible Differential (ID)* of G, which also enables distinguishing and cryptanalysis.

Let $\mathsf{sgn} : \mathbb{F} \to \{0,1\}$ be defined as

$$\mathsf{sgn}(a) := \begin{cases} 0 & a = 0, \\ 1 & a \neq 0. \end{cases}$$

Then, for $x = (x[1], \ldots, x[w]) \in \mathbb{F}^w$, we define $\chi(x) := (\mathsf{sgn}(x[1]), \ldots, \mathsf{sgn}(x[w])) \in \{0,1\}^w$, which, in some sense, summarizes the "pattern" of the vector x.

Let $\alpha, x \in \{0,1\}^{wn}$, and let $\langle \alpha, x\rangle$ be the inner product between α and x. Then, given a function $G : \mathbb{F}^w \to \mathbb{F}^w$, the correlation cor of the linear approximation for an output mask α_2 and an input mask α_1 is defined by

$$\mathsf{cor}_G(\alpha_1, \alpha_2) := \frac{1}{2^{wn}} \sum_{x \in \mathbb{F}^w} (-1)^{\langle \alpha_1, x\rangle \oplus \langle \alpha_2, G(x)\rangle}.$$

If $\mathsf{cor}_G(\alpha_1, \alpha_2) \gg 2^{-wn}$, then α_1, α_2 constitute a good linear approximation of G and can be used for linear cryptanalysis [Mat94]. On the other hand, if $\mathsf{cor}_G(\alpha_1, \alpha_2) = 0$, then $(\alpha_1 \to \alpha_2)$ is called a Zero Correlation (ZC) linear hull of G. Such linear approximations without any bias also enable distinguishing [BR14, BW12].

2.4 Structures and their Differential/Linear Properties

Cryptanalytic practice usually focuses on detecting IDs and ZC linear hulls that are independent from the concrete S-boxes and keys. Concretely, attacks try to determine whether there is a difference (mask) of an S-box or not, regardless of the value of this difference (mask). The model of *structures* was proposed by Sun et al. [SLR+15, SLG+16] to characterize the intuition of "being independent of the choices of S-boxes". Below we present [SLR+15, Definition 2] adapted to our notations.

Definition 1 (Structures)**.** Let $f : \mathbb{F}^w \to \mathbb{F}^w$ be a cryptographic function defined upon bijective S-boxes on $\mathbb{F}$.

1. A *structure* $\mathcal{E}_f$ on $\mathbb{F}^w$ is defined as a set of functions f' which are exactly the same as f except that the S-boxes can take *all possible* bijective transformations on $\mathbb{F}$.
2. Let $a, b \in \mathbb{F}^w$. If *for any* $f' \in \mathcal{E}_f$, $a \to b$ is an impossible differential (resp. zero correlation linear hull) of f', then $a \to b$ is called an impossible differential (resp. zero correlation linear hull) of $\mathcal{E}_f$.

In fact, truncated ID and ZC attacks against word oriented blockciphers typically focus on ID and ZC distinguishers on the corresponding structures. Notable examples following this strategy include attacks against the AES [BR14, MDRMH10] and Camellia [BGW+14]. The structure-based approach is thus of some practical relevance, and has motivated researches on provable security w.r.t. IDs/ZCs of structures. To our knowledge, this structure-based approach remains the only method to investigate provable security against ID and ZC attacks on general blockcipher constructions ("unconditional" ID/ZC security proofs are limited to certain blockciphers such as the AES [WJ18]).

3 Rate 1/2: Birthday SPRP Security at 5 Rounds

In this section, we focus on the SPRP security of P-SPNs with rate 1/2. For simplicity, we assume that the width w is even. We will frequently write $M \in \mathbb{F}^{w \times w}$ in the block form of 4 submatrices in $\mathbb{F}^{w/2 \times w/2}$. For this, we follow the convention using U, B, L, R for *upper*, *bottom*, *left*, and *right* resp., i.e.,

$$M = \begin{pmatrix} M_{\mathrm{UL}} & M_{\mathrm{UR}} \\ M_{\mathrm{BL}} & M_{\mathrm{BR}} \end{pmatrix}.$$

We use brackets, i.e., $(M^{-1})_{\mathrm{XX}}$, $\mathrm{XX} \in \{\mathrm{UL}, \mathrm{UR}, \mathrm{BL}, \mathrm{BR}\}$, to distinguish submatrices of M^{-1} (the inverse of M) from M_{XX}^{-1}, the inverse of M_{XX}.

We will first introduce a useful operator on the linear transformation T in Sect. 3.1. Then, in Sect. 3.2 we prove security for 5 rounds. Nandi's idea [Nan15] gives rise to a simple chosen-plaintext attack against 3 rounds. For completeness, we present a description adapted to our context in Appendix A.

3.1 A Useful Operator on the Linear Layer

As per our convention, we view $u, v \in \mathbb{F}^w$ as column vectors. During the proof, we will need to derive the "second halves" $u_2 := u[w/2 + 1..w]$ and $v_2 := v[w/2 + 1..w]$ from the

"first halves" $u_1 := u[1..w/2], v_1 := v[1..w/2]$, and the equality $v = T \cdot u$. To this end, the equality $v = T \cdot u$ implies

$$\left\{ \begin{array}{rl} T_{\text{UR}} \cdot u_2 & = T_{\text{UL}} \cdot u_1 \oplus v_1 \\ T_{\text{BR}} \cdot u_2 \oplus v_2 & = T_{\text{BL}} \cdot u_1 \end{array} \right. ,$$

$$\left(\begin{array}{c} u_2 \\ v_2 \end{array} \right) = \left(\begin{array}{cc} T_{\text{UR}} & 0 \\ T_{\text{BR}} & I \end{array} \right)^{-1} \left(\begin{array}{cc} T_{\text{UL}} & I \\ T_{\text{BL}} & 0 \end{array} \right) \left(\begin{array}{c} u_1 \\ v_1 \end{array} \right).$$

By this, we define an operator on T as follows:

$$\widehat{T} := \left(\begin{array}{cc} T_{\text{UR}}^{-1} \cdot T_{\text{UL}} & T_{\text{UR}}^{-1} \\ T_{\text{BR}} \cdot T_{\text{UR}}^{-1} \cdot T_{\text{UL}} \oplus T_{\text{BL}} & T_{\text{BR}} \cdot T_{\text{UR}}^{-1} \end{array} \right). \tag{4}$$

It can be seen that, u_2, v_2 can be written as u_1, v_1 multiplied by $\widehat{T}$, i.e.,

$$\left(\begin{array}{c} u_2 \\ v_2 \end{array} \right) = \left(\begin{array}{cc} T_{\text{UR}}^{-1} & 0 \\ T_{\text{BR}} \cdot T_{\text{UR}}^{-1} & I \end{array} \right) \left(\begin{array}{cc} T_{\text{UL}} & I \\ T_{\text{BL}} & 0 \end{array} \right) \left(\begin{array}{c} u_1 \\ v_1 \end{array} \right) = \widehat{T} \cdot \left(\begin{array}{c} u_1 \\ v_1 \end{array} \right).$$

This operator will be useful in both Sect. 3.2 and Sect. 4.

Note that

$$v = T \cdot u \iff \left(\begin{array}{c} u_2 \\ v_2 \end{array} \right) = \widehat{T} \cdot \left(\begin{array}{c} u_1 \\ v_1 \end{array} \right),$$

with $\mathsf{wt}(u_2) + \mathsf{wt}(v_2) + \mathsf{wt}(u_1) + \mathsf{wt}(v_1) = \mathsf{wt}(u) + \mathsf{wt}(v)$. This implies the following interesting property.

Lemma 1. *$\widehat{T}$ is MDS if and only if T is MDS.*

3.2 SPRP Security at 5 Rounds

We will prove security for 5-round P-SPNs built upon 5 "S-boxes"/random permutations $\mathcal{S} = \{S_1, S_2, S_3, S_4, S_5\}$ and *a single linear layer* T. Formally,

$$\begin{aligned} \mathcal{C}5_{\mathbf{k}}^{\mathcal{S}}(x) := k_5 \oplus \mathsf{PS}^{S_5}\big(k_4 \oplus T\big(\mathsf{PS}^{S_4}\big(k_3 \oplus T\big(\mathsf{PS}^{S_3}\big(k_2 \oplus T\big(\mathsf{PS}^{S_2}\big(\\ k_1 \oplus T\big(\mathsf{PS}^{S_1}\big(k_0 \oplus x, 1/2\big)\big), 1/2\big)\big), 1/2\big)\big), 1/2\big)\big), 1/2\big)\big)\big). \end{aligned} \tag{5}$$

Using a single linear layer simplifies both the construction and the notations. Recall from our convention that $T_{\text{UL}}, \ldots, (T^{-1})_{\text{BR}}$ constitute the eight submatrices of T and T^{-1}. In fact, $(T^{-1})_{\text{UL}}, \ldots, (T^{-1})_{\text{BR}}$ can be derived from $T_{\text{UL}}, \ldots, T_{\text{BR}}$, but the expressions are too complicated to use.

We next characterize the properties on T that is sufficient for security.

Definition 2 (Good Linear Layer for 5 Rounds)**.** A matrix $T \in \mathbb{F}^{w \times w}$ is *good*, if T is MDS, and the 6 induced matrices T_{BR}, $T_{\text{UR}}^{-1} \cdot T_{\text{UL}} \cdot T_{\text{UR}}$, $\big(T_{\text{BR}} \cdot T_{\text{UR}}^{-1} \cdot T_{\text{UL}} \oplus T_{\text{BL}}\big) \cdot T_{\text{UR}}$, $(T^{-1})_{\text{BR}}$, $T_{\text{UR}}^{-1} \cdot (T^{-1})_{\text{UR}}$, and $T_{\text{BR}} \cdot T_{\text{UR}}^{-1} \cdot (T^{-1})_{\text{UR}}$ are such that:

1. They contain no zero entries, and
2. Any column vector of the 6 induced matrices consists of $w/2$ distinct entries.

We remark that, as T is MDS, all the four matrices $T_{\text{UL}}, T_{\text{UR}}, T_{\text{BL}}$ and T_{BR} are all MDS (and invertible). A natural question is whether such strong T exists at all. For this, we make an exhaustive search for $n = 8, 11$ and find some candidates: see Appendix B.

With such a good T, we have the following theorem on 5-round P-SPNs.

Theorem 1. *Assume $w \geq 2$, and $q_S + wq_C/2 \leq 2^n/2$. Let $\mathcal{C}5$ be a 5-round, linear P-SPN structure defined in Eq. (5), with distribution $\mathcal{K}$ over keys $(k_0, \ldots, k_5)$. If k_0 and k_5 are uniformly distributed and the matrix T fulfills Definition 2, then*

$$\mathsf{Adv}^{\mathsf{sprp}}_{\mathcal{C}5}(q_C, q_S) \leq \frac{6wq_Cq_S + 3w^2q_C^2}{2^n} + \frac{q_C^2}{2^{wn/2}}. \tag{6}$$

All the remaining of this subsection devotes to prove Theorem 1. The main flow follows the general paradigm of the H-coefficient technique. In detail, we first establish notations in subsect. 3.2.1. We then complete the two steps *defining and analyzing bad transcripts* and *bounding the ratio $\mu(\tau)/\nu(\tau)$ for good transcripts* in subsect. 3.2.2 and 3.2.3 resp. For clarity, the proofs of some of the lemmas are deferred to subsect. 3.3.

Remark 1. Rate 1/2 P-SPN may remind the reader of the Feistel network, which also applies the random round functions to a half of the data in each round. However, the two schemes significantly deviate in detail, and thus rate 1/2 P-SPN consumes one more round than Feistel (which needs 4 rounds) to allow for provable security, and the concrete proof approaches are also different. We refer the reader to Appendix C for a complete discussion.

Remark 2. The Misty network slightly resembles a rate 1/2 P-SPN with $w = 2$. As a Misty-R round has basically the same cryptographic strength as the inverse of a Misty-L round (see [Lee13]), below we focus on Misty-R. The "diffusion layer" of Misty-R, which maps $\binom{u_1}{u_2}$ to $\binom{u_2}{u_1 \oplus u_2}$, is much weaker than Definition 2. This matches the observation that Misty-R achieves faster diffusion in the forward direction than that in the backward, and thus 5 Misty-R rounds are needed for SPRP security. In contrast, for rate 1/2 P-SPN with a good linear layer and $w = 2$, actually 4 rounds could be secure, as briefed in Appendix C. In all, the linear layers we use are significantly stronger than Misty's and indeed help achieving better security.

3.2.1 Proof setup

Fix a deterministic distinguisher D. Wlog, we assume D makes exactly q_C (non-redundant) forward/inverse queries to its left oracle that is either $\mathcal{C}5^{\mathcal{S}}_{\mathbf{k}}$ or P, and exactly q_S (non-redundant) forward/inverse queries to each of the oracle S_i on its right side. We call a query from D to its left oracle a *construction query*, and a query from D to one of its right oracles an *S-box query*.

The interaction between D and its oracles is recorded in the form of 6 lists of pairs $Q_{\mathcal{C}} \subseteq \{0,1\}^{wn} \times \{0,1\}^{wn}$ and $Q_{S_1}, \ldots, Q_{S_5} \subseteq \{0,1\}^n \times \{0,1\}^n$. Among them, $Q_{\mathcal{C}} = ((x^{(1)}, y^{(1)}), \ldots, (x^{(q_C)}, y^{(q_C)}))$ lists the construction queries-responses of D *in chronological order*, where the i th pair $(x^{(i)}, y^{(i)})$ indicates the i th such query is either a construction query $x^{(i)}$ that was answered by $y^{(i)}$ or an inverse query $y^{(i)}$ that was answered by $x^{(i)}$. $Q_{S_1}, \ldots, Q_{S_5}$ are defined similarly with respect to queries to $S_1, \ldots, S_5$. Define $Q_{\mathcal{S}} := (Q_{S_1}, \ldots, Q_{S_5})$. Note that D's interaction with its oracles can be unambiguously reconstructed from these sets since D is deterministic. For convenience, for $i \in \{1, 2, 3, 4, 5\}$ we define

$$\mathrm{Dom}_i := \big\{a : (a, b) \in Q_{S_i} \text{ for some } b \in \mathbb{F}\big\}, \quad \mathrm{Rng}_i := \big\{b : (a, b) \in Q_{S_i} \text{ for } a \in \mathbb{F}\big\}.$$

Following [CS14], we augment the transcript $(Q_{\mathcal{C}}, Q_{\mathcal{S}})$ with a key value $\mathbf{k} = (k_0, \ldots, k_5)$. In the real world, $\mathbf{k}$ is the actual key used by the construction. In the ideal world, $\mathbf{k}$ is a dummy key sampled independently from all other values according to the prescribed key distribution $\mathcal{K}$. Thus, a transcript τ has the final form $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})$.

3.2.2 Bad transcripts

Let $\mathcal{T}$ be the set of all possible transcripts that can be generated by D in the ideal world (note that this includes all transcripts that can be generated with nonzero probability in the real world). As in Sect. 2.2, let μ, ν be the distributions over transcripts in the real and ideal worlds, respectively.

We define a set $\mathcal{T}_2 \subseteq \mathcal{T}$ of *bad transcripts* as follows: a transcript $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})$ is bad if and only if one of the following events occurs:

1. There exist a pair $(x, y) \in Q_{\mathcal{C}}$ and an index $i \in \{w/2+1, \ldots, w\}$ such that $(x \oplus k_0)[i] \in \mathrm{Dom}_1$ or $(y \oplus k_5)[i] \in \mathrm{Rng}_5$.

2. There exist a pair $(x, y) \in Q_{\mathcal{C}}$ and distinct $i, i' \in \{w/2+1, \ldots, w\}$ such that $(x \oplus k_0)[i] = (x \oplus k_0)[i']$ or $(y \oplus k_5)[i] = (y \oplus k_5)[i']$.

3. There exist distinct $(x, y), (x', y') \in Q_{\mathcal{C}}$ and distinct $i, i' \in \{w/2+1, \ldots, w\}$ such that $(x \oplus k_0)[i] = (x' \oplus k_0)[i']$ or $(y \oplus k_5)[i] = (y' \oplus k_5)[i']$.

4. There exist two indices $i, \ell \in \{1, \ldots, q_C\}$ such that $\ell > i$, and:

   - $(x^{(\ell)}, y^{(\ell)})$ was due to a forward query, and $y^{(\ell)}[\frac{w}{2}+1..w] = y^{(i)}[\frac{w}{2}+1..w]$; or,
   - $(x^{(\ell)}, y^{(\ell)})$ was due to a backward query, and $x^{(\ell)}[\frac{w}{2}+1..w] = x^{(i)}[\frac{w}{2}+1..w]$.

As in Sect. 2.2, $\mathcal{T}_1 := \mathcal{T} \backslash \mathcal{T}_2$ denotes the set of *good* transcripts.

To understand the conditions, consider a good transcript $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})$ and let's see some properties (informally). First, since the 1st condition is not fulfilled, each construction query induces $w/2$ inputs to the 1st round S-box and $w/2$ inputs to the 5th round S-box, the outputs of which are *not* fixed by $Q_{\mathcal{S}}$. Second, since neither the 2nd nor the 3rd condition is fulfilled, the inputs to the 1st round (5th round, resp.) S-box induced by the construction queries are distinct unless unavoidable. These ensure that the induced 2nd and 4th intermediate values are somewhat random and free from multiple forms of collisions. Finally, the last condition will be crucial for some structural properties of the queries that will be crucial in the subsequent analysis (see subsect. 3.3.2, the proof of Lemma 3).

Let's then analyze the probabilities of the conditions in turn. Since, in the ideal world, the values k_0, k_5 are independent of $Q_{\mathcal{C}}, Q_{\mathcal{S}}$ and (individually) uniform in $\{0,1\}^{wn}$, it is easy to see that the probabilities of the first three events do not exceed $wq_Cq_S/2^n$, $\binom{w/2}{2} \cdot \frac{2q_C}{2^n} \leq w^2 q_C/2^{n+2}$, and $\binom{w/2}{2} \cdot \binom{q_C}{2} \cdot \frac{2}{2^n} \leq w^2 q_C(q_C-1)/2^{n+2}$ respectively.

