Beyond-Birthday-Bound Security for Linear Substitution-Permutation Networks

Yuan Gao[1,2], Chun Guo[1,2(✉)], Meiqin Wang[1,2(✉)], and Jiejing Wen[1,2(✉)]

[1] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China,
[2] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China

May 6, 2020

gaoyuanwangan@mail.sdu.edu.cn,chun.guo@sdu.edu.cn,mqwang@sdu.edu.cn

Abstract. Recent works (Cogliati et al., CRYPTO 2018) have initiated provable treatments of Substitution-Permutation Networks (SPNs), one of the most popular approach to construct modern blockciphers. Such theoretical SPN models may employ *non-linear* diffusion layers, which enables beyond-birthday-bound provable security. Though, for the model of real world blockciphers, i.e., SPN models with *linear diffusion layers*, existing provable results are capped at birthday security up to $2^{n/2}$ adversarial queries, where n is the size of the idealized S-boxes.
This paper overcomes this birthday barrier and proves that a 4-round SPN with linear diffusion layers and independent round keys is secure up to $2^{2n/3}$ queries. Besides, this paper considers tweaking linear SPNs by xoring a tweak with each round key, and prove that 6-round such tweakable linear SPN is secure up to $2^{2n/3}$ queries. These provides additional theoretic supports for the real world SPN (tweakable) blockciphers.

Keywords: tweakable blockciphers · substitution-permutation networks · beyond-birthday-bound

1 Introduction

Substitution-Permutation Networks. Most modern blockciphers are

built via two different generic structures: Feistel networks or substitution-permutation networks (SPNs). These two approaches revolve around the extension of a "complex" function or permutation on a small domain to a keyed pseudorandom permutation on a larger domain by iterating several times simple rounds. SPNs start with a set of public permutations on the set of n-bit strings which are called S-boxes. These public permutations are then extended to a keyed permutation on wn-bit inputs for some integer w by iterating the following steps:

1. break down the state in w n-bit blocks;
2. compute an S-box on each block of the state;

3. apply a keyed permutation layer to the whole wn-bit state (which is also applied to the plaintext before the first round).

Many well-known block ciphers including AES, Serpent and PRESENT follow this approach.

Proving the security of a particular concrete block cipher is currently beyond our techniques. Thus, the usual approach is to prove that the high-level structure is sound in a relevant security model. As for Feistel networks, a substantial line of work starting with Luby and Rackoff's seminal work [LR88] and culminating with Patarin's results [Pat03, Pat04] proves optimal security with a sufficient number of rounds. Numerous other articles [Pat10, HR10, HKT11, Tes14, CHK+16] study the security of (variants of) Feistel networks in various security models. On the other hand, SPNs have comparatively seen very little interest which seems rather surprising.

Tweaking SPNs. Recently, a similar study was undertaken for the second large class of block ciphers besides Feistel ciphers, namely key-alternating ciphers [DR01], a super-class of Substitution-Permutation Networks (SPNs). An r-round key-alternating cipher based on a tuple of public n-bit permutations $(P_1, ..., P_r)$ maps a plaintext $x \in \{0, 1\}^n$ to the ciphertext defined as where the n-bit round keys $k_0, ..., k_r$ are either independent or derived from a master key k. When the P_i's are modeled as public permutation oracles, construction (1) is also referred to as the (iterated) Even-Mansour construction, in reference to Even and Mansour who pioneered the analysis of this construction in the Random Permutation Model [EM97]. While Even and Mansour limited themselves to proving birthday-bound security in the case r = 1, larger numbers of rounds were studied in subsequent works [BKL+12, Ste12, LPS12]. The general case has been recently (tightly) settled by Chen and Steinberger [CS14], who proved that the r-round iterated Even-Mansour cipher with r-wise independent round keys ensures security up to roughly 2^{rn} r+1 adversarial queries. In order to incorporate a tweak t in the iterated Even-Mansour construction, it is tantalizing to generalize (1) by replacing round keys k_i by some function $f_i(\mathbf{k}, \mathbf{t})$ of the master key **k** and the tweak **t** (see Figure 1). We will refer to such a construction as a Tweakable Even-Mansour (TEM) construction. This is exactly the spirit of the TWEAKEY framework introduced by Jean et al. [JNP14]. In fact, these authors go one step further and propose to unify the key and tweak inputs into what they dub the tweakey. The main topic of this paper being provable security (in the traditional model where the key is secret and the tweak is chosen by the adversary), we will not make such a bold move here, since we are not aware of any formal security model adequately capturing what Jean et al. had in mind.

The investigation of the theoretical soundness of this design strategy was initiated in three recent papers. First, Cogliati and Seurin [CS15], and independently Farshim and Procter [FP15], analyzed the simple case of an n-bit key k and an n-bit tweak t simply xored together at each round, i.e., $f_i(k, t) = k_t$ for each $i = 0, ..., r$. They gave attacks up to two rounds, and proved birthday-bound security for three rounds. In fact, the security of this construction caps at $2^{n/2}$ queries independently of the number of rounds. Indeed, it can be written

$\widehat{E}(k,t,x) = E(k \oplus t, x)$, where E is the conventional iterated Even-Mansour cipher with the trivial key-schedule (i.e., the same round key is xored between each round), and by a result of Bellare and Kohno [BK03, Corollary 5.7], a tweakable block cipher of this form can never offer more than $\kappa/2$ bits of security, where κ is the key-length of E (i.e., $\kappa = n$ in the case at hand). Hence, if we want beyond-birthday-bound security, we have no choice but to consider more complex functions f_i (at the bare minimum, these functions, even if linear, should prevent the TBC construction from being of the form $E(k \oplus t, x)$ for some block cipher E with n-bit keys).

This was undertaken by Cogliati, Lampe, and Seurin [CLS15], who considered nonlinear ways of mixing the key and the tweak. More specifically, they studied the case where $f_i(\mathbf{k}, t) = H_{k_i}(t)$, where the family of functions (H_k) is uniform and almost XOR-universal, and the master key is $\mathbf{k} = (k_0, ..., k_r)$. Cogliati et al. showed that one round is secure up to the birthday bound, and that two rounds are secure up to roughly $2^{2n/3}$ adversarial queries. They also provided a (non-tight) asymptotic security bound improving as the number of rounds grows. However, implementing a xor-universal hash function might be costly, and linear functions f_i's would be highly preferable for obvious efficiency reasons.

1.1 Our Results

In this paper, we ask whether it is possible to achieve security beyond the birthday barrier with linear SPN structures. In detail, we focus on linear SPNs with independent S-boxes and independent round keys, and we will focus on the case where $w \geq 2$, since, when $w = 1$, we recover the standard Even-Mansour construction that has already been the focus of a long line of work (as briefly reviewed later). For such linear SPNs, we prove the first beyond-birthday-bound (BBB) result on 4 rounds. To tweak such linear SPNs, we consider the simplest approach, i.e., directly xoring a wn-bit tweak with each round key, and prove BBB result on 6 rounds. We will elaborate in detail as follows.

BBB Security for 4-round linear SPNs.

Tweaking linear SPNs and BBB Security at 6 rounds.

1.2 Related Work

Unfortunately, none of the currently known black-box TBC constructions with beyond-birthday-bound security can be deemed truly practical (even though some of them might come close to it [Men15]). Hence, it might be beneficial to "open the hood" and to study how to build a TBC from some lower level primitive than a full-fledged conventional block cipher, e.g., a pseudorandom function or a public permutation. For example, Goldenberg et al. [GHL+07] investigated how to include a tweak in Feistel ciphers. This was extended to generalized Feistel ciphers by Mitsuda and Iwata [MI08].

2 Preliminaries

Throughout this work, we fix positive integers w and n, and let $N = 2^n$. An element x in $\{0,1\}^{wn}$ can be viewed as a concatenation of w blocks of length n. The ith block of this representation will be denoted $x[i]$ for $i = 1, \ldots, w$, so we have $x = x[1] \| x[2] \| \ldots \| x[w]$. For any integer r such that $r \geq s$, we will write $(r)_s = r!/(r-s)!$, and define $(r)_0 := 1$ for completeness.