For the 4th condition, consider the ℓ th construction query $(x^{(\ell)}, y^{(\ell)})$. When it is forward, in the ideal world it means D issued $P(x^{(\ell)})$ to the $2wn$-bit random permutation P and received $y^{(\ell)}$, which is uniform in $2^{wn} - \ell + 1$ possibilities. Thus, when $\ell \leq q_C \leq 2^{wn}/2$,

$$\begin{aligned}
&\Pr\left[\exists i \leq \ell - 1 : y^{(\ell)}\left[\frac{w}{2}+1..w\right] = y^{(i)}\left[\frac{w}{2}+1..w\right]\right] \\
&= \sum_{i \leq \ell-1, z \in \mathbb{F}^{w/2}} \Pr\left[y^{(\ell)} = \left(z \| y^{(i)}\left[\frac{w}{2}+1..w\right]\right)\right] \leq \frac{(\ell-1)\cdot 2^{wn/2}}{2^{wn}-\ell+1} \leq \frac{2(\ell-1)}{2^{wn/2}}.
\end{aligned}$$

Similar result follows when $(x^{(\ell)}, y^{(\ell)})$ is backward. A union bound thus yields

$$\Pr[\nu \in \mathcal{T}_2] \leq \frac{wq_Cq_S}{2^n} + \frac{w^2q_C^2}{2^{n+2}} + \sum_{\ell=1}^{q_C} \frac{2(\ell-1)}{2^{wn/2}} \leq \frac{wq_Cq_S}{2^n} + \frac{w^2q_C^2}{2^{n+2}} + \frac{q_C^2}{2^{wn/2}}. \tag{7}$$

3.2.3 Bounding the ratio $\mu(\tau)/\nu(\tau)$

Let $\Omega_X = \big(\mathcal{P}(n)\big)^5 \times \mathcal{K}$ be the probability space underlying the real world, whose measure is the product of the uniform measure on $(\mathcal{P}(n))^5$ and the measure induced by the distribution $\mathcal{K}$ on keys. (Thus, each element of Ω_X is a tuple $(\mathcal{S}, \mathbf{k})$ with $\mathcal{S} = (S_1, \ldots, S_5)$, $S_1, \ldots, S_5 \in \mathcal{P}(n)$ and $\mathbf{k} = (k_0, \ldots, k_5) \in \mathcal{K}$.) Also let $\Omega_Y = \mathcal{P}(wn) \times \big(\mathcal{P}(n)\big)^5 \times \mathcal{K}$ be the probability space underlying the ideal world, whose measure is the product of the uniform measure on $\mathcal{P}(wn)$ with the measure on Ω_X.

Let $\tau' = (Q_{\mathcal{C}}^{\tau'}, Q_{\mathcal{S}}^{\tau'}, \mathbf{k}^{\tau'})$ be a transcript. We introduce four types of *compatibility* as follows.

- First, an element $\omega = (\mathcal{S}^*, \mathbf{k}^*) \in \Omega_X$ is *compatible with* τ' if $\mathbf{k}^* = \mathbf{k}^{\tau'}$, if $S_i^*(a) = b$ for all $(a, b) \in Q_{S_i}$ and all i, and if $\mathcal{C}_{\mathbf{k}^*}^{\mathcal{S}^*}(x) = y$ for all $(x, y) \in Q_{\mathcal{C}}^{\tau'}$.
- Second, an element $\omega = (P^*, \mathcal{S}^*, \mathbf{k}^*) \in \Omega_Y$ is *compatible with* τ' if: (a) $\mathbf{k}^* = \mathbf{k}^{\tau'}$, and (b) $S_i^*(a) = b$ for all $(a, b) \in Q_{S_i}^{\tau'}$, and (c) $P^*(x) = y$ for all $(x, y) \in Q_{\mathcal{C}}^{\tau'}$. We write
$$\omega \downarrow \tau'$$
to indicate that an element $\omega \in \Omega_X \cup \Omega_Y$ is compatible with τ'.
- Third, a tuple of S-boxes $\mathcal{S}^* \in (\mathcal{P}(n))^5$ is *compatible* with $\tau' = (Q_{\mathcal{C}}^{\tau'}, Q_{\mathcal{S}}^{\tau'}, \mathbf{k})$, and write $\mathcal{S}^* \downarrow \tau'$, if $(\mathcal{S}^*, \mathbf{k}) \in \Omega_X$ is compatible with τ', where $\mathbf{k}$ is the key value of the fixed transcript τ.
- Last, we say that $(P^*, \mathcal{S}^*) \in \mathcal{P}(wn) \times (\mathcal{P}(n))^5$ is *compatible* with $\tau' = (Q_{\mathcal{C}}^{\tau'}, Q_{\mathcal{S}}^{\tau'}, \mathbf{k}^{\tau'})$, and write $(P^*, \mathcal{S}^*) \downarrow \tau'$, if $(P^*, \mathcal{S}^*, \mathbf{k}^{\tau'}) \downarrow \tau'$.

For the rest of the proof we fix a transcript $\tau = (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \in \mathcal{T}_1$. Since $\tau \in \mathcal{T}$, it is easy to see (cf. [CS14]) that

$$\mu(\tau) = \Pr[\omega \leftarrow \Omega_X : \omega \downarrow \tau], \qquad \nu(\tau) = \Pr[\omega \leftarrow \Omega_Y : \omega \downarrow \tau],$$

where the notation indicates that ω is sampled from the relevant probability space according to that space's probability measure. We bound $\mu(\tau)/\nu(\tau)$ by reasoning about the latter probabilities. In detail, with the third and fourth types of compatibility notions, the product structure of Ω_X, Ω_Y implies

$$\begin{aligned}\Pr[\omega \leftarrow \Omega_X : \omega \downarrow \tau] &= \Pr[\mathbf{k}^* = \mathbf{k}] \cdot \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau],\\ \Pr[\omega \leftarrow \Omega_Y : \omega \downarrow \tau] &= \Pr[\mathbf{k}^* = \mathbf{k}] \cdot \Pr_{P^*,\mathcal{S}^*}[(P^*, \mathcal{S}^*) \downarrow \tau],\end{aligned}$$

where $\mathcal{S}^*$ and $(P^*, \mathcal{S}^*)$ are sampled uniformly from $(\mathcal{P}(n))^5$ and $\mathcal{P}(wn) \times (\mathcal{P}(n))^5$, respectively. Thus,

$$\frac{\mu(\tau)}{\nu(\tau)} = \frac{\Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau]}{\Pr_{P^*,\mathcal{S}^*}[(P^*, \mathcal{S}^*) \downarrow \tau]}.$$

By these, and by $|Q_{\mathcal{C}}| = q_C, |Q_{S_1}| = \ldots = |Q_{S_5}| = q_S$, it is immediate that

$$\Pr_{P^*,\mathcal{S}^*}\big[(P^*, \mathcal{S}^*) \downarrow \tau\big] = \frac{1}{(2^{wn})_{q_C} \cdot \big((2^n)_{q_S}\big)^5},$$

To compute $\Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau]$ we start by writing

$$\begin{aligned}\Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow \tau] &= \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k})]\\ &= \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})] \cdot \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})]\\ &= \frac{1}{((2^n)_{q_S})^5} \cdot \Pr_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})].\end{aligned}$$

To analyze $\mathrm{Pr}_{\mathcal{S}^*}[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})]$, we proceed in two steps. First, based on $Q_{\mathcal{C}}$ and two outer S-boxes S_1^*, S_5^*, we derive the 2nd and 4th rounds intermediate values: these constitute a special transcript Q_{mid} on the middle 3 rounds. We characterize conditions on S_1^*, S_5^* that will ensure certain good properties in the derived Q_{mid}, which will ease the analysis. Therefore, in the second step, we analyze such "good" Q_{mid} to yield the final bounds. Each of the two steps will take a paragraph as follows.

The outer 2 rounds. Given a tuple of S-boxes $\mathcal{S}^*$, we let $\mathsf{Bad}(\mathcal{S}^*)$ be a predicate of $\mathcal{S}^*$ that holds if any of the following conditions is met:

- (B-1) There exist $(x, y) \in Q_{\mathcal{C}}$ and $i \in \{w/2+1, \ldots, w\}$ such that $\big(T(\mathsf{PS}^{S_1^*}(x \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i] \in \mathrm{Dom}_2$ or $\big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i] \in \mathrm{Rng}_4$.
- (B-2) There exist $(x, y) \in Q_{\mathcal{C}}$ and distinct indices $i, i' \in \{w/2+1, \ldots, w\}$ such that $\big(T(\mathsf{PS}^{S_1^*}(x \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i] = \big(T(\mathsf{PS}^{S_1^*}(x \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i']$, or $\big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i] = \big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i']$.
- (B-3) There exist distinct pairs $(x, y), (x', y') \in Q_{\mathcal{C}}$ and two indices $i, i' \in \{w/2+1, \ldots, w\}$ such that:
  1. $x\big[\frac{w}{2}+1..w\big] \neq x'\big[\frac{w}{2}+1..w\big]$, yet $\big(T(\mathsf{PS}^{S_1^*}(x \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i] = \big(T(\mathsf{PS}^{S_1^*}(x' \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i']$; or
  2. $x\big[\frac{w}{2}+1..w\big] = x'\big[\frac{w}{2}+1..w\big]$, $i \neq i'$, yet $\big(T(\mathsf{PS}^{S_1^*}(x \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i] = \big(T(\mathsf{PS}^{S_1^*}(x' \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i']$; or
  3. $y\big[\frac{w}{2}+1..w\big] \neq y'\big[\frac{w}{2}+1..w\big]$, yet it holds $\big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i] = \big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y' \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i']$; or
  4. $y\big[\frac{w}{2}+1..w\big] = y'\big[\frac{w}{2}+1..w\big]$, $i \neq i'$, yet $\big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i] = \big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y' \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i']$.

(B-1) captures the case that a 2nd round S-box input or a 4th round S-box output has been in $Q_{\mathcal{S}}$, (B-2) captures collisions among the 2nd round S-box inputs & 4th round S-box outputs for a single construction query, while (B-3) captures various collisions between the 2nd round S-box inputs, resp. 4th round S-box outputs, from two distinct queries. Note that essentially, $\mathsf{Bad}(\mathcal{S}^*)$ only concerns with the randomness of the outer 2 S-boxes S_1^* and S_5^*. For simplicity, define $\mathsf{Good}(\mathcal{S}^*) := (\mathcal{S}^* \downarrow Q_{\mathcal{S}}) \wedge \neg\mathsf{Bad}(\mathcal{S}^*)$. Then it holds

$$\begin{aligned}
&\mathrm{Pr}_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \\
\geq\ &\mathrm{Pr}_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \\
=\ &\mathrm{Pr}_{\mathcal{S}^*}\big[\mathsf{Good}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \cdot \mathrm{Pr}_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big], \qquad (8)
\end{aligned}$$

Hence, all that remains is to lower bound the two terms in the product of (8). We serve the result below, and defer the proof to subsect. 3.3.1.

Lemma 2. *When $q_S + w \leq 2^n/2$, we have*

$$\mathrm{Pr}_{\mathcal{S}^*}\big[\mathsf{Bad}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \leq \frac{8wq_Cq_S + 2w^2q_C^2}{2^{n+2}}. \qquad (9)$$

Analyzing the 3 middle rounds. Our next step is to lower bound the term $\mathrm{Pr}_{\mathcal{S}^*}\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big]$ from Eq. (8). Given $\mathcal{S}^*$ for which $\mathsf{Good}(\mathcal{S}^*)$ holds, for every $(x^{(i)}, y^{(i)}) \in Q_{\mathcal{C}}$ we define $u_1^{(i)} := x^{(i)} \oplus k_0$, $v_1^{(i)} := \mathsf{PS}^{S_1^*}(u_1^{(i)}, 1/2)$ (this means $v_1^{(i)}[1..w/2] =$

$u_1^{(i)}[1..w/2])$, $u_2^{(i)} := T \cdot v_1^{(i)} \oplus k_1$; $v_5^{(i)} := y^{(i)} \oplus k_5$, $u_5^{(i)} := \big(\mathsf{PS}^{S_5^*}\big)^{-1}(v_5^{(i)}, 1/2)$, $v_4^{(i)} := T^{-1} \cdot (u_5^{(i)} \oplus k_4)$. With these, we obtain

$$Q_{mid} = \Big(\big(u_1^{(1)}, u_2^{(1)}, v_4^{(1)}, v_5^{(1)}\big), \ldots, \big(u_1^{(q_C)}, u_2^{(q_C)}, v_4^{(q_C)}, v_5^{(q_C)}\big)\Big),$$

in which the tuples follow exactly the same chronological order as in $Q_{\mathcal{C}}$. Define

$$\mathcal{C}3^{\mathcal{S}^*}(u) = \mathsf{PS}^{S_4^*}\big(T \cdot \big(\mathsf{PS}^{S_3^*}\big(T \cdot \big(\mathsf{PS}^{S_2^*}\big(u, 1/2\big)\big) \oplus k_2, 1/2\big)\big) \oplus k_3, 1/2\big),$$

and write $\mathcal{S}^* \downarrow (\mathsf{Set}, Q_{\mathcal{S}}, \mathbf{k})$ for the event that "$\mathcal{C}3^{\mathcal{S}^*}(u_2) = v_4$ for every (u_1, u_2, v_4, v_5) in the set Set". Then it can be seen

$$\Pr\big[\mathcal{S}^* \downarrow (Q_{\mathcal{C}}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big] = \Pr\big[\mathcal{S}^* \downarrow (Q_{mid}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big]. \tag{10}$$

To bound Eq. (10), we will divide Q_{mid} into multiple sets according to collisions on the "second halves" $u_1[w/2+1..w]$ and $v_5[w/2+1..w]$, and consider the probability that $\mathcal{S}^*$ is compatible with each set in turn. In detail, the sets are arranged according to the following rules:

- $Q_{m_1} := \big\{(u_1, u_2, v_4, v_5) \in Q_{mid} : u_1[w/2+1..w] = u_1^{(1)}[w/2+1..w]\big\}$;
- For $\ell = 2, 3, \ldots$, if $\cup_{i=1}^{\ell-1} Q_{m_i} = Q_{m_1} \cup Q_{m_2} \cup \ldots \cup Q_{m_{\ell-1}} \subset Q_{mid}$, then we define Q_{m_ℓ}. Let j be the minimum index such that $(u_1^{(j)}, u_2^{(j)}, v_4^{(j)}, v_5^{(j)})$ remains in $Q_{mid} \backslash \cup_{i=1}^{\ell-1} Q_{m_i}$. Then:
  - If $v_5^{(j)}$ has collisions, i.e., there exists $(u_1^*, u_2^*, v_4^*, v_5^*) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ such that $v_5^*[w/2+1..w] = v_5^{(j)}[w/2+1..w]$, then we define $Q_{m_\ell} := \big\{(u_1, u_2, v_4, v_5) \in Q_{mid} \backslash \cup_{i=1}^{\ell-1} Q_{m_i} : v_5[w/2+1..w] = v_5^{(j)}[w/2+1..w]\big\}$. We call such sets **Type-II**.
  - Else, $Q_{m_\ell} := \big\{(u_1, u_2, v_4, v_5) \in Q_{mid} : u_1[w/2+1..w] = u_1^{(j)}[w/2+1..w]\big\}$. We call such sets as well as Q_{m_1} **Type-I**.

Assume that Q_{mid} is divided into α sets by the above rules, with $|Q_{m_\ell}| = \beta_\ell$. Then $\sum_{\ell=1}^{\alpha} \beta_\ell = q_C$, and

$$\begin{aligned} &\Pr\big[\mathcal{S}^* \downarrow (Q_{mid}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big] \\ = &\prod_{\ell=1}^{\alpha} \Pr\big[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big]. \end{aligned} \tag{11}$$

Now we could focus on analyzing the ℓ th set Q_{m_ℓ}. Assume that

$$Q_{m_\ell} = \Big(\big(u_1^{(\ell,1)}, u_2^{(\ell,1)}, v_4^{(\ell,1)}, v_5^{(\ell,1)}\big), \ldots, \big(u_1^{(\ell,\beta_\ell)}, u_2^{(\ell,\beta_\ell)}, v_4^{(\ell,\beta_\ell)}, v_5^{(\ell,\beta_\ell)}\big)\Big).$$

The superscript (ℓ, i) indicates that it is the i th tuple in this ℓ th set Q_{m_ℓ}. For this index ℓ, we define six sets $\mathrm{ExtDom}_i^{(\ell)}$ and $\mathrm{ExtRng}_i^{(\ell)}$, $i = 2, 3, 4$, as follows:

$$\begin{aligned}
&\mathrm{ExtDom}_2^{(\ell)} := \big\{u_2[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \{w/2+1, \ldots, w\}\big\} \\
&\mathrm{ExtRng}_2^{(\ell)} := \big\{S_2^*(a) : a \in \mathrm{ExtDom}_2^{(\ell)}\big\} \\
&\mathrm{ExtDom}_3^{(\ell)} := \Big\{\big(T\big(\mathsf{PS}^{S_2^*}(u_2, \frac{1}{2})\big) \oplus k_2\big)[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j = \frac{w}{2}+1, .., w\Big\} \\
&\mathrm{ExtRng}_3^{(\ell)} := \big\{S_3^*(a) : a \in \mathrm{ExtDom}_3^{(\ell)}\big\}, \qquad \mathrm{ExtDom}_4^{(\ell)} := \big\{(S_4^*)^{-1}(b) : b \in \mathrm{ExtRng}_4^{(\ell)}\big\} \\
&\mathrm{ExtRng}_4^{(\ell)} := \Big\{v_4[j] : (u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}, j \in \big\{\frac{w}{2}+1, \ldots, w\big\}\Big\}
\end{aligned}$$

Note that, conditioned on $\mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)$, the values in $\mathrm{ExtDom}_i^{(\ell)}$ and $\mathrm{ExtRng}_i^{(\ell)}$, $i = 2, 3, 4$, are compatible with the set $\cup_{i=1}^{\ell-1} Q_{m_i}$. For Q_{m_ℓ}, two useful properties regarding the arrangement of tuples and the derived intermediate values resp. could be exhibited.

Lemma 3. *Consider the ℓ th set $Q_{m_\ell} = \big((u_1^{(\ell,1)}, u_2^{(\ell,1)}, v_4^{(\ell,1)}, v_5^{(\ell,1)}), \dots\big)$. If it is of* **Type-I**, *then the number of tuples $(u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ with $u_1[\frac{w}{2}+1..w] = u_1^{(\ell,1)}[\frac{w}{2}+1..w]$ is at most 1; if it is of* **Type-II**, *then the number of $(u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ with $v_5[\frac{w}{2}+1..w] = v_5^{(\ell,1)}[\frac{w}{2}+1..w]$ is at most 1.*

The proof is deferred to subsect. 3.3.2.

Lemma 4. *Consider the ℓ th set Q_{m_ℓ} and any two distinct $\big(u_1^{(\ell,i_1)}, u_2^{(\ell,i_1)}, v_4^{(\ell,i_1)}, v_5^{(\ell,i_1)}\big)$ and $\big(u_1^{(\ell,i_2)}, u_2^{(\ell,i_2)}, v_4^{(\ell,i_2)}, v_5^{(\ell,i_2)}\big)$ in Q_{m_ℓ}. Then, there exist two indices $j_1, j_2 \in \{w/2+1..w\}$ such that,*

- *when Q_{m_ℓ} is of* **Type-I**: *$u_2^{(\ell,i_1)}[j_1] \notin Dom_2 \cup ExtDom_2^{(\ell)}$, $u_2^{(\ell,i_2)}[j_2] \notin Dom_2 \cup ExtDom_2^{(\ell)}$, and $(u_2^{(\ell,i_1)}[j_1], u_2^{(\ell,i_1)}[j_2]) \neq (u_2^{(\ell,i_2)}[j_1], u_2^{(\ell,i_2)}[j_2])$;*
- *when Q_{m_ℓ} is of* **Type-II**: *$v_4^{(\ell,i_1)}[j_1] \notin Rng_4 \cup ExtRng_4^{(\ell)}$, $v_4^{(\ell,i_2)}[j_2] \notin Rng_4 \cup ExtRng_4^{(\ell)}$, and $(v_4^{(\ell,i_1)}[j_1], v_4^{(\ell,i_1)}[j_2]) \neq (v_4^{(\ell,i_2)}[j_1], v_4^{(\ell,i_2)}[j_2])$.*

The proof is deferred to subsect. 3.3.3. With the help of these two lemmas, we are able to bound the probability that the randomness is compatible with the ℓ th set Q_{m_ℓ}.

Lemma 5. *For the ℓ th set Q_{m_ℓ}, it holds*

$$\begin{aligned} &\Pr\big[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \\ \geq\ &\Big(1 - \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{2^{n+2}}\Big) \cdot \frac{1}{2^{w\beta_\ell n}}. \end{aligned} \tag{12}$$

The proof is deferred to subsect. 3.3.4.

From Eq. (12), Eq. (11), and using $\sum_{\ell=1}^{\alpha} \beta_\ell = q_C$, we obtain

$$\begin{aligned} &\Pr\big[\mathcal{S}^* \downarrow (Q_{mid}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathsf{Good}(\mathcal{S}^*)\big] \\ \geq\ &\prod_{\ell=1}^{\alpha} \Big(\Big(1 - \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{2^{n+2}}\Big) \cdot \frac{1}{2^{w\beta_\ell n}}\Big) \\ \geq\ &\Big(1 - \sum_{\ell=1}^{\alpha} \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{2^{n+2}}\Big) \cdot \frac{1}{2^{wn\sum_{\ell=1}^{\alpha}\beta_\ell}} \\ \geq\ &\Big(1 - \frac{12wq_C(q_S + wq_C/2) + 3w^2q_C^2}{2^{n+2}}\Big) \cdot \frac{1}{2^{wnq_C}}. \end{aligned}$$

Gathering this and Eqs. (10), (9), (8), and (7), we finally reach

$$\begin{aligned} \frac{\mu(\tau)}{\nu(\tau)} &\geq \Big(1 - \frac{8wq_Cq_S + 2w^2q_C^2}{2^{n+2}}\Big)\Big(1 - \frac{12wq_C(q_S + wq_C/2) + 3w^2q_C^2}{2^{n+2}}\Big) \cdot \frac{(2^{wn})_{q_C}}{2^{wnq_C}} \\ &\geq 1 - \frac{20wq_Cq_S + 11w^2q_C^2}{2^{n+2}}. \end{aligned}$$

Further using Eq. (7) yield the bound in Eq. (6) and complete the proof.

3.3 Deferred Proofs for Theorem 1

3.3.1 Proof of Lemma 2

This requires to bound $\Pr_{\mathcal{S}^*}\big[(\text{B-}\ell) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big]$ for $\ell = 1, 2, 3$. Consider the condition (B-1) first. Fix some $(x, y) \in Q_{\mathcal{C}}$ and an index $i \in \{w/2+1, \ldots, w\}$. Since τ is good, $(x \oplus k_0)[w] \notin \mathrm{Dom}_1$, and $(x \oplus k_0)[w] \neq (x \oplus k_0)[i']$ for $i' \neq w$. So after conditioning on $\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})$ and the values of $S_1^*((x \oplus k_0)[i'])$ for $i' \neq w$, the value $S_1^*((x \oplus k_0)[w])$ is uniform in a set of size $2^n - q_S - w/2 + 1$. The MDS property implies that every entry in the w th column of T is nonzero, and thus

$$\Pr_{\mathcal{S}^*}\Big[\big(T(\mathsf{PS}^{S_1^*}(x \oplus k_0, \frac{1}{2})) \oplus k_1\big)[i] \in \mathrm{Dom}_2 \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\Big] \leq \frac{q_S}{2^n - q_S - w/2}.$$

Similarly by symmetry,

$$\Pr_{\mathcal{S}^*}\Big[\big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2})) \oplus k_4\big)[i] \in \mathrm{Rng}_4 \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\Big] \leq \frac{q_S}{2^n - q_S - w/2}.$$

Summing over $(x, y) \in Q_{\mathcal{C}}$, $i \in \{w/2+1, \ldots, w\}$, we reach

$$\Pr_{\mathcal{S}^*}\big[\text{(B-1)} \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \leq \frac{w q_C q_S}{2^n - q_S - w/2}. \tag{13}$$

Next, consider (B-2). Fix $(x, y) \in Q_{\mathcal{C}}$ and $i, i' \in \{1, \ldots, w/2\}$, and let $u_1 = x \oplus k_0$, $u_2 = T(\mathsf{PS}^{S_1^*}(u_1, \frac{1}{2})) \oplus k_1$. Then the "second half" $u_2[w/2+1..w] = T_{\text{BL}} \cdot u_1[1..w/2] \oplus T_{\text{BR}} \cdot \overline{S_1^*}\big(u_1[w/2+1..w]\big) \oplus k_1[w/2+1..w]$. Since T is MDS, T_{BR} is also MDS. This means T_{BR} is invertible, and further that the i th and i' th rows of T_{BR} are linearly independent and, in particular, there exists an index $j_0 \in \{1, \ldots, w/2\}$ such that the (i, j_0) th and (i', j_0) th entries of T_{BR} are not equal. After conditioning on $\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})$ and the values of $S_1^*(u_1[w/2+j_1])$ for $j_1 \neq j_0$, the value of $S_1^*(u_1[w/2+j_0])$ is uniform in $2^n - q_S - w/2 + 1$ values. Therefore,

$$\Pr_{\mathcal{S}^*}\Big[u_2\Big[\frac{w}{2} + i\Big] = u_2\Big[\frac{w}{2} + i'\Big] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\Big] \leq \frac{1}{2^n - q_S - w/2}.$$

Similarly by symmetry, the probability to have $\big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2}))\big)[w/2+i] = \big(T^{-1}((\mathsf{PS}^{S_5^*})^{-1}(y \oplus k_5, \frac{1}{2}))\big)[w/2+i']$ is also at most $1/(2^n - q_S - w/2)$. By a union bound over all pairs $(x, y) \in Q_{\mathcal{C}}$ and all $i, i' \in \{1, \ldots, w/2\}$, we reach

$$\Pr_{\mathcal{S}^*}\big[\text{(B-2)} \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\big] \leq \binom{w/2}{2} \cdot \frac{2q_C}{2^n - q_S - w/2} \leq \frac{w^2 q_C}{4(2^n - q_S - w/2)}. \tag{14}$$

We now consider (B-3). We first fix $(x, y), (x', y') \in Q_{\mathcal{C}}$ and $i, i' \in \{w/2+1, \ldots, w\}$ with $x[w/2+1..w] \neq x'[w/2+1..w]$ for the 1st condition. This means $x[j_0] \neq x'[j_0]$ for some $j_0 \in \{w/2+1, \ldots, w\}$. Since τ is good, $(x \oplus k_0)[j_0] \neq (x \oplus k_0)[j_1]$ for all $j_1 \neq j_0$ and $(x \oplus k_0)[j_0] \neq (x' \oplus k_0)[j_1]$ for all j_1. So after conditioning on $\mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})$ and the values of $S_1^*((x \oplus k_0)[j_1])$ for $j_1 \neq j_0$ and $S_1^*((x' \oplus k_0)[j_1])$ for $j_1 \in \{w/2+1, \ldots, w\}$, the value of $S_1^*((x \oplus k_0)[j_0])$ is uniform in $\geq 2^n - q_S - w + 1$ possibilities. Because every entry in the j_0 th column of T is nonzero, we have

$$\begin{aligned}&\Pr_{\mathcal{S}^*}\Big[\big(T(\mathsf{PS}^{S_1^*}(x \oplus k_0)) \oplus k_1\big)[i] = \big(T(\mathsf{PS}^{S_1^*}(x' \oplus k_0)) \oplus k_1\big)[i'] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\Big] \\ \leq\ & \frac{1}{2^n - q_S - w}.\end{aligned}$$

We next fix $(x, y), (x', y') \in Q_{\mathcal{C}}$ and $i \neq i' \in \{w/2+1, \ldots, w\}$ with $x[w/2+1..w] = x'[w/2+1..w]$ for the 2nd condition. While this case concerns with distinct construction

queries, the argument is an extension of that of (B-2). In detail, let $u_1 = x \oplus k_0$, $u_2 = T(\mathsf{PS}^{S_1^*}(u_1, \frac{1}{2})) \oplus k_1$, $u_1' = x' \oplus k_0$, and $u_2' = T(\mathsf{PS}^{S_1^*}(u_1', \frac{1}{2})) \oplus k_1$. By the analysis for (B-2), we have $\Pr_{\mathcal{S}^*}\left[u_2[i] = u_2[i'] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \frac{1}{2^n - q_S - w/2}$. Since $x[w/2+1..w] = x'[w/2+1..w]$, it can be seen $u_2 \oplus u_2' = T \cdot (x \oplus x')$, meaning that

$$u_2'[i'] = u_2[i'] \oplus \underbrace{\left(T_{\text{BL}} \cdot (x[1..w/2] \oplus x'[1..w/2])\right)\left[i' - \frac{w}{2}\right]}_{\delta}.$$

The offset δ is fixed by τ and is independent from S_1^*. Therefore,

$$\begin{aligned}\Pr_{\mathcal{S}^*}\left[u_2[i] = u_2'[i'] \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq\ & \Pr_{\mathcal{S}^*}\left[u_2[i] = u_2[i'] \oplus \delta \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \\ \leq\ & \frac{1}{2^n - q_S - w/2}.\end{aligned}$$

For each choice of $(x, y), (x', y')$, the 1st and 2nd conditions are mutual exclusive (i.e., only one may be fulfilled). Hence, summing over all pairs $(x, y, i), (x', y', i') \in Q_{\mathcal{C}} \times \{w/2+1, \ldots, w\}$, the probability that either of the two is fulfilled is at most

$$\binom{wq_C/2}{2} \cdot \frac{2}{2^n - q_S - w} \leq \frac{w^2 q_C(q_C - 1)}{8(2^n - q_S - w)}.$$

Similarly by symmetry, the probability that either the 3rd or the 4th condition is fulfilled is at most $\frac{w^2 q_C(q_C-1)}{8(2^n - q_S - w)}$. Thus

$$\Pr_{\mathcal{S}^*}\left[\text{(B-3)} \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \frac{w^2 q_C(q_C - 1)}{4(2^n - q_S - w)}. \tag{15}$$

Summing over Eqs. (13), (14), and (15), we reach Eq. (9):

$$\Pr_{\mathcal{S}^*}\left[\mathsf{Bad}(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\emptyset, Q_{\mathcal{S}}, \mathbf{k})\right] \leq \frac{wq_C q_S}{2^n - q_S - w/2} + \frac{w^2 q_C^2}{4(2^n - q_S - w)}$$

3.3.2 Proof of Lemma 3

Wlog, consider the case of **Type-I** Q_{m_ℓ}, as the other case is just symmetric. Assume otherwise, and assume that $\mathsf{tuple}_1 = \left(u_1^{(j_1)}, u_2^{(j_1)}, v_4^{(j_1)}, v_5^{(j_1)}\right)$ and $\mathsf{tuple}_2 = \left(u_1^{(j_2)}, u_2^{(j_2)}, v_4^{(j_2)}, v_5^{(j_2)}\right)$ in $\cup_{i=1}^{\ell-1} Q_{m_i}$ are such two tuples with the smallest indices j_1, j_2. Wlog assume $j_2 > j_1$, i.e., tuple_2 was later. Then tuple_2 was necessarily a forward query, as otherwise $u_1^{(j_1)}[\frac{w}{2}+1..w] = u_1^{(j_2)}[\frac{w}{2}+1..w]$ would contradict the goodness of τ (the 4th condition). By this and further by the 4th condition, $v_5^{(j_2)}$ is "new", and tuple_2 cannot be in any **Type-II** set Q_{m_i}, $i \leq \ell - 1$. This means there exists a **Type-I** set Q_{m_i}, $i \leq \ell - 1$, such that $\mathsf{tuple}_2 \in Q_{m_i}$. By our rules, the tuples in the purported Q_{m_ℓ} should have been Q_{m_i}, and thus Q_{m_ℓ} should not exist, reaching a contradiction.

3.3.3 Proof of Lemma 4

Wlog consider a **Type-I** Q_{m_ℓ}. First, note that by ¬(B-1) (the 1st condition), $u_2^{(\ell,i_1)}[j] \notin \text{Dom}_2$ and $u_2^{(\ell,i_2)}[j] \notin \text{Dom}_2$ for any $j \in \{w/2+1..w\}$. We then distinguish two cases depending on $\cup_{i=1}^{\ell-1} Q_{m_i}$ (which contribute to $\text{ExtDom}_2^{(\ell)}$):

Case 1: $u_1^{(\ell,i_1)}[\frac{w}{2}+1..w] \neq u_1[\frac{w}{2}+1..w]$ for all $(u_1, u_2, v_4, v_5) \in \cup_{i=1}^{\ell-1} Q_{m_i}$. Then by ¬(B-3), $u_2^{(\ell,i_1)}[j], u_2^{(\ell,i_2)}[j] \notin \text{ExtDom}_2^{(\ell)}$ *for all* $j \in \{\frac{w}{2}+1, \ldots, w\}$. Among these $w/2$ indices, there exists j_1 such that $u_2^{(\ell,i_1)}[j_1] \neq u_2^{(\ell,i_2)}[j_1]$. For any $j_2 \neq j_1$, we have $u_2^{(\ell,i_1)}[j_1] \neq u_2^{(\ell,i_2)}[j_2]$ by ¬(B-3) (the 2nd condition). Therefore, setting $j' = j_1$, we complete the argument for this case.

Case 2: there exists $(u_1^*, u_2^*, v_4^*, v_5^*) \in \cup_{i=1}^{\ell-1} Q_{m_i}$ with $u_1^*[\frac{w}{2}+1..w] = u_1^{(\ell,i_1)}[\frac{w}{2}+1..w]$. Then by construction, we have $u_2^{(\ell,i_1)}[\frac{w}{2}+1..w] = u_2^*[\frac{w}{2}+1..w] \oplus \Delta_{i_1}$ and $u_2^{(\ell,i_2)}[\frac{w}{2}+1..w] = u_2^*[\frac{w}{2}+1..w] \oplus \Delta_{i_2}$, where $\Delta_{i_1} = T_{\text{BL}} \cdot \big(u_1^*[1..\frac{w}{2}] \oplus u_1^{(\ell,i_1)}[1..\frac{w}{2}]\big)$ and $\Delta_{i_2} = T_{\text{BL}} \cdot \big(u_1^*[1..\frac{w}{2}] \oplus u_1^{(\ell,i_2)}[1..\frac{w}{2}]\big)$. Let $\mathcal{J}_1$ be the subset of $\{\frac{w}{2}+1, \ldots, w\}$ such that $\Delta_{i_1}[j] \neq 0$ iff. $j \in \mathcal{J}_1$, and $\mathcal{J}_2 \subseteq \{\frac{w}{2}+1, \ldots, w\}$ be such that $\Delta_{i_2}[j] \neq 0$ iff. $j \in \mathcal{J}_2$. We distinguish three subcases depending on $\mathcal{J}_1$ and $\mathcal{J}_2$:

- Subcase 2.1: $\mathcal{J}_1 \backslash \mathcal{J}_2 \neq \emptyset$. Then, let $j_1 \in \mathcal{J}_1 \backslash \mathcal{J}_2$, and $j_2 \in \mathcal{J}_2$ in arbitrary. This means $j_1 \neq j_2$, and $u_2^{(\ell,i_1)}[j_1] \neq 0 = u_2^{(\ell,i_2)}[j_1]$. Moreover,
  - $u_2^{(\ell,i_1)}[j_1] \neq u_2^*[j_3]$ for any $j_3 \notin \{\frac{w}{2}+1, \ldots, w\} \backslash \{j_1\}$, by $\neg$(B-3) (the 2nd condition); $u_2^{(\ell,i_1)}[j_1] \neq u_2^*[j_1]$ since $j_1 \notin \mathcal{J}_1$. Thus $u_2^{(\ell,i_1)}[j_1] \notin \text{ExtDom}_2^{(\ell)}$. Similarly for $u_2^{(\ell,i_2)}$.
  - $u_1^{(\ell,i_1)}[\frac{w}{2}+1..w] \neq u_1^{**}[\frac{w}{2}+1..w]$ for any $(u_1^{**}, u_2^{**}, v_4^{**}, v_5^{**}) \neq (u_1^*, u_2^*, v_4^*, v_5^*)$ in $\cup_{i=1}^{\ell-1} Q_{m_i}$ (by Lemma 3), and thus $u_2^{(\ell,i_1)}[j_1] \neq u_2^{**}[j']$ for any $j' \in \{\frac{w}{2}+1, \ldots, w\}$ by $\neg$(B-3) (the 1st condition). Similarly for $u_2^{(\ell,i_2)}$.
- Subcase 2.2: $\mathcal{J}_2 \backslash \mathcal{J}_1 \neq \emptyset$. Then, let $j_2 \in \mathcal{J}_2 \backslash \mathcal{J}_1$, and $j_1 \in \mathcal{J}_1$, and the argument is similar to subcase 2.1 by symmetry.
- Subcase 2.3: $\mathcal{J}_1 = \mathcal{J}_2$. Then there exists $j \in \mathcal{J}_1$ such that $\Delta_{i_1}[j] \neq \Delta_{i_2}[j]$, as otherwise $\Delta_{i_1} = \Delta_{i_2}$ meaning a contradiction. Let $j_1 = j_2 = j$, then it's easy to see all the claims hold.