Tweakable Blockciphers. For an integer $m \geq 1$, the set of all permutations on $\{0,1\}^m$ will be denoted $\mathsf{Perm}(m)$. A tweakable permutation with tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $\widetilde{P} : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that, for any tweak $t \in \mathcal{T}$,

$$x \mapsto \widetilde{P}(t, x)$$

is a permutation of $\mathcal{X}$. The set of all tweakable permutations with tweak space $\mathcal{T}$ and message space $\{0,1\}^m$ will be denoted $\widetilde{\mathsf{Perm}}(\mathcal{T}, m)$.

A tweakable blockcipher, or a keyed tweakable permutation, with key space $\mathcal{K}$, tweak space $\mathcal{T}$ and message space $\mathcal{X}$ is a mapping $T : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that, for any key $k \in \mathcal{K}$,

$$(t, x) \mapsto T(k, t, x).$$

is a tweakable permutation with tweak space $\mathcal{T}$ and message space $\mathcal{X}$.

(Tweakable) Linear Substitution-Permutation Networks. A *substitution-permutation network* (SPN) defines a keyed permutation via repeated invocation of two transformations: blockwise computation of a public, cryptographic permutation called an "S-box," and application of a keyed, non-cryptographic permutation. In this paper we will only introduce a model of linear SPNs. Formally, let $\mathcal{K}$ and $\mathcal{T}$ be two sets, and let $\mathbf{f} = (f_0, ..., f_r)$ be a $(r+1)$-tuple of functions from $\mathcal{K} \times \mathcal{T}$ to $\{0,1\}^n$.

Formally, an r-round SPN taking inputs of length wn is defined by $r+1$ round keys $tk_0, tk_1, \ldots, tk_r \in \{0,1\}^{wn}$, r permutations $S_1, \ldots, S_r : \{0,1\}^n \to \{0,1\}^n$, and $r-1$ invertible linear permutations $T_1, \ldots, T_{r-1} \in \mathbb{F}^{w \times w}$. Given an input $x \in \{0,1\}^{wn}$, the output of the SPN is computed as follows:

- Let $x_1 := x$.
- For $i = 1$ to $r-1$ do:
    1. $y_i := \overline{S_i}(x_i \oplus tk_{i-1})$, where $\overline{S_i}(x[1] \oplus tk_{i-1}[1] \| \ldots \| x[w] \oplus tk_{i-1}[w]) \stackrel{\text{def}}{=} S_i(x[1] \oplus tk_{i-1}[1]) \| \ldots \| S_i(x[w] \oplus tk_{i-1}[w])$.
    2. $x_{i+1} := T_i \cdot y_i$.
- $x_{r+1} := \overline{S_r}(x_r \oplus tk_{r-1}) \oplus tk_r$.
- The output is x_{r+1}.

Note that this model matches the structure of popular SPN ciphers such as the AES, Serpent, the ISO/IEC lightweight standard PRESENT, and the popular tweakable blockciphers Skinny. Also note that our model follows [?, Sect. 4.2] and uses different S-boxes in different rounds. We remark that some other [?, Sect. 3] assumed the same S-box in every round. Finally, we refer to [?, Sect. 2.1] for a more general model of SPNs and its connection to the above model.

We will mostly be interested in the case where we say that the construction has linear tweak and key mixing.

Multi-user Security Definitions. Let $\mathsf{SP}^T[\mathcal{S}]$ be an r-round SPN based on a set of S-boxes $\mathcal{S} = (S_1, \ldots, S_r)$ and an invertible linear permutation T with key space $\mathcal{K}$ and tweak space $\mathcal{T}$. So $\mathsf{SP}^T[\mathcal{S}]$ becomes a keyed tweakable permutation on $\{0,1\}^{wn}$ with key space $\mathcal{K}^{r+1}$ and tweak space $\mathcal{T}$.