By the above, for **Type-I** sets, the claims hold in all cases. Thus the claim.

3.3.4 Proof of Lemma 5

We distinguish two cases depending on the type of Q_{m_ℓ}.

Case 1: Q_{m_ℓ} is Type-I. By our dividing rules, the tuples in this Q_{m_ℓ} may have the same inputs to the 2nd round S-boxes. We define a bad predicate BadII_ℓ that concerns with the 2nd round S-box outputs $v_2^{(\ell,1)} := \mathsf{PS}^{S_2^*}(u_2^{(\ell,1)}, 1/2), \ldots, v_2^{(\ell,\beta_\ell)} := \mathsf{PS}^{S_2^*}(u_2^{(\ell,\beta_\ell)}, 1/2)$: based on these values, for $i = 1, \ldots, \beta_\ell$, we define 2 vectors in accordance with the computations in $\mathcal{C}3$: $u_3^{(\ell,i)} := T \cdot v_2^{(\ell,i)} \oplus k_2$, and

$$
\begin{aligned}
& v_3^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] \| u_4^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] \\
:= \;& \widehat{T} \cdot \Big(u_3^{(\ell,i)}\Big[1..\frac{w}{2}\Big] \| \Big(u_4^{(\ell,i)}\Big[1..\frac{w}{2}\Big] \oplus k_3\Big[1..\frac{w}{2}\Big]\Big)\Big) \oplus \Big(0^{\frac{w}{2}} \| k_3\Big[\frac{w}{2}+1..w\Big]\Big) \\
= \;& \widehat{T} \cdot \Big(u_3^{(\ell,i)}\Big[1..\frac{w}{2}\Big] \| u_4^{(\ell,i)}\Big[1..\frac{w}{2}\Big]\Big) \oplus \underbrace{\widehat{T}\Big(0^{\frac{w}{2}} \| k_3\Big[1..\frac{w}{2}\Big]\Big) \oplus \Big(0^{\frac{w}{2}} \| k_3\Big[\frac{w}{2}+1..w\Big]\Big)}_{f_1(k_3)}. \qquad (16)
\end{aligned}
$$

With these notations, $\mathsf{BadII}_\ell(\mathcal{S}^*)$ is fulfilled, if either (C-1) or (C-2) is fulfilled:

- (C-1) S_2^* leads to unfresh intermediate values: there exists $i \in \{1, \ldots, \beta_\ell\}$ and $j \in \{w/2+1, \ldots, w\}$ such that $u_3^{(\ell,i)}[j] \in \text{Dom}_3 \cup \text{ExtDom}_3^{(\ell)}$, or $v_3^{(\ell,i)}[j] \in \text{Rng}_3 \cup \text{ExtRng}_3^{(\ell)}$, or $u_4^{(\ell,i)}[j] \in \text{Dom}_4 \cup \text{ExtDom}_4^{(\ell)}$.
- (C-2) S_2^* leads to colliding intermediate values: there exists distinct $(i,j), (i',j') \in \{1, \ldots, \beta_\ell\} \times \{w/2+1, \ldots, w\}$ such that $u_3^{(\ell,i)}[j] = u_3^{(\ell,i')}[j']$, or $v_3^{(\ell,i)}[j] = v_3^{(\ell,i')}[j']$, or $u_4^{(\ell,i)}[j] = u_4^{(\ell,i')}[j']$.

Consider (C-1) first. Fix $(i,j) \in \{1,\ldots,\beta_\ell\} \times \{w/2+1,\ldots,w\}$, and consider the condition $u_3^{(\ell,i)}[j] \in \mathrm{Dom}_3 \cup \mathrm{ExtDom}_3^{(\ell)}$ first. By Lemma 4, conditioned on $\neg\mathsf{Bad}(\mathcal{S}^*)$ and the values in $\mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, there exists $j' \in \{w/2+1,\ldots,w\}$ such that $v_2^{(\ell,i)}[j'] = S_2^*\big(u_2^{(\ell,i)}[j']\big)$ is uniform in at least $2^n - q_S - wq_C/2$ possibilities. Since

$$u_3^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] = T_{\mathrm{BL}} \cdot u_2^{(\ell,i)}\Big[1..\frac{w}{2}\Big] \oplus T_{\mathrm{BR}} \cdot v_2^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] \oplus k_2\Big[\frac{w}{2}+1..w\Big], \tag{17}$$

and since every entry in the $(j'-w/2)$ th column of T_{BR} is nonzero, for any $j \in \{w/2+1,\ldots,w\}$ we have

$$\begin{aligned}&\Pr_{\mathcal{S}^*}\Big[u_3^{(\ell,i)}[j] \in (\mathrm{Dom}_3 \cup \mathrm{ExtDom}_3^{(\ell)}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\Big] \\ \le\ & \frac{q_S + wq_C/2}{2^n - q_S - wq_C/2}.\end{aligned}$$

We proceed to consider $v_3^{(\ell,i)}[j]$ and $u_4^{(\ell,i)}[j]$. Note that

$$u_3^{(\ell,i)}\Big[1..\frac{w}{2}\Big] = T_{\mathrm{UL}} \cdot u_2^{(\ell,i)}\Big[1..\frac{w}{2}\Big] \oplus T_{\mathrm{UR}} \cdot v_2^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] \oplus k_2\Big[1..\frac{w}{2}\Big].$$

Gathering this and Eqs. (16) and (4), it can be seen $v_3^{(\ell,i)}[w/2+1..w]$ is written as

$$\begin{aligned}v_3^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] &= T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \cdot u_3^{(\ell,i)}\Big[1..\frac{w}{2}\Big] \oplus T_{\mathrm{UR}}^{-1} \cdot u_4^{(\ell,i)}\Big[1..\frac{w}{2}\Big] \oplus f_1(k_3)\Big[1..\frac{w}{2}\Big] \\ &= T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \cdot T_{\mathrm{UR}} \cdot v_2^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] \\ &\quad \oplus\ f_2\Big(u_2^{(\ell,i)}\Big[1..\frac{w}{2}\Big], u_4^{(\ell,i)}\Big[1..\frac{w}{2}\Big], k_2, k_3\Big),\end{aligned} \tag{18}$$

where f_2 is a (complicated) function of $u_2^{(\ell,i)}[1..w/2]$, $u_4^{(\ell,i)}[1..w/2]$, k_2, and k_3, and is independent from $v_2^{(\ell,i)}[w/2+1..w]$. Similarly,

$$\begin{aligned}u_4^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] = \ & \big(T_{\mathrm{BR}} \cdot T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \oplus T_{\mathrm{BL}}\big) \cdot T_{\mathrm{UR}} \cdot v_2^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] \\ & \oplus f_3\Big(u_2^{(\ell,i)}\Big[1..\frac{w}{2}\Big], u_4^{(\ell,i)}\Big[1..\frac{w}{2}\Big], k_2, k_3\Big),\end{aligned} \tag{19}$$

where f_3 is independent from $v_2^{(\ell,i)}$. As we assumed that neither $T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \cdot T_{\mathrm{UR}}$ nor $(T_{\mathrm{BR}} \cdot T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \oplus T_{\mathrm{BL}}) \cdot T_{\mathrm{UR}}$ contains zero entries (see Definition 2), and,—by Lemma 4,—conditioned on $\neg\mathsf{Bad}(\mathcal{S}^*)$ and the values in $\mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, there exists $j' \in \{w/2+1,\ldots,w\}$ such that $v_2^{(\ell,i)}[j'] = S_2^*\big(u_2^{(\ell,i)}[j']\big)$ is uniform in $\ge 2^n - q_S - wq_C/2$ possibilities, the probability to have $v_3^{(\ell,i)}[j] \in \mathrm{Rng}_3 \cup \mathrm{ExtRng}_3^{(\ell)}$ or $u_4^{(\ell,i)}[j] \in \mathrm{Dom}_4 \cup \mathrm{ExtDom}_4^{(\ell)}$ is at most $\frac{2(q_S+wq_C/2)}{2^n-q_S-wq_C/2}$. Summing over the $\beta_\ell w/2$ choices of $(i,j) \in \{1,\ldots,\beta_\ell\} \times \{w/2+1,\ldots,w\}$, we reach

$$\Pr\big[\text{(C-1)} \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \le \frac{3\beta_\ell w(q_S + wq_C/2)}{2(2^n - q_S - wq_C/2)}.$$

Next, consider (C-2). Depending on whether $i_1 = i_2$, we will divide the discussion into two cases.

For the case of $i_1 = i_2 \in \{1,\ldots,\beta_\ell\}$, fix distinct $j_1, j_2 \in \{w/2+1,\ldots,w\}$. Consider the condition $u_3^{(\ell,i_1)}[j_1] = u_3^{(\ell,i_1)}[j_2]$ first. By Lemma 4, conditioned on $\mathsf{Good}(\mathcal{S}^*)$ and the values in $\mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, there exists $j_3 \in \{w/2+1,\ldots,w\}$ such that $v_2^{(\ell,i)}[j_3]$ is uniform in at least $2^n - q_S - wq_C/2$ possibilities. We refer to Eq. (17) for the expression of $u_3^{(\ell,i)}\big[\frac{w}{2}+1..w\big]$. By the 2nd condition in Definition 2, the $(j_1 - w/2, j_3 - w/2)$ th

and $(j_2 - w/2, j_3 - w/2)$ th entries of T_{BR} are not equal. So, the probability to have $u_3^{(\ell,i_1)}[j_1] = u_3^{(\ell,i_1)}[j_2]$ is equal to the probability that $v_2^{(\ell,i)}[j_3]$ equals some fixed value, which is at most $1/(2^n - q_S - wq_C/2)$.

For the conditions $v_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_1)}[j_2]$ and $u_4^{(\ell,i_1)}[j_1] = u_4^{(\ell,i_1)}[j_2]$, the arguments follow similar flows. Concretely, we refer to Eqs. (18) and (19) for the expressions of $v_3^{(\ell,i)}\big[\frac{w}{2}+1..w\big]$ and $u_4^{(\ell,i)}\big[\frac{w}{2}+1..w\big]$ resp. By the 2nd condition in Definition 2, the $(j_1 - w/2, j_3 - w/2)$ th and $(j_2 - w/2, j_3 - w/2)$ th entries of $T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \cdot T_{\mathrm{UR}}$ differ; the $(j_1 - w/2, j_3 - w/2)$ th and $(j_2 - w/2, j_3 - w/2)$ th entries of $(T_{\mathrm{BR}} \cdot T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \oplus T_{\mathrm{BL}}) \cdot T_{\mathrm{UR}}$ differ. By these, the probability to have $v_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_1)}[j_2]$ or $u_4^{(\ell,i_1)}[j_1] = u_4^{(\ell,i_1)}[j_2]$ is at most $2/(2^n - q_S - wq_C/2)$.

For the case of $i_1 \neq i_2$, fix $j_1, j_2 \in \{w/2+1, \ldots, w\}$. By Lemma 4, there exists $j_3, j_4 \in \{w/2+1, \ldots, w\}$ such that:

- $u_2^{(\ell,i_1)}[j_3] \notin \mathrm{Dom}_2 \cup \mathrm{ExtDom}_2^{(\ell)}$, $u_2^{(\ell,i_2)}[j_4] \notin \mathrm{Dom}_2 \cup \mathrm{ExtDom}_2^{(\ell)}$, and
- either $u_2^{(\ell,i_1)}[j_3] \neq u_2^{(\ell,i_2)}[j_3]$ or $u_2^{(\ell,i_1)}[j_4] \neq u_2^{(\ell,i_2)}[j_4]$.

Wlog assume $u_2^{(\ell,i_1)}[j_3] \neq u_2^{(\ell,i_2)}[j_3]$. Note that, by ¬(B-3) (the 2nd condition), $u_2^{(\ell,i_1)}[j_3] \neq u_2^{(\ell,i_2)}[j_5]$ for any $j_5 \in \{w/2+1, \ldots, w\} \backslash \{j_3\}$. Therefore, conditioned on the values in $\mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, on the $w/2-1$ values $\big\{S_2^*\big(u_2^{(\ell,i_1)}[j]\big)\big\}_{j \in \{w/2+1,\ldots,w\} \backslash \{j_3\}}$, and on the $w/2$ values $\big\{S_2^*\big(u_2^{(\ell,i_2)}[j]\big)\big\}_{j \in \{w/2+1,\ldots,w\}}$, $S_2^*\big(u_2^{(\ell,i_1)}[j_3]\big)$ remains uniform in at least $2^n - q_S - wq_C/2$ possibilities. By this,

- since (the $(j_3 - w/2)$ th column of) T_{BR} has no zero entry, the probability to have $u_3^{(\ell,i_1)}[j_1] = u_3^{(\ell,i_2)}[j_2]$ is equal to the probability that $S_2^*(u_2^{(\ell,i_1)}[j_3])$ equals some fixed value, which is at most $1/(2^n - q_S - wq_C/2)$;
- since $T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \cdot T_{\mathrm{UR}}$ has no zero entry, the probability to have $v_3^{(\ell,i_1)}[j_1] = v_3^{(\ell,i_2)}[j_2]$ is at most $1/(2^n - q_S - wq_C/2)$;
- since $(T_{\mathrm{BR}} \cdot T_{\mathrm{UR}}^{-1} \cdot T_{\mathrm{UL}} \oplus T_{\mathrm{BL}}) \cdot T_{\mathrm{UR}}$ has no zero entry, the probability to have $u_4^{(\ell,i_1)}[j_1] = u_4^{(\ell,i_2)}[j_2]$ is at most $1/(2^n - q_S - wq_C/2)$.

By a union bound over the conditions and over all i_1, i_2, j_1, j_2, we reach

$$\Pr_{\mathcal{S}^*}\big[(\text{C-2}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \leq \binom{w\beta_\ell/2}{2} \cdot \frac{3}{2^n - q_S - wq_C/2}.$$

Using $q_S + wq_C/2 \leq 2^n/2$, we finally have

$$\Pr_{\mathcal{S}^*}\big[\mathsf{BadII}_\ell(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \leq \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{2^{n+2}}.$$

Now, conditioned on $\neg\mathsf{BadII}_\ell(\mathcal{S}^*)$, $\mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k})$, and $\mathsf{Good}(\mathcal{S}^*)$, the event that $\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k})$ is equivalent to S_3^* and S_4^* satisfying $w\beta_\ell$ new and distinct equations, i.e., $S_3^*\big(u_3^{(\ell,i)}[j]\big) = v_3^{(\ell,i)}[j]$, $S_4^*\big(u_4^{(\ell,i)}[j]\big) = v_4^{(\ell,i)}[j]$, $i = 1, \ldots, \beta_\ell$, $j \in \{w/2+1, \ldots, w\}$: they are new due to ¬(C-1), and they are distinct due to ¬(C-2) and ¬(B-3). The probability that S_3^* and S_4^* satisfy these equations is *at least* $1/2^{w\beta_\ell n}$. Therefore,

$$\begin{aligned}
&\Pr\big[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \\
\geq\ &\Pr\big[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \neg\mathsf{BadII}_\ell(\mathcal{S}^*) \mid \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \\
\geq\ &\big(1 - \Pr[\mathsf{BadII}_\ell(\mathcal{S}^*)]\big) \\
&\quad \cdot \Pr\big[\mathcal{S}^* \downarrow (Q_{m_\ell}, Q_{\mathcal{S}}, \mathbf{k}) \mid \neg\mathsf{BadII}_\ell(\mathcal{S}^*) \wedge \mathcal{S}^* \downarrow (\cup_{i=1}^{\ell-1} Q_{m_i}, Q_{\mathcal{S}}, \mathbf{k}) \wedge \mathsf{Good}(\mathcal{S}^*)\big] \\
\geq\ &\Big(1 - \frac{12\beta_\ell w(q_S + wq_C/2) + 3\beta_\ell^2 w^2}{2^{n+2}}\Big) \cdot \frac{1}{2^{w\beta_\ell n}}.
\end{aligned}$$

Case 2: Q_{m_ℓ} is Type-II. The argument is symmetric to the above for **Type-I** group. More concretely, we define a bad predicate BadII_ℓ that concerns with the 4nd round S-box inputs as well as the other values involved in the backward computation. For every $(u_1^{(\ell,i)}, u_2^{(\ell,i)}, v_4^{(\ell,i)}, v_5^{(\ell,i)}) \in Q_{m_\ell}$, $i = 1, \ldots, \beta_\ell$, define $u_4^{(\ell,i)} := \big(\mathsf{PS}^{S_4^*}\big)^{-1}(v_4^{(\ell,i)}, \frac{1}{2})$, $v_3^{(\ell,i)} := T^{-1} \cdot \big(u_4^{(\ell,i)} \oplus k_3\big)$,

$$\begin{pmatrix} v_2^{(\ell,i)}\big[\frac{w}{2}+1..w\big] \\ u_3^{(\ell,i)}\big[\frac{w}{2}+1..w\big] \end{pmatrix} = \widehat{T} \cdot \begin{pmatrix} u_2^{(\ell,i)}\big[1..\frac{w}{2}\big] \\ v_3^{(\ell,i)}\big[1..\frac{w}{2}\big] \oplus k_2\big[1..\frac{w}{2}\big] \end{pmatrix} \oplus \begin{pmatrix} 0^{\frac{w}{2}} \\ k_2\big[\frac{w}{2}+1..w\big] \end{pmatrix}.$$