In the multi-user setting, let ℓ denote the number of users. In the real world, ℓ secret keys $\mathbf{k}_1, \ldots, \mathbf{k}_\ell \in \mathcal{K}^{r+1}$ are chosen independently at random. A set of independent S-boxes $\mathcal{S} = (S_1, \ldots, S_r)$ is also randomly chosen from $\mathsf{Perm}(n)^r$. A distinguisher $\mathcal{D}$ is given oracle access to $(\mathsf{SP}^T_{\mathbf{k}_1}[\mathcal{S}], \ldots, \mathsf{SP}^T_{\mathbf{k}_\ell}[\mathcal{S}])$ as well as $\mathcal{S} = (S_1, \ldots, S_r)$. In the ideal world, $\mathcal{D}$ is given a set of independent random tweakable permutations $\widetilde{\mathcal{P}} = (\widetilde{P}_1, \ldots, \widetilde{P}_\ell) \in \widetilde{\mathrm{Perm}}(\mathcal{T}, wn)^\ell$ instead of $(\mathsf{SP}^T_{\mathbf{k}_1}[\mathcal{S}], \ldots, \mathsf{SP}^T_{\mathbf{k}_\ell}[\mathcal{S}])$. Oracle access to $\mathcal{S} = (S_1, \ldots, S_r)$ is still allowed in this world.

The adversarial goal is to tell apart the two worlds $(\mathsf{SP}^T_{\mathbf{k}_1}[\mathcal{S}], \ldots, \mathsf{SP}^T_{\mathbf{k}_\ell}[\mathcal{S}], \mathcal{S})$ and $(\widetilde{P}_1, \ldots, \widetilde{P}_\ell, \mathcal{S})$ by adaptively making forward and backward queries to each of the constructions and the S-boxes. Formally, $\mathcal{D}$'s distinguishing advantage is defined by

$$\begin{aligned}\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(\mathcal{D}) = \Pr&\left[\widetilde{P}_1, \ldots, \widetilde{P}_\ell \xleftarrow{\$} \widetilde{\mathsf{Perm}}(wn)^\ell, \mathcal{S} \xleftarrow{\$} \mathsf{Perm}(n)^r : 1 \leftarrow \mathcal{D}^{\mathcal{S}, \widetilde{P}_1, \ldots, \widetilde{P}_\ell}\right] \\ &- \Pr\left[\mathbf{k}_1, \ldots, \mathbf{k}_\ell \xleftarrow{\$} \mathcal{K}^\ell, \mathcal{S} \xleftarrow{\$} \mathrm{Perm}(n)^r : 1 \leftarrow \mathcal{D}^{\mathcal{S}, \mathsf{SP}^T_{k_1}[\mathcal{S}], \ldots, \mathsf{SP}^T_{k_\ell}[\mathcal{S}]}\right].\end{aligned}$$

For $p, q > 0$, we define

$$\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(p, q) = \max_{\mathcal{D}} \mathrm{Adv}_{\mathsf{SP}^T}(\mathcal{D})$$

where the maximum is taken over all adversaries $\mathcal{D}$ making at most p queries to each of the S-boxes and at most q queries to the outer tweakable permutations. In the single-user setting with $l = 1$. $\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(\mathcal{D})$ and $\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(p, q)$ will also be written as $\mathrm{Adv}^{\mathrm{su}}_{\mathsf{SP}^T}(\mathcal{D})$ and $\mathrm{Adv}^{\mathrm{su}}_{\mathsf{SP}^T}(p, q)$, respectively.

Note that, if we set $\mathcal{T}$ to a singleton set, then the classical definition of strong pseudorandom permutations is recovered. This will be the target of Sect. 3.

The H-coefficient Technique. Suppose that a distinguisher $\mathcal{D}$ makes p queries to each of the S-boxes, and total q queries to the construction oracles. The queries made to the j-th construction oracle, denoted C_j, are recorded in a query history

$$\mathcal{Q}_{C_j} = (j, t_{j,i}, x_{j,i}, y_{j,i})_{1 \le i \le q_j}$$

for $j = 1, ..., \ell$, where q is the number of queries made to C_j and $(j, t_{j,i}, x_{j,i}, y_{j,i})$ represents the evaluation obtained by the ith query to C_j. So according to the instantiation, it implies either $\mathsf{SP}^T_{\mathbf{k}_j}[\mathcal{S}](t_{j,i}, x_{j,i}) = y_{j,i}$ or $\widetilde{P}_j(t_{j,i}, x_{j,i}) = y_{j,i}$. Let