These indicate

$$\begin{aligned}
v_3^{(\ell,i)}\Big[1..\frac{w}{2}\Big] &= (T^{-1})_{\mathrm{UR}} \cdot u_4\Big[\frac{w}{2}+1..w\Big] \oplus f_4\Big(u_4\Big[1..\frac{w}{2}\Big], k_3\Big), \\
v_3^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] &= (T^{-1})_{\mathrm{BR}} \cdot u_4\Big[\frac{w}{2}+1..w\Big] \oplus f_5\Big(u_4\Big[1..\frac{w}{2}\Big], k_3\Big), \\
v_2^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] &= T_{\mathrm{UR}}^{-1} \cdot (T^{-1})_{\mathrm{UR}} \cdot u_4\Big[\frac{w}{2}+1..w\Big] \oplus f_6\Big(u_2\Big[1..\frac{w}{2}\Big], u_4\Big[1..\frac{w}{2}\Big], k_2, k_3\Big), \\
u_3^{(\ell,i)}\Big[\frac{w}{2}+1..w\Big] &= T_{\mathrm{BR}} \cdot T_{\mathrm{UR}}^{-1} \cdot (T^{-1})_{\mathrm{UR}} \cdot u_4\Big[\frac{w}{2}+1..w\Big] \oplus f_7\Big(u_2\Big[1..\frac{w}{2}\Big], u_4\Big[1..\frac{w}{2}\Big], k_2, k_3\Big),
\end{aligned}$$

where f_4, f_5, f_6, f_7 are functions independent from $u_4\big[\frac{w}{2}+1..w\big] = \overline{(S_4^*)^{-1}}\big(v_4\big[\frac{w}{2}+1..w\big]\big)$. Then, $\mathsf{BadII}_\ell(\mathcal{S}^*)$ is fulfilled, if either (C-1) or (C-2) is fulfilled:

- (C-1) There exists $i \in \{1, \ldots, \beta_\ell\}$ and $j \in \{w/2+1, \ldots, w\}$ such that $v_2^{(\ell,i)}[j] \in \mathrm{Rng}_2 \cup \mathrm{ExtRng}_2^{(\ell)}$, or $u_3^{(\ell,i)}[j] \in \mathrm{Dom}_3 \cup \mathrm{ExtDom}_3^{(\ell)}$, or $v_3^{(\ell,i)}[j] \in \mathrm{Rng}_3 \cup \mathrm{ExtRng}_3^{(\ell)}$.
- (C-2) There exists distinct pairs $(i,j), (i',j') \in \{1, \ldots, \beta_\ell\} \times \{w/2+1, \ldots, w\}$ such that $v_2^{(\ell,i)}[j] = v_2^{(\ell,i')}[j']$, or $u_3^{(\ell,i)}[j] = u_3^{(\ell,i')}[j']$, or $v_3^{(\ell,i)}[j] = v_3^{(\ell,i')}[j']$.

The argument then follows similarly, using the goodness (see Definition 2) of the three matrices $(T^{-1})_{\mathrm{BR}}$, $T_{\mathrm{UR}}^{-1} \cdot (T^{-1})_{\mathrm{UR}}$, and $T_{\mathrm{BR}} \cdot T_{\mathrm{UR}}^{-1} \cdot (T^{-1})_{\mathrm{UR}}$, and yielding $w\beta_\ell$ new and distinct equations on S_2^* and S_3^*. Thus Eq. (12) remains true.

4 Security Against Impossible Differential Attacks

We consider impossible differential and zero-correlation linear security in subsect. 4.1 and 4.2 resp.

4.1 Impossible Differential Security

As a warm-up, we first present our negative result on 3-round P-SPNs. We stress that this is unconditional, i.e., the IDs exist regardless of the S-boxes and linear layers in use.

Theorem 2. *There always exist IDs on 3-round P-SPNs with rate $r < 1$, even if two different linear layers T_1 and T_2 are used in the first two rounds respectively.*

Proof. We show $\exists \Delta_1, \Delta_4 \in \mathbb{F}^{(1-r)w}$ such that $\Pr(\Delta_1 \| 0^{wr} \xrightarrow{3\text{ rounds}} \Delta_4 \| 0^{wr}) = 0$. Fix Δ_1, and assume that $T_1 \cdot (\Delta_1 \| 0^{wr}) = \Delta_2 \| \Delta_3$ for $\Delta_2 \in \mathbb{F}^{w(1-r)}$ and $\Delta_3 \in \mathbb{F}^{wr}$, which means $\Pr(\Delta_1 \| 0^{wr} \xrightarrow{\text{Round 1}} \Delta_2 \| \Delta_3) = 1$. Now, for any Δ_4, to have $\Pr(\Delta_2 \| \Delta_3 \xrightarrow{\text{Rounds 2, 3}} \Delta_4 \| 0^{wr}) > 0$, there shall exist $X \in \mathbb{F}^{wr}$ that (at least) fulfills $T_2 \cdot (\Delta_2 \| X) = \Delta_4 \| 0^{wr}$. Viewing X as unknowns, the number of unknowns wr is less than the equations w. Thus there necessarily exits Δ_4 for which *no* X satisfies $T_2 \cdot (\Delta_2 \| X) = \Delta_4 \| 0^{wr}$, i.e., $\Pr(\Delta_1 \| 0^{wr} \xrightarrow{3\text{ rounds}} \Delta_4 \| 0^{wr}) = 0$. □

The positive results are stated w.r.t. the idealized model P-SPN structures $\mathcal{E}_{\text{P-SPN}}$ (see Definition 1), i.e., it relies on the assumption that the IDs are independent from the S-boxes. Formally, this means $\Pr(\Delta_1 \xrightarrow{\mathcal{E}_{\overline{S}}} \Delta_2) > 0$ as long as $\chi(\Delta_1) = \chi(\Delta_2)$, where $\mathcal{E}_{\overline{S}}$ is a "(full) S-layer structure". Under this assumption, we have the main result of this section, i.e., the provable security of 4-round, rate 3/4 P-SPN structures $\mathcal{E}_{\text{P-SPN}}$ *using the same MDS linear layer T in every round.*

Theorem 3. *When $w + 2 \leq 2^n$, for the P-SPN structure $\mathcal{E}_{P\text{-}SPN}$ built upon an MDS linear layer T and with rate $r \geq 3/4$, there does not exist 4-round truncated impossible differentials.*

Proof. We proceed by showing that every pair $(\Delta_{in}, \Delta_{out})$ of differences is possible in $\mathcal{E}_{\text{P-SPN}}$, i.e., writing $\Delta_1 = \Delta_{in}[1..w(1-r)], \Delta_2 = \Delta_{in}[w(1-r)+1..w]$, $\Delta_{10} = \Delta_{out}[1..w(1-r)], \Delta_{12} = \Delta_{out}[w(1-r)+1..w]$, there exists a sequence of differences $\Delta_3, \Delta_5, \Delta_6, \Delta_8, \Delta_9, \Delta_{11} \in \mathbb{F}^{wr}$, $\Delta_4, \Delta_7 \in \mathbb{F}^{w(1-r)}$, such that:

- $\chi(\Delta_2) = \chi(\Delta_3)$ (so that $\Pr(\Delta_2 \xrightarrow{\mathcal{E}_{\overline{S}}} \Delta_3) > 0$); $\chi(\Delta_5) = \chi(\Delta_6)$; $\chi(\Delta_8) = \chi(\Delta_9)$; $\chi(\Delta_{11}) = \chi(\Delta_{12})$; and

$$T \cdot \begin{pmatrix} \Delta_1 \\ \Delta_3 \end{pmatrix} = \begin{pmatrix} \Delta_4 \\ \Delta_5 \end{pmatrix}, \quad T \cdot \begin{pmatrix} \Delta_4 \\ \Delta_6 \end{pmatrix} = \begin{pmatrix} \Delta_7 \\ \Delta_8 \end{pmatrix}, \quad T \cdot \begin{pmatrix} \Delta_7 \\ \Delta_9 \end{pmatrix} = \begin{pmatrix} \Delta_{10} \\ \Delta_{11} \end{pmatrix}.$$

We distinguish three cases as follows.

Case 1: $\boldsymbol{\Delta_2 = \Delta_{12} = 0^{wr}}$. Then $\Delta_4, \Delta_5, \Delta_7, \Delta_9$ are fixed by Δ_1 and Δ_{10}, and our goal is to prove the existence of Δ_6 and Δ_8 that satisfy the above constraints. Since T is MDS, $\mathsf{wt}(\Delta_1 \| \Delta_2) = \mathsf{wt}(\Delta_1) \leq w(1-r)$ implies $\mathsf{wt}(\Delta_4 \| \Delta_5) \geq w + 1 - w(1-r) = wr + 1$. Furthermore, $\mathsf{wt}(\Delta_6) = \mathsf{wt}(\Delta_5) \geq w + 1 - \mathsf{wt}(\Delta_1) - \mathsf{wt}(\Delta_4) \geq w + 1 - 2w(1-r) \geq \frac{w}{2} + 1$ by $r \geq 3/4$. Similarly, $\mathsf{wt}(\Delta_8) \geq w + 1 - 2w(1-r) \geq \frac{w}{2} + 1$.

Assume that the set of indices $\mathcal{I} = \{i_1, \ldots, i_\alpha\}$ is such that $\Delta_6[i] \neq 0$ if and only if $i \in \mathcal{I}$. Similarly, assume that $\mathcal{J} = \{j_1, \ldots, j_\beta\}$ is such that $\Delta_8[j] \neq 0$ if and only if $j \in \mathcal{J}$. As argued, $\alpha = |\mathcal{I}| \geq w/2 + 1$, $\beta = |\mathcal{J}| \geq w/2 + 1$. Then the above 2nd equation is written as

$$T \cdot \begin{pmatrix} \Delta_4 \\ \Delta_6[1] \\ \cdots \\ \Delta_6[wr] \end{pmatrix} = \begin{pmatrix} \Delta_7 \\ \Delta_8[1] \\ \cdots \\ \Delta_8[wr] \end{pmatrix}.$$

It can be seen there exists a matrix T' obtained by rearranging the rows and columns of T, such that

$$T' \cdot \begin{pmatrix} \Delta_4 \\ 0^{wr-\alpha} \\ \Delta_6[i_{\frac{w}{2}+1}] \\ \cdots \\ \Delta_6[i_\alpha] \\ \Delta_6[i_1] \\ \cdots \\ \Delta_6[i_{\frac{w}{2}}] \end{pmatrix} = \begin{pmatrix} \Delta_7 \\ 0^{wr-\beta} \\ \Delta_8[j_{\frac{w}{2}+1}] \\ \cdots \\ \Delta_8[j_\beta] \\ \Delta_8[j_1] \\ \cdots \\ \Delta_8[j_{\frac{w}{2}}] \end{pmatrix} \implies \begin{pmatrix} \Delta_6[i_1] \\ \cdots \\ \Delta_6[i_{\frac{w}{2}}] \\ \Delta_8[j_1] \\ \cdots \\ \Delta_8[j_{\frac{w}{2}}] \end{pmatrix} = \widehat{T'} \cdot \underbrace{\begin{pmatrix} \Delta_4 \\ 0^{wr-\alpha} \\ \Delta_6[i_{\frac{w}{2}+1}] \\ \cdots \\ \Delta_6[i_\alpha] \\ \Delta_7 \\ 0^{wr-\beta} \\ \Delta_8[j_{\frac{w}{2}+1}] \\ \cdots \\ \Delta_8[j_\beta] \end{pmatrix}}_{\text{denoted } \mathbf{z}}.$$

Now, once we fix $\Delta_6[i_{\frac{w}{2}+1}], \ldots, \Delta_6[i_\alpha], \Delta_8[j_{\frac{w}{2}+1}], \ldots, \Delta_8[j_\beta - 1]$ to any non-zero values, the number of non-zero choices for $\Delta_8[j_\beta]$ that give rise to $\Delta_6[i_1] \neq \mathsf{0}, \ldots, \Delta_6[i_{\frac{w}{2}}] \neq \mathsf{0}, \Delta_8[j_1] \neq \mathsf{0}, \ldots, \Delta_8[j_{\frac{w}{2}}] \neq \mathsf{0}$ is at least $2^n - w - 1$. The argument is as follows. Write

$$\widehat{T'} = \begin{pmatrix} \mathbf{t}_{1,1}^\mathsf{T} & t_{1,2} \\ \cdots & \cdots \\ \mathbf{t}_{w,1}^\mathsf{T} & t_{w,2} \end{pmatrix},$$

where $\mathbf{t}_{1,1}, \ldots, \mathbf{t}_{w,1} \in \mathbb{F}^{w-1}$, $t_{1,2}, \ldots, t_{w,2} \in \mathbb{F}$. Note that T' is MDS, since it is obtained by rearranging rows and columns of T. By Lemma 1, $\widehat{T'}$ is also MDS, meaning that $t_{1,2} \neq \mathsf{0}, \ldots, t_{w,2} \neq \mathsf{0}$. Therefore, (1) To ensure $\Delta_6[i_1] \neq \mathsf{0}$, $\Delta_8[j_\beta]$ shall fulfill $\Delta_8[j_\beta] \neq t_{1,2}^{-1} \cdot \big(\mathbf{t}_{1,1}^\mathsf{T} \cdot \mathbf{z}[1..w-1]\big)$; …; ($w$) To ensure $\Delta_8[j_{\frac{w}{2}}] \neq \mathsf{0}$, $\Delta_8[j_\beta]$ shall fulfill $\Delta_8[j_\beta] \neq t_{w,2}^{-1} \cdot \big(\mathbf{t}_{w,1}^\mathsf{T} \cdot \mathbf{z}[1..w-1]\big)$. These plus the condition $\Delta_8[j_\beta] \neq \mathsf{0}$ exclude at most $w+1$ values in total, and thus the claim.

By these, when $2^n - w - 1 \geq 1$, there always exist $\Delta_6[i_1] \neq \mathsf{0}, \ldots, \Delta_6[i_\alpha] \neq \mathsf{0}, \Delta_8[j_1] \neq \mathsf{0}, \ldots, \Delta_8[j_\beta] \neq \mathsf{0}$ satisfying $T \cdot (\Delta_4 \| \Delta_6) = (\Delta_7 \| \Delta_8)$, which means $\Pr(\Delta_1 \| \mathsf{0}^{wr} \xrightarrow{4 \text{ rounds}} \Delta_{10} \| \mathsf{0}^{wr}) > 0$, i.e., the 4-round differential is possible.

Case 2: $\boldsymbol{\Delta_2 \neq \mathsf{0}^{wr}, \Delta_{12} = \mathsf{0}^{wr}}$. Then $\Delta_7 \| \Delta_9$ is fixed by Δ_{10}, and $\mathsf{wt}(\Delta_8) = \mathsf{wt}(\Delta_9) \geq w/2 + 1$ as argued. We show that there exists $\Delta_3 \in \mathbb{F}^{wr}$ such that

$$\begin{pmatrix} \Delta_4 \\ \Delta_5 \end{pmatrix} = T \cdot \begin{pmatrix} \Delta_1 \\ \Delta_3 \end{pmatrix}$$

satisfies $\mathsf{wt}(\Delta_5) \geq w/2 + 1$—and then, the existence of the other intermediate differences follow from the above argument for Case 1. For this, note that since $\Delta_2 \neq \mathsf{0}^{wr}$, there exists $i \in \{1, \ldots, wr\}$ such that $\Delta_3[i] \neq \mathsf{0}$. By this, write

$$T = \begin{pmatrix} \mathbf{t}_{1,1}^\mathsf{T} & \mathbf{t}_{1,2}^\mathsf{T} & t_{1,3} & \mathbf{t}_{1,4}^\mathsf{T} \\ \cdots & \cdots & \cdots & \cdots \\ \mathbf{t}_{w,1}^\mathsf{T} & \mathbf{t}_{w,2}^\mathsf{T} & t_{w,3} & \mathbf{t}_{w,4}^\mathsf{T} \end{pmatrix},$$

where $\mathbf{t}_{1,1}, \ldots, \mathbf{t}_{w,1} \in \mathbb{F}^{w(1-r)}$, $\mathbf{t}_{1,2}, \ldots, \mathbf{t}_{w,2} \in \mathbb{F}^{i-1}$, $t_{1,3}, \ldots, t_{w,3} \in \mathbb{F}$, and $\mathbf{t}_{1,4}, \ldots, \mathbf{t}_{w,4} \in \mathbb{F}^{wr-i}$. Then, given $\Delta_3[1..i-1]$ and $\Delta_3[i+1..wr]$, to ensure that $\Delta_5[j] \neq \mathsf{0}$ for $w/2+1$ indices $j = w/2, \ldots, w$, $\Delta_3[i]$ can take any value in the set $\mathbb{F} \backslash \big\{\mathsf{0}, t_{\frac{w}{2},3}^{-1} \cdot (\mathbf{t}_{\frac{w}{2},1}^\mathsf{T} \cdot \Delta_1 \oplus \mathbf{t}_{\frac{w}{2},2}^\mathsf{T} \cdot \Delta_3[1..i-1] \oplus \mathbf{t}_{\frac{w}{2},4}^\mathsf{T} \cdot \Delta_3[i+1..wr]), \ldots, t_{w,3}^{-1} \cdot (\mathbf{t}_{w,1}^\mathsf{T} \cdot \Delta_1 \oplus \mathbf{t}_{w,2}^\mathsf{T} \cdot \Delta_3[1..i-1] \oplus \mathbf{t}_{w,4}^\mathsf{T} \cdot \Delta_3[i+1..wr])\big\}$, the size of which is at least $2^n - \frac{w}{2} - 2$. By this and our assumption $w+2 \leq 2^n \Rightarrow \frac{w}{2} + 2 < 2^n$, such $\Delta_3[i]$—and further Δ_3—exist, and thus the claim.

Case 3: When $\boldsymbol{\Delta_2 = \mathsf{0}^{wr}}$ while $\boldsymbol{\Delta_{12} \neq \mathsf{0}^{wr}}$, the argument is similar to Case 2 by symmetry; when $\Delta_2 \neq \mathsf{0}^{wr}$ and $\Delta_{12} \neq \mathsf{0}^{wr}$, following the same line as Case 2, it can be shown that there always exists $\Delta_3, \Delta_9 \in \mathbb{F}^{wr}$ such that $\Delta_4 \| \Delta_5 = T \cdot (\Delta_1 \| \Delta_3)$ and $\Delta_7 \| \Delta_9 = T^{-1} \cdot (\Delta_{10} \| \Delta_{11})$ satisfy $\mathsf{wt}(\Delta_5) \geq w/2 + 1, \mathsf{wt}(\Delta_{11}) \geq w/2 + 1$, and then the possibility is established by a similar counting argument as before. These conclude the proof. □

4.2 Zero-Correlation Linear Security

The positive results regarding ZC attacks again rely on structures. Formally, this means $\mathsf{cor}_{\mathcal{E}_S}(\alpha_1, \alpha_2) \neq 0$ as long as $\chi(\alpha_1) = \chi(\alpha_2)$. Under this idealized assumption, Sun et al. showed that the existence of impossible differential in an SPN is equivalent to the existence of zero correlation linear hull in the "dual structure" of this SPN [SLG+16]. But the "dual structure" of P-SPNs has never been formalized. For simplicity, we establish the ZC security via Theorem 3.

Theorem 4. *When $w+2 \leq 2^n$, for the P-SPN structure $\mathcal{E}_{P\text{-}SPN}$ built upon an MDS linear layer T and with rate $r \geq 3/4$, there does not exist 4-round zero correlation linear hull.*

Proof. Assume that $\mathcal{C}4$ is the 4-round rate r P-SPN structure $\mathcal{E}_{\text{P-SPN}}$ using an MDS T as the linear layer. For any $\alpha_1, \alpha_2 \in \mathbb{F}^w \backslash \{0^w\}$, we show that

$$\mathsf{cor}_{\mathcal{C}4}(\alpha_1, \alpha_2) = 0 \Longrightarrow \Pr\left(\alpha_1 \xrightarrow{\mathcal{C}4'} \alpha_3\right) = 0, \tag{20}$$

where $\mathcal{C}4'$ is the rate r P-SPN structure $\mathcal{E}_{\text{P-SPN}}$ built upon the MDS linear layer $(T^{\mathsf{T}})^{-1}$ (since T is MDS, T^{T} is also MDS and invertible). This implies the claim by Theorem 3.

To show Eq. (20), we show $\Pr\left(\alpha_1 \xrightarrow{\mathcal{C}4'} \alpha_3\right) > 0 \Longrightarrow \mathsf{cor}_{\mathcal{C}4}(\alpha_1, \alpha_2) > 0$. To this end, we write $\alpha_1 = \Delta_1 \| \Delta_2$, $\alpha_2 = \Delta_{10} \| \Delta_{12}$, $\Delta_1, \Delta_{10} \in \mathbb{F}^{w(1-r)}$, $\Delta_2, \Delta_{12} \in \mathbb{F}^{wr}$, then there exists a sequence of masks $\Delta_3, \Delta_5, \Delta_6, \Delta_8, \Delta_9, \Delta_{11} \in \mathbb{F}^{wr}$, $\Delta_4, \Delta_7 \in \mathbb{F}^{w(1-r)}$, such that $\chi(\Delta_2) = \chi(\Delta_3)$; $\chi(\Delta_5) = \chi(\Delta_6)$; $\chi(\Delta_8) = \chi(\Delta_9)$; $\chi(\Delta_{11}) = \chi(\Delta_{12})$; and

$$(T^{\mathsf{T}})^{-1} \cdot \begin{pmatrix} \Delta_1 \\ \Delta_3 \end{pmatrix} = \begin{pmatrix} \Delta_4 \\ \Delta_5 \end{pmatrix}, \ (T^{\mathsf{T}})^{-1} \cdot \begin{pmatrix} \Delta_4 \\ \Delta_6 \end{pmatrix} = \begin{pmatrix} \Delta_7 \\ \Delta_8 \end{pmatrix}, \ (T^{\mathsf{T}})^{-1} \cdot \begin{pmatrix} \Delta_7 \\ \Delta_9 \end{pmatrix} = \begin{pmatrix} \Delta_{10} \\ \Delta_{11} \end{pmatrix}.$$

Note that this implies

$$(\Delta_1^{\mathsf{T}}, \Delta_3^{\mathsf{T}}) = (\Delta_4^{\mathsf{T}}, \Delta_5^{\mathsf{T}}) \cdot T, \quad (\Delta_4^{\mathsf{T}}, \Delta_6^{\mathsf{T}}) = (\Delta_7^{\mathsf{T}}, \Delta_8^{\mathsf{T}}) \cdot T, \quad (\Delta_7^{\mathsf{T}}, \Delta_9^{\mathsf{T}}) = (\Delta_{10}^{\mathsf{T}}, \Delta_{11}^{\mathsf{T}}) \cdot T,$$

which further means $\mathsf{cor}_{\mathcal{C}4}(\alpha_1, \alpha_2) > 0$. Thus the claim. □

5 Linear Layers for P-SPNs with Rate Below 1/2

We first establish a theorem regarding the differential propagation in such "sparse" P-SPNs. The construction of the linear layers will be clear during its proof. For conceptual convenience, in (and only in) this section we let $\rho = r^{-1}$, and write $1/\rho$ (instead of r) for the rate.

Theorem 5. *For any integer ρ such that $\rho w \leq 2^n$, for rate $1/\rho$ P-SPNs, ρ rounds are necessary and sufficient to ensure at least one active S-box during differential propagation.*

Proof. **Necessity.** This seems a folklore. Formally, assume that the linear layers used in the i th round is T_i. Then, by construction, if there exists a $(\rho-1)$-round differential characteristic with no active S-box, then there exists $\Delta_1, \ldots, \Delta_{\rho-1} \in \mathbb{F}^w$ such that:

- (C-1) $T_1 \cdot \Delta_1 = \Delta_2, T_2 \cdot \Delta_2 = \Delta_3, \ldots, T_{\rho-2} \cdot \Delta_{\rho-2} = \Delta_{\rho-1}$, and
- (C-2) $\mathsf{wt}\big(\Delta_1\big[\frac{(\rho-1)w}{\rho} + 1..w\big]\big) = 0, \ldots, \mathsf{wt}\big(\Delta_{\rho-1}\big[\frac{(\rho-1)w}{\rho} + 1..w\big]\big) = 0.$

(So that $\Delta_1 \xrightarrow{\text{Round 1}} \Delta_2 \xrightarrow{\text{Round 2}} \ldots \xrightarrow{\text{Round } \rho-2} \Delta_{\rho-1} \xrightarrow{\text{Round } \rho-1} \Delta_\rho$ is a $(\rho-1)$-round characteristic with no active S-box. Note that the final round only contains a partial S-box layer, and thus the difference $\Delta_{\rho-1}$ is invariant.)

We show that the above equations are equivalent to a linear equation system with $\frac{(\rho-1)^2 wn}{\rho}$ equations and $\frac{(\rho-1)^2 wn}{\rho}$ unknowns, and this system always has non-zero solutions. For this, consider the i th equation $T_i \cdot \Delta_i = \Delta_{i+1}$. By condition (C-2), it can be written in the following block form

$$\begin{pmatrix} T_{i,1} & \star \\ T_{i,2} & \star \end{pmatrix} \begin{pmatrix} \Delta_i\big[1..\frac{(\rho-1)w}{\rho}\big] \\ 0^{\frac{w}{\rho}} \end{pmatrix} = \begin{pmatrix} \Delta_{i+1}\big[1..\frac{(\rho-1)w}{\rho}\big] \\ 0^{\frac{w}{\rho}} \end{pmatrix},$$

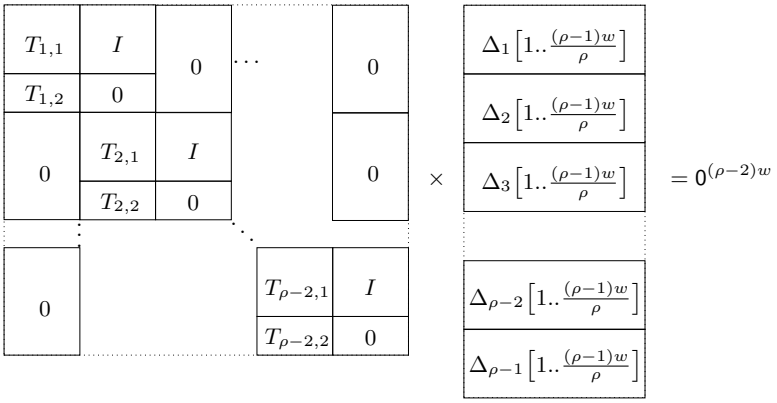

Figure 4: The homogeneous linear equation system derived in the proof of Theorem 5.

where $T_{i,1} \in \mathbb{F}^{\frac{(\rho-1)w}{\rho} \times \frac{(\rho-1)w}{\rho}}$, $T_{i,2} \in \mathbb{F}^{\frac{w}{\rho} \times \frac{(\rho-1)w}{\rho}}$. The right most $\frac{w}{\rho}$ columns of T_i are multiplied by $0^{w/\rho}$ and have no influence, and thus we simply refer to them by $\star$. The equations imply the following homogeneous system:

$$\begin{pmatrix} T_{i,1} & I \\ T_{i,2} & 0 \end{pmatrix} \begin{pmatrix} \Delta_i[1..\frac{(\rho-1)w}{\rho}] \\ \Delta_{i+1}[1..\frac{(\rho-1)w}{\rho}] \end{pmatrix} = 0^{\frac{2(\rho-1)w}{\rho}},$$

where the I is the identity matrix in $\mathbb{F}^{\frac{(\rho-1)w}{\rho} \times \frac{(\rho-1)w}{\rho}}$.

For $i = 1, \ldots, \rho-2$, we obtain $\rho-2$ such homogeneous systems on $\frac{(\rho-1)^2 w}{\rho}$ unknowns $\Delta_1[1..\frac{(\rho-1)w}{\rho}], \ldots, \Delta_{\rho-2}[1..\frac{(\rho-1)w}{\rho}], \Delta_{\rho-1}[1..\frac{(\rho-1)w}{\rho}]$. Combining them yields a homogeneous system shown in Fig. 4. The system has $\frac{(\rho-1)^2 w}{\rho}$ unknowns, and its coefficient matrix has only $(\rho-2)w$ rows. As $(\rho-2) < \frac{(\rho-1)^2}{\rho}$, this system always has (approximately $\frac{2^n w}{\rho}$) non-zero solutions, and every such solution turns out to be a differential characteristic on $\rho-1$ rounds with no active S-box.

Sufficiency. We explicitly construct such a tuple of $\rho-1$ transformations $T_{M1}, \ldots, T_{M\rho-1}$ via the following steps.

1. Construct a $[\rho w, w, (\rho-1)w+1]$ MDS code. Assume that

   $$G = \left(G_1^{\mathsf{T}}, G_2^{\mathsf{T}}, \ldots, G_\rho^{\mathsf{T}}\right) \in \mathbb{F}^{w \times 2^n}$$

   is the generator matrix of this code, where $G_1^{\mathsf{T}}, \ldots, G_\rho^{\mathsf{T}} \in \mathbb{F}^{w \times w}$.

2. Then the $\rho-1$ matrices are defined by the (transpose of the) ρw columns of G as $T_{Mi} = G_1^{-1} \cdot G_{i+1} \cdot \prod_{j=1}^{i-1} T_{Mj}^{-1}$. More clearly,

   $$\begin{aligned} T_{M1} &= G_1^{-1} \cdot G_2, \\ T_{M2} &= G_1^{-1} \cdot G_3 \cdot T_{M1}^{-1}, \\ T_{M3} &= G_1^{-1} \cdot G_4 \cdot T_{M1}^{-1} \cdot T_{M2}^{-1}, \\ T_{M4} &= G_1^{-1} \cdot G_5 \cdot T_{M1}^{-1} \cdot T_{M2}^{-1} \cdot T_{M3}^{-1}, \ldots \end{aligned}$$

Using the above $T_{M1}, \ldots, T_{M\rho-1}$, we argue that there does not exist ρ-round differential with 0 active S-box. Assume otherwise, then there exists an input difference Δ_1 such

that $\mathsf{wt}(\Delta_1[\frac{(\rho-1)w}{\rho}+1..w])=0$, $\mathsf{wt}(\Delta_2[\frac{(\rho-1)w}{\rho}+1..w])=0$, ..., $\mathsf{wt}(\Delta_\rho[\frac{(\rho-1)w}{\rho}+1..w])=0$, where $\Delta_2 = T_{M1}\cdot\Delta_1$, ..., $\Delta_\rho = T_{M\rho-1}\cdot\Delta_{\rho-1}$. By our construction, $(\Delta_1,\ldots,\Delta_\rho)$ is a code word of a $[\rho w, w, (\rho-1)w+1]$ code. Therefore, $\sum_{i=1}^{\rho}\mathsf{wt}(\Delta_i)\geq(\rho-1)w+1$. By the pigeonhole principle, there exists $i\in\{1,\ldots,\rho\}$ such that $\mathsf{wt}(\Delta_i)\geq\frac{(\rho-1)w}{\rho}+1$, and thus $\mathsf{wt}(\Delta_i[\frac{(\rho-1)w}{\rho}+1..w])\geq 1$. This contradicts our assumption of no active S-box and completes the proof. □

Note that, while the above transformations $T_{M1}, T_{M2},\ldots$ appear quite complicated, *they are all MDS*. To see this, consider $T_{Mi} = G_1^{-1}\cdot G_{i+1}\cdot\prod_{j=1}^{i-1}T_{Mj}^{-1}$. It can be seen the set $\{(x, T_{Mi}\cdot x) : x\in\mathbb{F}^w\}$ is equal to the set $\{(G_1^{-1}\cdot G_i\cdot T_{Mi-1}\cdot\ldots\cdot T_{M1}\cdot x, G_1^{-1}\cdot G_{i+1}\cdot x) : x\in\mathbb{F}^w\}$, which further equals $\{(G_i\cdot x, G_{i+1}\cdot x) : x\in\mathbb{F}^w\}$ by the definitions. By the property of MDS codes, the set $\{(x^\mathsf{T}\cdot G_i^\mathsf{T}, x^\mathsf{T}\cdot G_{i+1}^\mathsf{T}) : x\in\mathbb{F}^w\}$ constitute all the codewords of a small MDS code. Therefore, T_{Mi} is MDS.

Practical parameters. It has been proved that, when $w\geq 2$, a linear $[\rho w, w, (\rho-1)w+1]$ MDS code exists only if $\rho w\leq 2^n+w-1$ [MS77, Corollary 7]. Though, for general w, explicit constructions are only given for $\rho w\leq 2^n+1$ using the theory of Reed-Solomon codes [MS77, Theorem 9]. We refer to [MS77, Theorem 9] for the detailed construction. This means the above approach for rate r is effective iff. $wr^{-1}\leq 2^n+1$ (recall that $\rho=r^{-1}$), meaning an inapplicability for very small n. Indeed, a typical choice in the lightweight setting is to use 4-bit S-boxes, i.e., $n=4$. Unfortunately, even if we target a (smaller) 64-bit blockcipher, i.e., $w=16$, the $[2^4+1, 16, 2]$ does not imply even a single MDS linear transformation. Similarly, nothing meaningful can be achieved for the LowMC parameter $n=3$ [ARS+15].

Though, meaningful results can be derived for larger n. In detail, assuming targeting 128-bit P-SPNs with the AES parameter $n=8$ (i.e., $w=16$), $[64, 16, 49]$ codes can be constructed for P-SPNs with rate 1/4 (i.e., 4 S-boxes per round, matching the Zorro parameters [GGNS13]), while $[128, 16, 113]$ codes can be constructed for P-SPNs with rate 1/8 (i.e., 2 S-boxes per round). See the column with the header (8,128) in Table 2.

Larger values for n are certainly preferred, but such S-boxes seem to be more costly. To remedy, we advocate using *large-but-weak* S-boxes, which significantly enlarges the design space. For example, 11-bit S-boxes with acceptable performance can be found in [BDMD+20] or constructed via the SHA3 approach [BDPA11], 64-bit ARX S-boxes have been recently constructed [BBdS+20], and power-based S-boxes on non-binary field of size around 2^{255} was used in [GKK+19]. As discussed in [BDMD+20], some of these large S-boxes *are even cheaper* for relevant scenarios such as side-channel masking. As shown in Table 2, with $n=11$, if we target a 352-bit P-SPN (i.e., $w=32$), then linear layers for P-SPNs with rates ranging from 1/2 to 1/32 can be constructed. We omit the calculations for various other meaningful cases and only summarize some (im)possibilities in Table 2.

6 Conclusion

We provide the first systematic provable security analysis of SP networks with partial non-linear layers (P-SPNs), regarding SPRP security and provable security against impossible differential and zero-correlation linear attacks. For P-SPNs with rate $r<1/2$, $r^{-1}\in\mathbb{N}$, we also propose the first dedicated linear layers that consist of $r^{-1}-1$ different transformations and ensures at least one active S-boxes in r^{-1} rounds. Our results have justified P-SPNs as a sound approach comparable to or even surpass the normal SPNs in some well-defined sense.

We leave several open problems as follows.

Table 2: Linear layers for P-SPNs: (in)applicability of our MDS code-based method. The numbers (which literally equal wr^{-1}) indicate the length of the MDS code required for the corresponding group of parameters, which is followed by either $\times$ meaning that linear layers *cannot* be constructed via our method & the explicit constructions of [MS77, Theorem 9], or ✓ otherwise. "-" means the group of parameters is meaningless due to $rw < 1$.

(n,blocksize)	(4,64)	(8,64)	(8,128)	(8,256)	(9,144)	(11,88)	(11,352)
Rate $r = 1/2$	32 $\times$	16 ✓	32 ✓	64 ✓	32 ✓	16 ✓	48 ✓
Rate $r = 1/4$	64 $\times$	32 ✓	64 ✓	128 ✓	64 ✓	32 ✓	96 ✓
Rate $r = 1/8$	128 $\times$	64 ✓	128 ✓	256 ✓	128 ✓	64 ✓	192 ✓
Rate $r = 1/16$	256 $\times$	-	256 ✓	512 $\times$	256 ✓	-	384 ✓
Rate $r = 1/32$	-	-	-	1024 $\times$	512 ✓	-	1024 ✓

(i) Characterize the security of 4-round rate 1/2 P-SPN. We didn't find any Chosen-Ciphertext Attack (CCA), and it may be possible to prove CCA security using a more complicated analysis and a stronger assumption on the linear layer.