$$\mathcal{Q}_C = \mathcal{Q}_{C_1} \cup \ldots \cup \mathcal{Q}_{C_\ell}.$$

For $j = 1, \ldots, r$, the queries made to S_j are recorded in a query history

$$\mathcal{Q}_{S_j} = (j, u_{j,i}, v_{j,i})_{1 \leq i \leq p}$$

where $(j, u_{j,i}, v_{j,i})$ represents the evaluation $S_j(u_{j,i}) = v_{j,i}$ obtained by the ith query to S_j. Let

$$\mathcal{Q}_S = \mathcal{Q}_{S_1} \cup \ldots \cup \mathcal{Q}_{S_r}$$

Then the pair of query histories

$$\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$$

will be called the transcript of the attack: it contains all the information that $\mathcal{D}$ has obtained at the end of the attack. In this work, we will only consider information theoretic distinguishers. Therefore we can assume that a distinguisher is deterministic without making any redundant query, and hence the output of $\mathcal{D}$ can be regarded as a function of τ, denoted $\mathcal{D}(\tau)$ or $\mathcal{D}(\mathcal{Q}_C, \mathcal{Q}_S)$.

Fix a transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, a key $\mathbf{k} \in \mathcal{K}^{r+1}$, a tweakable permutation $\widetilde{P} \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)$, a set of S-boxes $\mathcal{S} = (S_1, \ldots, S_r) \in \mathsf{Perm}(n)^r$ and $j \in \{1, \ldots, \ell\}$: if $S_j(u_{j,i}) = v_{j,i}$ for every $i = 1, ..., p$, then we will write $S_j \vdash \mathcal{Q}_{S_j}$. We will write $\mathcal{S} \vdash \mathcal{Q}_S$ if $S_j \vdash \mathcal{Q}_{S_j}$ for every $j = 1, ..., r$. Similarly, if $\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}](t_{j,i}, x_{j,i}) = y_{j,i}$ (resp. $\widetilde{P}(t_{j,i}, x_{j,i}) = y_{j,i}$) for every $i = 1, ..., q_j$, then we will write $\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_{C_j}$ (resp. $\widetilde{P} \vdash \mathcal{Q}_{C_j}$).

Let $\mathbf{k}_1, \ldots, \mathbf{k}_\ell \in \mathcal{K}^{\ell+1}$ and $\widetilde{\mathcal{P}} = (\widetilde{P}_1, \ldots, \widetilde{P}_\ell) \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)^\ell$, if $\mathsf{SP}^T_{\mathbf{k}_j}[\mathcal{S}] \vdash \mathcal{Q}_{C_j}$ (resp. $\widetilde{P}_j \vdash \mathcal{Q}_{C_j}$) for every $j = 1, \ldots, \ell$, then we will write $(\mathsf{SP}^T_{\mathbf{k}_j}[\mathcal{S}])_{j=1,\ldots,\ell} \vdash \mathcal{Q}_C$ (resp. $\widetilde{P} \vdash \mathcal{Q}_C$).

If there exist $\widetilde{\mathcal{P}} \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)^\ell$ and $\mathcal{S} \in \mathsf{Perm}(n)^r$ that outputs τ at the end of the interaction with $\mathcal{D}$, then we will call the transcript τ attainable. So for any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, there exist $\widetilde{\mathcal{P}} \in \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)^\ell$ and $\mathcal{S} \in \mathsf{Perm}(n)^r$ such that $\widetilde{\mathcal{P}} \vdash \mathcal{Q}_C$ and $\mathcal{S} \vdash \mathcal{Q}_S$. For an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, let

$$\mathsf{p}_1(\tau) = \Pr\left[\widetilde{\mathcal{P}} \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{T}, wn)^\ell, \mathcal{S} \xleftarrow{\$} \mathsf{Perm}(n)^r : \widetilde{\mathcal{P}} \vdash \mathcal{Q}_C \bigwedge \mathcal{S} \vdash \mathcal{Q}_S\right],$$

$$\mathsf{p}_2(\tau) = \Pr\left[\mathbf{k}_1, \ldots, \mathbf{k}_\ell \xleftarrow{\$} \mathcal{K}^\ell, \mathcal{S} \xleftarrow{\$} \mathsf{Perm}(n)^r : (\mathsf{SP}^T_{\mathbf{k}_j}[\mathcal{S}])_j \vdash \mathcal{Q}_C \bigwedge \mathcal{S} \vdash \mathcal{Q}_S\right].$$

With these definitions, the core lemma of the H-coefficients technique (without defining "bad" transcripts) is stated as follows.

Lemma 1. *Let $\varepsilon \geq 0$. Suppose that for any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$,*

$$\mathsf{p}_2(\tau) \geq (1 - \varepsilon)\mathsf{p}_1(\tau). \tag{1}$$

Then one has

$$\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(\mathcal{D}) \leq \varepsilon.$$

The lower bound (1) is called *ϵ-point-wise proximity* of the transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$. The point-wise proximity of a transcript in the multi-user setting is guaranteed by the point-wise proximity of $(\mathcal{Q}_{C_j}, \mathcal{Q}_S)$ for each $j = 1, \ldots, \ell$ in the single user setting. The following lemma is a restatement of Lemma 3 in [**?**].

Lemma 2. *Let $\varepsilon : \mathbb{N} \times \mathbb{N} \to \mathbb{R}^{\geq 0}$ be a function such that*

1. *$\varepsilon(x, y) + \varepsilon(x, z) \leq \varepsilon(x, y + z)$ for every $x, y, z \in \mathbb{N}$,*
2. *$\varepsilon(\cdot, z)$ and $\varepsilon(z, \cdot)$ are non-decreasing functions on $\mathbb{N}$ for every $z \in \mathbb{N}$.*

Suppose that for any distinguisher $\mathcal{D}$ in the single-user setting that makes p primitive queries to each of the underlying S-boxes and makes q construction queries, and for any attainable transcript τ obtained by $\mathcal{D}$, one has

$$\mathsf{p}_2\left(\tau\right) \geq (1 - \varepsilon(p, q))\mathsf{p}_1\left(\tau\right).$$

Then for any distinguisher $\mathcal{D}$ in the multi-user setting that makes p primitive queries to each of the underlying S-boxes and makes total q construction queries, and for any attainable transcript τ obtained by $\mathcal{D}$, one has

$$\mathsf{p}_2\left(\tau\right) \geq (1 - \varepsilon(p + wq, q))\mathsf{p}_1\left(\tau\right).$$

3 SPRP Security of 4-Round SPNs

In this section, we prove beyond-birthday-bound SPRP security for 4-round linear SPNs. Concretely, let $\mathsf{SP}_{\mathbf{k}}[\mathcal{S}]$ be the 4-round SPN using any linear transformations T. I.e.,

$$\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}](x) := k_4 \oplus \overline{S_4}(k_3 \oplus T(\overline{S_3}(k_2 \oplus T(\overline{S_2}(k_1 \oplus T(\overline{S_1}(k_0 \oplus x))))))). \tag{2}$$

We show that SP^T is an SPRP as long as: (i) the linear layer T contains no zero entries, and (ii) the round keys k_0, k_1, k_2, k_3, k_4 are uniform and independent.

Theorem 1. *Assume $w \geq 2$, and $p + wq \leq N/2$. Let $\mathsf{SP}_{\mathbf{k}}[\mathcal{S}]$ be a 4-round, linear SPN as defined by Eq. (2). If round keys $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4)$ are uniform and independent, and T contains no zero entries, then*

$$\begin{aligned}
\mathrm{Adv}^{\mathrm{su}}_{\mathsf{SP}^T}(p, q) \leq& \frac{q^2}{2^{nw}} + \frac{8w^2q(p + wq)^2 + w^2q}{2^n}.\\
\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(p, q) \leq& \frac{q^2}{2^{nw}} + \frac{8w^2q(p + wq)^2 + w^2q}{2^n}\\
&+ \frac{16w^2q(p + wq)(p + wq + 3q) + 4w^2q(p + 3wq)^2}{2^{2n}}.
\end{aligned}$$

The proof of Theorem 1 relies on the following lemma and on Lemmas 1 and 2.