(ii) Seek for principled design for good linear layers given in Definition 2. Note that if T is an extended Cauchy matrix fulfilling certain conditions [RS85], then T is MDS and the conditions on T_{BR} are indeed fulfilled. We remark that (extended) Cauchy matrices were helpful in quite a number of prior nice works [KR18, GKK+19]. Though, it remains to verify if the other (much more complicated) requirements are all fulfilled & to characterize the conditions (we are not aware of relevant research).

(iii) Investigate whether larger rates imply better (at least non-decreasing) security. Intuitively, this seems true. Our proof of Theorem 1 could indeed be tweaked to cover 5-round P-SPNs with rate beyond 1/2 (i.e., by revealing the "extra" S-box queries inside the construction queries to the adversary, and treating them equivalently as those in $Q_{\mathcal{S}}$), but general positive results seem difficult and remain open.

(iv) Investigate whether computational hardness assumptions (such as the hardness of LPN or MQ problems) help breaking the troublesome n-bit information theoretic security barrier in P-SPNs.

(v) Seek for provable security of SPNs and P-SPNs against ID/ZC attacks under more realistic assumptions. As mentioned, attempts have been made w.r.t. AES-like SPNs [WJ18].

(vi) Seek for more persuasive theory results justifying the advantages of P-SPNs. Possible approaches include lower bounds on algebraic degrees (as recently explored in [HLLT20]) and certain forms of security amplifications (as in [Vau03, MPR07, LTV21]).

(vii) Explore more applications of large-but-weak S-boxes in concrete P-SPN blockciphers.

Acknowledgments

Chun Guo was partly supported by the Program of Qilu Young Scholars (Grant No. 61580089963177) of Shandong University, the National Natural Science Foundation of China (Grant No. 62002202), the National Key Research and Development Project under Grant No.2018YFA0704702, and the Shandong Nature Science Foundation of China (Grant No. ZR2020MF053). Weijia Wang was partly supported by the Program of Qilu Young Scholars (Grant No. 61580082063088) of Shandong University, National Natural Science Foundation of China (Grant No. 62002204). We sincerely appreciate Lorenzo Grassi,

Christian Rechberger, Markus Schofnegger, Qingju Wang, as well as the anonymous reviewers for their invaluable comments.

References

[ARS+15] Martin R. Albrecht, Christian Rechberger, Thomas Schneider, Tyge Tiessen, and Michael Zohner. Ciphers for MPC and FHE. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 430–454. Springer, Heidelberg, April 2015.

[BBdS+20] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Léo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. Alzette: A 64-bit ARX-box - (feat. CRAX and TRAX). In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2020, Part III*, LNCS, pages 419–448. Springer, Heidelberg, August 2020.

[BBS99] Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials. In Jacques Stern, editor, *EUROCRYPT'99*, volume 1592 of *LNCS*, pages 12–23. Springer, Heidelberg, May 1999.

[BDD+15] Achiya Bar-On, Itai Dinur, Orr Dunkelman, Virginie Lallemand, Nathan Keller, and Boaz Tsaban. Cryptanalysis of SP networks with partial non-linear layers. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part I*, volume 9056 of *LNCS*, pages 315–342. Springer, Heidelberg, April 2015.

[BDMD+20] Begül Bilgin, Lauren De Meyer, Sébastien Duval, Itamar Levi, and François-Xavier Standaert. Low and depth and efficient inverses: a guide on s-boxes for low-latency masking. *IACR Transactions on Symmetric Cryptology*, 2020(1):144–184, May 2020.

[BDPA11] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The Keccak reference. 2011.

[BFMT16] Thierry P. Berger, Julien Francq, Marine Minier, and Gaël Thomas. Extended Generalized Feistel Networks Using Matrix Representation to Propose a New Lightweight Block Cipher: Lilliput. *IEEE Trans. Computers*, 65(7):2074–2089, 2016.

[BGW+14] Andrey Bogdanov, Huizheng Geng, Meiqin Wang, Long Wen, and Baudoin Collard. Zero-correlation linear cryptanalysis with FFT and improved attacks on ISO standards Camellia and CLEFIA. In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *SAC 2013*, volume 8282 of *LNCS*, pages 306–323. Springer, Heidelberg, August 2014.

[BLN18] Ritam Bhaumik, Eik List, and Mridul Nandi. ZCZ - achieving n-bit SPRP security with a minimal number of tweakable-block-cipher calls. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part I*, volume 11272 of *LNCS*, pages 336–366. Springer, Heidelberg, December 2018.

[BR14] Andrey Bogdanov and Vincent Rijmen. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. *Des. Codes Cryptography*, 70(3):369–383, 2014.

[BW12] Andrey Bogdanov and Meiqin Wang. Zero correlation linear cryptanalysis with reduced data complexity. In Anne Canteaut, editor, *FSE 2012*, volume 7549 of *LNCS*, pages 29–48. Springer, Heidelberg, March 2012.

[CDK+18] Benoît Cogliati, Yevgeniy Dodis, Jonathan Katz, Jooyoung Lee, John P. Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang. Provable security of (tweakable) block ciphers based on substitution-permutation networks. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2018, Part I*, volume 10991 of *LNCS*, pages 722–753. Springer, Heidelberg, August 2018.

[CS14] Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, Heidelberg, May 2014.

[DFLM19] Patrick Derbez, Pierre-Alain Fouque, Baptiste Lambin, and Victor Mollimard. Efficient Search for Optimal Diffusion Layers of Generalized Feistel Networks. *IACR Trans. Symmetric Cryptol.*, 2019(2):218–240, 2019.

[DKP+19] Itai Dinur, Daniel Kales, Angela Promitzer, Sebastian Ramacher, and Christian Rechberger. Linear equivalence of block ciphers with partial non-linear layers: Application to LowMC. In Yuval Ishai and Vincent Rijmen, editors, *EUROCRYPT 2019, Part I*, volume 11476 of *LNCS*, pages 343–372. Springer, Heidelberg, May 2019.

[DKS+17] Yevgeniy Dodis, Jonathan Katz, John Steinberger, Aishwarya Thiruvengadam, and Zhe Zhang. Provable security of substitution-permutation networks. Cryptology ePrint Archive, Report 2017/016, 2017. http://eprint.iacr.org/2017/016.

[Dod18] Yevgeniy Dodis. Small Box Cryptography and The Provable Security of SPNs. *EUROCRYPT 2018 rump session*, 2018.

[DSSL16] Yevgeniy Dodis, Martijn Stam, John P. Steinberger, and Tianren Liu. Indifferentiability of confusion-diffusion networks. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 679–704. Springer, Heidelberg, May 2016.

[GGNS13] Benoît Gérard, Vincent Grosso, María Naya-Plasencia, and François-Xavier Standaert. Block ciphers that are easier to mask: How far can we go? In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES 2013*, volume 8086 of *LNCS*, pages 383–399. Springer, Heidelberg, August 2013.

[git19] The Dusk Network Project. 2019.

[GKK+19] Lorenzo Grassi, Daniel Kales, Dmitry Khovratovich, Arnab Roy, Christian Rechberger, and Markus Schofnegger. Starkad and Poseidon: New hash functions for zero knowledge proof systems. Cryptology ePrint Archive, Report 2019/458, 2019. https://eprint.iacr.org/2019/458.

[GLR+20] Lorenzo Grassi, Reinhard Lüftenegger, Christian Rechberger, Dragos Rotaru, and Markus Schofnegger. On a generalization of substitution-permutation networks: The HADES design strategy. In Vincent Rijmen and Yuval Ishai, editors, *EUROCRYPT 2020, Part II*, LNCS, pages 674–704. Springer, Heidelberg, May 2020.

[GM02] Henri Gilbert and Marine Minier. New results on the pseudorandomness of some blockcipher constructions. In Mitsuru Matsui, editor, *FSE 2001*, volume 2355 of *LNCS*, pages 248–266. Springer, Heidelberg, April 2002.

[GRS20] Lorenzo Grassi, Christian Rechberger, and Markus Schofnegger. Proving Resistance Against Infinitely Long Subspace Trails: How to Choose the Linear Layer. Cryptology ePrint Archive, Report 2020/500, 2020. https://eprint.iacr.org/2020/500.

[Hal04] Shai Halevi. EME*: Extending EME to handle arbitrary-length messages with associated data. In Anne Canteaut and Kapalee Viswanathan, editors, *INDOCRYPT 2004*, volume 3348 of *LNCS*, pages 315–327. Springer, Heidelberg, December 2004.

[HLLT20] Phil Hebborn, Baptiste Lambin, Gregor Leander, and Yosuke Todo. Lower Bounds on the Degree of Block Ciphers. *IACR Cryptol. ePrint Arch.*, 2020:1051, 2020. To appear at ASIACRYPT 2020.

[HR03] Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In Dan Boneh, editor, *CRYPTO 2003*, volume 2729 of *LNCS*, pages 482–499. Springer, Heidelberg, August 2003.

[HR04] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In Tatsuaki Okamoto, editor, *CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304. Springer, Heidelberg, February 2004.

[HR10] Viet Tung Hoang and Phillip Rogaway. On generalized Feistel networks. In Tal Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 613–630. Springer, Heidelberg, August 2010.

[IK01] Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of the AES finalists - RC6 and Serpent. In Bruce Schneier, editor, *FSE 2000*, volume 1978 of *LNCS*, pages 231–243. Springer, Heidelberg, April 2001.

[KL15] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography, 2nd edition*. Chapman & Hall/CRC Press, 2015.

[KR18] Pierre Karpman and Daniel S. Roche. New instantiations of the CRYPTO 2017 masking schemes. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part II*, volume 11273 of *LNCS*, pages 285–314. Springer, Heidelberg, December 2018.

[Lee13] Jooyoung Lee. Security of the Misty structure beyond the birthday bound. Cryptology ePrint Archive, Report 2013/430, 2013. http://eprint.iacr.org/2013/430.

[LM91] Xuejia Lai and James L. Massey. A proposal for a new block encryption standard. In Ivan Damgård, editor, *EUROCRYPT'90*, volume 473 of *LNCS*, pages 389–404. Springer, Heidelberg, May 1991.

[LR88] Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[LTV21] Tianren Liu, Stefano Tessaro, and Vinod Vaikuntanathan. The t-wise Independence of Substitution-Permutation Networks. *IACR Cryptol. ePrint Arch.*, 2021:507, 2021.

[Mat94] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In Tor Helleseth, editor, *EUROCRYPT'93*, volume 765 of *LNCS*, pages 386–397. Springer, Heidelberg, May 1994.

[Mat97] Mitsuru Matsui. New block encryption algorithm MISTY. In Eli Biham, editor, *FSE'97*, volume 1267 of *LNCS*, pages 54–68. Springer, Heidelberg, January 1997.

[MDRMH10] Hamid Mala, Mohammad Dakhilalian, Vincent Rijmen, and Mahmoud Modarres-Hashemi. Improved impossible differential cryptanalysis of 7-round AES-128. In Guang Gong and Kishan Chand Gupta, editors, *INDOCRYPT 2010*, volume 6498 of *LNCS*, pages 282–291. Springer, Heidelberg, December 2010.

[MPR07] Ueli M. Maurer, Krzysztof Pietrzak, and Renato Renner. Indistinguishability amplification. In Alfred Menezes, editor, *CRYPTO 2007*, volume 4622 of *LNCS*, pages 130–149. Springer, Heidelberg, August 2007.

[MS77] F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam: North Holland, 1977.

[MV00] Shiho Moriai and Serge Vaudenay. On the pseudorandomness of top-level schemes of block ciphers. In Tatsuaki Okamoto, editor, *ASIACRYPT 2000*, volume 1976 of *LNCS*, pages 289–302. Springer, Heidelberg, December 2000.

[MV15] Eric Miles and Emanuele Viola. Substitution-Permutation Networks, Pseudorandom Functions, and Natural Proofs. *J. ACM*, 62(6):46:1–46:29, 2015.

[Nan14] Mridul Nandi. XLS is not a strong pseudorandom permutation. In Palash Sarkar and Tetsu Iwata, editors, *ASIACRYPT 2014, Part I*, volume 8873 of *LNCS*, pages 478–490. Springer, Heidelberg, December 2014.

[Nan15] Mridul Nandi. On the optimality of non-linear computations of length-preserving encryption schemes. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part II*, volume 9453 of *LNCS*, pages 113–133. Springer, Heidelberg, November / December 2015.

[NR99] Moni Naor and Omer Reingold. On the construction of pseudorandom permutations: Luby-Rackoff revisited. *Journal of Cryptology*, 12(1):29–66, January 1999.

[Pat09] Jacques Patarin. The "coefficients H" technique (invited talk). In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *SAC 2008*, volume 5381 of *LNCS*, pages 328–345. Springer, Heidelberg, August 2009.

[PW20] Thomas Peyrin and Haoyang Wang. The MALICIOUS framework: Embedding backdoors into tweakable block ciphers. In Hovav Shacham and Alexandra Boldyreva, editors, *CRYPTO 2020, Part III*, LNCS, pages 249–278. Springer, Heidelberg, August 2020.

[RR07] Thomas Ristenpart and Phillip Rogaway. How to enrich the message space of a cipher. In Alex Biryukov, editor, *FSE 2007*, volume 4593 of *LNCS*, pages 101–118. Springer, Heidelberg, March 2007.

[RS85] Ron M. Roth and Gadiel Seroussi. On generator matrices of MDS codes. *IEEE Trans. Inf. Theory*, 31(6):826–830, 1985.

[SLG+16] Bing Sun, Meicheng Liu, Jian Guo, Vincent Rijmen, and Ruilin Li. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 196–213. Springer, Heidelberg, May 2016.

[SLR+15] Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda AlKhzaimi, and Chao Li. Links among impossible differential, integral and zero correlation linear cryptanalysis. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 95–115. Springer, Heidelberg, August 2015.

[SM10] Tomoyasu Suzaki and Kazuhiko Minematsu. Improving the generalized Feistel. In Seokhie Hong and Tetsu Iwata, editors, *FSE 2010*, volume 6147 of *LNCS*, pages 19–39. Springer, Heidelberg, February 2010.

[Vau03] Serge Vaudenay. Decorrelation: A theory for block cipher security. *Journal of Cryptology*, 16(4):249–286, September 2003.

[WJ18] Qian Wang and Chenhui Jin. Upper bound of the length of truncated impossible differentials for AES. *Des. Codes Cryptogr.*, 86(7):1541–1552, 2018.

[YPL11] Aaram Yun, Je Hong Park, and Jooyoung Lee. On Lai-Massey and quasi-Feistel ciphers. *Des. Codes Cryptogr.*, 58(1):45–72, 2011.

[ZCD+19] Greg Zaverucha, Melissa Chase, David Derler, Steven Goldfeder, Claudio Orlandi, Sebastian Ramacher, Christian Rechberger, Daniel Slamanig, Jonathan Katz, Xiao Wang, and Vladmir Kolesnikov. Picnic. Technical report, National Institute of Standards and Technology, 2019. available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-2-submissions.

[ZMI90] Yuliang Zheng, Tsutomu Matsumoto, and Hideki Imai. On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In Gilles Brassard, editor, *CRYPTO'89*, volume 435 of *LNCS*, pages 461–480. Springer, Heidelberg, August 1990.

A A Chosen-Plaintext Attack on 3 Rounds

Nandi showed that no wn-bit linear structure making less than $2w$ calls to the n-bit block function can be secure [Nan15]. We adapt that idea to our context. Concretely, let $\mathcal{C}3$ be the 3-round P-SPN using any linear transformations T_1, T_2. I.e.,

$$\mathcal{C}3^{\mathcal{S}}_{\mathbf{k}}(x) := k_3 \oplus \mathsf{PS}^{S_3}(k_2 \oplus T_2(\mathsf{PS}^{S_2}(k_1 \oplus T_1(\mathsf{PS}^{S_1}(k_0 \oplus x, 1/2)), 1/2)), 1/2).$$

We show a chosen-plaintext attacker D, given access to an oracle $\mathcal{O} : \{0,1\}^{wn} \to \{0,1\}^{wn}$, that distinguishes whether $\mathcal{O}$ is an instance of $\mathcal{C}3^{\mathcal{S}}_{\mathbf{k}}$ using uniform keys or a wn-bit random permutation. The attacker D proceeds as follows:

1. Fix $\delta \in \mathbb{F}\backslash\{0\}$ in arbitrary, let $\Delta_3 = \delta \| 0^{w/2-1}$, and compute two $wn/2$-bit differences $\Delta_1 := (T_1)^{-1}_{\mathrm{BL}} \cdot \Delta_3$ and $\Delta_2 := (T_1)_{\mathrm{UL}} \cdot \Delta_1$. Note that this means $T_1 \cdot (\Delta_1 \| 0^{w/2}) = \Delta_2 \| \Delta_3$.
2. For all $\delta^* \in \mathbb{F}\backslash\{0\}$, compute $\Delta^* := T_2 \cdot (\Delta_2 \| \delta^* \| 0^{w/2-1})$, and add $\Delta^*[1..w/2]$ into a set Set.[5]

[5] Here we consider the information theoretic setting, with no limit on the time complexity. In practice, n is usually small, and this enumeration remains feasible.

3. Choose inputs x, x' such that $x \oplus x' = \Delta_1 \| 0^{w/2}$, query $\mathcal{O}(x)$ and $\mathcal{O}(x')$ to obtain y and y' respectively, and compute the output difference $\Delta_4 := y \oplus y'$.

4. If $\Delta_4[1..w/2] \in \mathsf{Set}$ then output 1; otherwise, output 0.

It is not hard to see that if $\mathcal{O}$ is a wn-bit random permutation then D outputs 1 with probability $O(2^n/2^{wn/2})$. On the other hand, we claim that when $\mathcal{O}$ is an instance of the 3-round P-SPN then D always outputs 1. For this, consider the propagation of the input difference $\Delta_1 \| 0^{w/2}$. By step 1, the 2nd round input difference must be $\Delta_2 \| \Delta_3$. Since $\Delta_3 = \delta \| 0^{w/2-1}$, the output difference of the PS^{S_2} action must be in the set $\{\delta^* \| 0^{w/2-1}\}_{\delta^* \in \mathbb{F} \setminus \{0\}}$ of size $2^n - 1$. This means the 3rd round input difference, denoted Δ_3^*, must be in a set of size $2^n - 1$. Since the 3rd round PS^{S_3} action does not affect $\Delta_3^*[1..w/2]$, it can be seen $\Delta_4[1..w/2]$, the first half of the final output difference, is also in a set of size $2^n - 1$. Furthermore, this set *is* the set Set derived in step 2. This completes the analysis.

B Candidate Good Linear Layers for Definition 2

Using the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$, two candidates for $n = 8$ and $w = 8, 16$ respectively are as follows.

$$\begin{pmatrix} 0\text{x}C4 & 0\text{x}57 & 0\text{x}E6 & 0\text{x}A7 & 0\text{x}63 & 0\text{x}EF & 0\text{x}E1 & 0\text{x}BE \\ 0\text{x}49 & 0\text{x}AA & 0\text{x}0A & 0\text{x}C5 & 0\text{x}88 & 0\text{x}7B & 0\text{x}D6 & 0\text{x}08 \\ 0\text{x}6A & 0\text{x}B3 & 0\text{x}F8 & 0\text{x}E9 & 0\text{x}26 & 0\text{x}9D & 0\text{x}BE & 0\text{x}CC \\ 0\text{x}F8 & 0\text{x}04 & 0\text{x}EA & 0\text{x}36 & 0\text{x}42 & 0\text{x}A4 & 0\text{x}1A & 0\text{x}DD \\ 0\text{x}1B & 0\text{x}46 & 0\text{x}3B & 0\text{x}AB & 0\text{x}D3 & 0\text{x}43 & 0\text{x}78 & 0\text{x}24 \\ 0\text{x}3C & 0\text{x}AB & 0\text{x}03 & 0\text{x}A4 & 0\text{x}E5 & 0\text{x}1F & 0\text{x}22 & 0\text{x}E9 \\ 0\text{x}23 & 0\text{x}20 & 0\text{x}84 & 0\text{x}A8 & 0\text{x}61 & 0\text{x}EB & 0\text{x}61 & 0\text{x}C5 \\ 0\text{x}B5 & 0\text{x}8C & 0\text{x}71 & 0\text{x}E3 & 0\text{x}93 & 0\text{x}09 & 0\text{x}12 & 0\text{x}22 \end{pmatrix},$$

$$\begin{pmatrix} 0\text{x}4A & 0\text{x}E5 & 0\text{x}32 & 0\text{x}5C & 0\text{x}FF & 0\text{x}F2 & 0\text{x}FB & 0\text{x}14 & 0\text{x}85 & 0\text{x}69 & 0\text{x}58 & 0\text{x}EA & 0\text{x}57 & 0\text{x}F6 & 0\text{x}9E & 0\text{x}0E \\ 0\text{x}C9 & 0\text{x}9D & 0\text{x}A3 & 0\text{x}AD & 0\text{x}5D & 0\text{x}A5 & 0\text{x}EE & 0\text{x}F7 & 0\text{x}6C & 0\text{x}30 & 0\text{x}5A & 0\text{x}7E & 0\text{x}17 & 0\text{x}36 & 0\text{x}21 & 0\text{x}75 \\ 0\text{x}E5 & 0\text{x}81 & 0\text{x}8D & 0\text{x}F7 & 0\text{x}66 & 0\text{x}29 & 0\text{x}A0 & 0\text{x}70 & 0\text{x}D4 & 0\text{x}B9 & 0\text{x}5D & 0\text{x}93 & 0\text{x}E1 & 0\text{x}1A & 0\text{x}6F & 0\text{x}2E \\ 0\text{x}84 & 0\text{x}55 & 0\text{x}D8 & 0\text{x}51 & 0\text{x}7C & 0\text{x}8F & 0\text{x}E4 & 0\text{x}9A & 0\text{x}5F & 0\text{x}4B & 0\text{x}7A & 0\text{x}5C & 0\text{x}C4 & 0\text{x}FC & 0\text{x}9C & 0\text{x}D1 \\ 0\text{x}41 & 0\text{x}F1 & 0\text{x}35 & 0\text{x}6F & 0\text{x}06 & 0\text{x}FB & 0\text{x}17 & 0\text{x}1C & 0\text{x}57 & 0\text{x}18 & 0\text{x}69 & 0\text{x}AA & 0\text{x}33 & 0\text{x}39 & 0\text{x}E2 & 0\text{x}D7 \\ 0\text{x}61 & 0\text{x}DE & 0\text{x}26 & 0\text{x}7B & 0\text{x}41 & 0\text{x}CF & 0\text{x}BD & 0\text{x}D5 & 0\text{x}BA & 0\text{x}FA & 0\text{x}57 & 0\text{x}D6 & 0\text{x}88 & 0\text{x}E9 & 0\text{x}58 & 0\text{x}F9 \\ 0\text{x}33 & 0\text{x}D5 & 0\text{x}18 & 0\text{x}8C & 0\text{x}6D & 0\text{x}4C & 0\text{x}CE & 0\text{x}18 & 0\text{x}EE & 0\text{x}0F & 0\text{x}20 & 0\text{x}D7 & 0\text{x}EE & 0\text{x}1D & 0\text{x}C9 & 0\text{x}BF \\ 0\text{x}4E & 0\text{x}E0 & 0\text{x}66 & 0\text{x}33 & 0\text{x}8A & 0\text{x}C9 & 0\text{x}C9 & 0\text{x}27 & 0\text{x}C7 & 0\text{x}C7 & 0\text{x}42 & 0\text{x}27 & 0\text{x}AE & 0\text{x}BD & 0\text{x}C3 & 0\text{x}09 \\ 0\text{x}54 & 0\text{x}33 & 0\text{x}C7 & 0\text{x}09 & 0\text{x}90 & 0\text{x}81 & 0\text{x}EA & 0\text{x}C8 & 0\text{x}B7 & 0\text{x}D2 & 0\text{x}C5 & 0\text{x}79 & 0\text{x}1A & 0\text{x}0F & 0\text{x}60 & 0\text{x}B6 \\ 0\text{x}B1 & 0\text{x}93 & 0\text{x}3D & 0\text{x}F3 & 0\text{x}CD & 0\text{x}A1 & 0\text{x}73 & 0\text{x}B2 & 0\text{x}66 & 0\text{x}07 & 0\text{x}82 & 0\text{x}3F & 0\text{x}02 & 0\text{x}42 & 0\text{x}81 & 0\text{x}73 \\ 0\text{x}F8 & 0\text{x}9F & 0\text{x}68 & 0\text{x}EC & 0\text{x}86 & 0\text{x}C5 & 0\text{x}EC & 0\text{x}C8 & 0\text{x}9E & 0\text{x}DE & 0\text{x}99 & 0\text{x}25 & 0\text{x}26 & 0\text{x}83 & 0\text{x}AB & 0\text{x}AF \\ 0\text{x}BF & 0\text{x}0E & 0\text{x}D4 & 0\text{x}53 & 0\text{x}DF & 0\text{x}9D & 0\text{x}95 & 0\text{x}84 & 0\text{x}25 & 0\text{x}2C & 0\text{x}74 & 0\text{x}FC & 0\text{x}E9 & 0\text{x}9F & 0\text{x}98 & 0\text{x}78 \\ 0\text{x}B5 & 0\text{x}81 & 0\text{x}CA & 0\text{x}96 & 0\text{x}75 & 0\text{x}83 & 0\text{x}57 & 0\text{x}39 & 0\text{x}02 & 0\text{x}CF & 0\text{x}4B & 0\text{x}57 & 0\text{x}FB & 0\text{x}02 & 0\text{x}2D & 0\text{x}E0 \\ 0\text{x}99 & 0\text{x}F7 & 0\text{x}30 & 0\text{x}EC & 0\text{x}57 & 0\text{x}D3 & 0\text{x}96 & 0\text{x}29 & 0\text{x}D3 & 0\text{x}C4 & 0\text{x}27 & 0\text{x}0E & 0\text{x}2A & 0\text{x}88 & 0\text{x}74 & 0\text{x}70 \\ 0\text{x}DE & 0\text{x}6A & 0\text{x}ED & 0\text{x}14 & 0\text{x}59 & 0\text{x}94 & 0\text{x}C4 & 0\text{x}4D & 0\text{x}8D & 0\text{x}11 & 0\text{x}BC & 0\text{x}78 & 0\text{x}A0 & 0\text{x}DC & 0\text{x}82 & 0\text{x}AE \\ 0\text{x}EE & 0\text{x}9A & 0\text{x}F9 & 0\text{x}D6 & 0\text{x}66 & 0\text{x}FD & 0\text{x}18 & 0\text{x}95 & 0\text{x}91 & 0\text{x}BD & 0\text{x}02 & 0\text{x}68 & 0\text{x}39 & 0\text{x}50 & 0\text{x}F4 & 0\text{x}31 \end{pmatrix}.$$

Using the primitive polynomial $x^{11} + x^2 + 1$ a candidate for $n = 11$ and $w = 8$ is as follows:

$$\begin{pmatrix} 0\text{x}416 & 0\text{x}297 & 0\text{x}0D9 & 0\text{x}5EC & 0\text{x}357 & 0\text{x}64A & 0\text{x}417 & 0\text{x}112 \\ 0\text{x}05C & 0\text{x}603 & 0\text{x}3DD & 0\text{x}226 & 0\text{x}4DB & 0\text{x}700 & 0\text{x}65C & 0\text{x}356 \\ 0\text{x}743 & 0\text{x}269 & 0\text{x}7D9 & 0\text{x}5D3 & 0\text{x}707 & 0\text{x}24A & 0\text{x}262 & 0\text{x}1AF \\ 0\text{x}214 & 0\text{x}0D7 & 0\text{x}596 & 0\text{x}035 & 0\text{x}685 & 0\text{x}5B9 & 0\text{x}6EC & 0\text{x}721 \\ 0\text{x}357 & 0\text{x}53D & 0\text{x}640 & 0\text{x}6EE & 0\text{x}6EE & 0\text{x}117 & 0\text{x}1A1 & 0\text{x}0FA \\ 0\text{x}4AB & 0\text{x}757 & 0\text{x}1AF & 0\text{x}385 & 0\text{x}790 & 0\text{x}090 & 0\text{x}261 & 0\text{x}1D3 \\ 0\text{x}44D & 0\text{x}55A & 0\text{x}5D8 & 0\text{x}0BD & 0\text{x}79E & 0\text{x}69C & 0\text{x}3CE & 0\text{x}7A8 \\ 0\text{x}2AD & 0\text{x}11B & 0\text{x}37D & 0\text{x}7FB & 0\text{x}0EF & 0\text{x}1A3 & 0\text{x}6CA & 0\text{x}24A \end{pmatrix}.$$

We have also found plenty of candidates for $n = 11$ and w up to 32, which are however omitted for the sake of space.

C 4 Rounds with Rate 1/2

While it might appear that we can follow the proof of 4-round Feistel network [LR88] to get a proof for *4-round rate 1/2 P-SPNs*, we find this untrue for $w \geq 4$. In detail, the proof idea for 4-round Feistel is as follows. It can be shown that, with high probability, the q_C construction queries $((x^{(1)}, y^{(1)}), \ldots, (x^{(q_C)}, y^{(q_C)}))$ induce $2q_C$ distinct pairs of input/outputs $((u_2^{(1)}, v_2^{(1)}), \ldots, (u_2^{(q_C)}, v_2^{(q_C)}), (u_3^{(1)}, v_3^{(1)}), \ldots, (u_3^{(q_C)}, v_3^{(q_C)}))$ on the 2nd and 3rd round functions G_2, G_3. Then, the probability that an interaction yields the transcript $((x^{(1)}, y^{(1)}), \ldots, (x^{(q_C)}, y^{(q_C)}))$ is $\Pr[G_2(u_2^{(i)}) = v_2^{(i)} \wedge G_3(u_3^{(i)}) = v_3^{(i)}, i = 1, \ldots, q_C] = 1/2^{2q_C n}$, which is close to the ideal world.

Following this, one may expect the same in 4-round rate 1/2 P-SPNs, i.e., q_C construction queries $((x^{(1)}, y^{(1)}), \ldots, (x^{(q_C)}, y^{(q_C)}))$ induce wq_C distinct pairs of input/outputs $((u_2^{(1)}[\frac{w}{2} +$

$1], v_2^{(1)}[\frac{w}{2}+1]), \ldots, (u_2^{(q_C)}[w], v_2^{(q_C)}[w]), (u_3^{(1)}[\frac{w}{2}+1], v_3^{(1)}[\frac{w}{2}+1]), \ldots, (u_3^{(q_C)}[w], v_3^{(q_C)}[w]))$ on the 2nd and 3rd round S-boxes. It is indeed the case for $w = 2$ (which is, however, less meaningful): briefly, for any distinct $((x, y), (x', y'))$, if $x[2] \neq x'[2]$ then the randomness of S_1 ensures $u_2[2] \neq u'_2[2]$ w.h.p., else the MDS property of the linear layer $T \in \mathbb{F}^{2\times 2}$ ensures $u_2[2] \neq u'_2[2]$, and similarly for $v_3[2] \neq v'_3[2]$. Though, for $w \geq 4$, it's easy to choose x, x' such that $T \cdot (x \oplus x')[w/2 + 2] = \mathsf{0}$, i.e., $u_2[w/2 + 2] = u'_2[w/2 + 2]$, breaking the expectation.

Facing the difficulty w.r.t. 4 rounds, we resort to more rounds for better readability. In fact, *6* rounds are needed to ensure that the q_C construction queries induce wq_C equations on two "fixed" middle rounds, i.e., in the 3rd and 4th rounds. Using a slightly more sophisticated idea as in Sect. 3.2, we tried to achieve wq_C equations in the 2nd, 3rd, and 4th rounds depending on the properties of the constructions queries in question. This enables a more (involved) proof with *5* rounds.

D Differential Security

As mentioned in Introduction, our conclusions on provable security against differential attacks are mainly negative: some trivial security lower bounds are indeed tight.

First, recall that Theorem 5 shows ρ rounds needed for at least 1 active S-box. One naturally asks if non-trivial lower bounds on the number of active S-boxes can be proved. Unfortunately, we find this impossible.

Theorem 6. *For any integer ρ, for rate $1/\rho$ P-SPNs, there always exist ρ-round differential characteristics with only 1 active S-box, even if $\rho - 1$ different linear layers $T_1, \ldots, T_{\rho-1}$ are used in the ρ rounds.*

Proof sketch. The proof is a simple extension of the existential proof for $(\rho-1)$-round probability-1 characteristics (Theorem 5). In detail, consider $\rho + 1$ differences $\Delta_1, \ldots, \Delta_{\rho+1}$ such that:

- (C-1) $T_1 \cdot \Delta_1 = \Delta_2, T_2 \cdot \Delta_2 = \Delta_3, \ldots, T_{\rho-1} \cdot \Delta_{\rho-1} = \Delta_\rho$, and
- (C-2) $\mathsf{wt}\big(\Delta_1\big[\frac{(\rho-1)w}{\rho} + 1..w\big]\big) = 0, \ldots, \mathsf{wt}\big(\Delta_{\rho-1}\big[\frac{(\rho-1)w}{\rho} + 1..w\big]\big) = 0$; $\Delta_\rho\big[\frac{(\rho-1)w}{\rho} + 1\big] \neq \mathsf{0}$, and $\Delta_\rho\big[\frac{(\rho-1)w}{\rho} + 2..w\big] \neq \mathsf{0}^{wr-1}$.

We have proved that, for $i = 1, \ldots, \rho-2$, we obtain a homogeneous system with $(\rho-2)w$ equations on $\frac{(\rho-1)^2 w}{\rho}$ unknowns $\Delta_1[1..\frac{(\rho-1)w}{\rho}], \ldots, \Delta_{\rho-2}[1..\frac{(\rho-1)w}{\rho}], \Delta_{\rho-1}[1..\frac{(\rho-1)w}{\rho}]$. The added equation $T_{\rho-1} \cdot \Delta_{\rho-1} = \Delta_\rho$ adds $\frac{(\rho-1)w}{\rho} + 1$ unknowns and $\frac{2w}{\rho}$ equations. By this, the final homogeneous system has $(\rho - 1)w$ equations on $(\rho - 1)w + 1$ unknowns, which always has non-trivial solutions. Hence, such characteristic always exists. □

Second, consider $r \geq \frac{1}{3}$. Using MDS linear layers, it is easy to see that the number of active S-boxes in 2-round differential characteristics is at least $w + 1 - 2w(1 - r)$, which is tight. For 3-round characteristics, $w + 1 - 2w(1 - r) + wr = (3r - 1)w + 1$ is a trivial lower bound for the number of active S-boxes. Unfortunately, this is also tight.

Theorem 7. *For rate r P-SPNs, there always exist 3-round differential characteristics with at most $(3r - 1)w + 1$ active S-boxes, even if two linear layers T_1, T_2 are used.*

Proof. We seek for a differential characteristic $\Delta_1 \| \Delta_2 \to \Delta_3 \| \mathsf{0}^{wr} \to \Delta_4 \| \Delta_5$ with $\Delta_1, \Delta_3, \Delta_4 \in \mathbb{F}^{(1-r)w}$ and $\Delta_2, \Delta_5 \in \mathbb{F}^{rw}$ requires solving the following equation system:

$$T_1 \cdot \begin{pmatrix} \Delta_1 \\ \Delta_2 \end{pmatrix} = \begin{pmatrix} \Delta_3 \\ \mathsf{0}^{wr} \end{pmatrix}, \quad T_2 \cdot \begin{pmatrix} \Delta_3 \\ \mathsf{0}^{wr} \end{pmatrix} = \begin{pmatrix} \Delta_4 \\ \Delta_5 \end{pmatrix}.$$

This system can be reorganized as $2w$ homogeneous equations on α variables, where $\alpha = \mathsf{wt}(\Delta_1) + \mathsf{wt}(\Delta_2) + \mathsf{wt}(\Delta_3) + \mathsf{wt}(\Delta_4) + \mathsf{wt}(\Delta_5)$. To ensure the existence of non-trivial solutions, it has to be $\alpha \geq 2w + 1$, which means $\mathsf{wt}(\Delta_2) + \mathsf{wt}(\Delta_4) \geq 2w + 1 - 3(1 - r)w = (3r - 1)w + 1$. Thus the claim. □