Lemma 3. *Assume $p + wq \leq N/2$. Let $\mathcal{D}$ be a distinguisher in the single-user setting that makes p primitive queries to each of S_1, S_2, S_3, and S_4, and makes q construction queries. Then for any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, one has*

$$\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq 1 - xxx. \tag{3}$$

3.1 Outline of the Proof

Throughout the proof, we fix a distinguisher $\mathcal{D}$ as described in the statement and fix an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$ obtained $\mathcal{D}$. Let

$$\begin{aligned}
\mathcal{Q}_{S_1}^{(0)} &= \{(u,v) \in \{0,1\}^n \times \{0,1\}^n : (1,u,v) \in \mathcal{Q}_S\}\,,\\
\mathcal{Q}_{S_2}^{(0)} &= \{(u,v) \in \{0,1\}^n \times \{0,1\}^n : (2,u,v) \in \mathcal{Q}_S\}\,,\\
\mathcal{Q}_{S_3}^{(0)} &= \{(u,v) \in \{0,1\}^n \times \{0,1\}^n : (3,u,v) \in \mathcal{Q}_S\}\,,\\
\mathcal{Q}_{S_4}^{(0)} &= \{(u,v) \in \{0,1\}^n \times \{0,1\}^n : (4,u,v) \in \mathcal{Q}_S\}
\end{aligned}$$

and denote the domains and ranges of $\mathcal{Q}_{S_1}^{(0)}, \mathcal{Q}_{S_2}^{(0)}, \mathcal{Q}_{S_3}^{(0)}, \mathcal{Q}_{S_4}^{(0)}$ by

$$\begin{aligned}
U_1^{(0)} &= \left\{u_1 \in \{0,1\}^n : (1,u_1,v_1) \in \mathcal{Q}_{S_1}^{(0)}\right\}, \quad V_1^{(0)} = \left\{v_1 \in \{0,1\}^n : (1,u_1,v_1) \in \mathcal{Q}_{S_1}^{(0)}\right\},\\
U_2^{(0)} &= \left\{u_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}_{S_2}^{(0)}\right\}, \quad V_2^{(0)} = \left\{v_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}_{S_2}^{(0)}\right\},\\
U_3^{(0)} &= \left\{u_3 \in \{0,1\}^n : (3,u_3,v_3) \in \mathcal{Q}_{S_3}^{(0)}\right\}, \quad V_3^{(0)} = \left\{v_3 \in \{0,1\}^n : (3,u_3,v_3) \in \mathcal{Q}_{S_3}^{(0)}\right\},\\
U_4^{(0)} &= \left\{u_4 \in \{0,1\}^n : (4,u_4,v_4) \in \mathcal{Q}_{S_4}^{(0)}\right\}, \quad V_4^{(0)} = \left\{v_4 \in \{0,1\}^n : (4,u_4,v_4) \in \mathcal{Q}_{S_4}^{(0)}\right\},
\end{aligned}$$

Point-wise proximity is usually established by enhancing the transcripts with auxiliary random variables, defining a large enough set of "good" randomness, and then, for each choice of a good random variable, lower bounding the probability of observing this transcript. Such random variables typically include the keys, and are usually called good if the adversary cannot use the randomness to follow the path of computation of the encryption/decryption of a query up to a contradiction. To this end, we follow [**?**, Sect. 4.2] and define an extension of the transcript in order to gather enough information to allow simple definition of bad randomness. Then, instead of summing over the choice of the randomness, we will define an extension of the transcript, that will provide the necessary information, and then sum over every possible good extension. In detail, a transcript τ is extended in the following manner:

- At the end of the interaction between $\mathcal{D}$ and the real world $(\mathcal{S}, \mathsf{SP}_{\mathbf{k}}^{T}[\mathcal{S}])$, we append τ with the keys $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4)$ and the two random permutations S_1, S_4 in use;
- At the end of the interaction between $\mathcal{D}$ and the ideal world $(\mathcal{S}, \widetilde{P})$, we append τ with randomly sampled keys $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4)$ and the two random permutations S_1, S_4 in use.

Note that, in either case, it is equivalent to sampling two new random permutations S_1, S_4 such that $S_1 \vdash \mathcal{Q}_{S_1}$ and $S_4 \vdash \mathcal{Q}_{S_4}$ and appending them to τ. With the above, for any $(x,y) \in \mathcal{Q}_C$ we define

$$a = T\big(\overline{S_1}\,(x \oplus k_0)\big), \quad b = T^{-1}\big(\overline{S_4^{-1}}\,(y \oplus k_4)\big).$$

This extends the list $\mathcal{Q}_C$ into a list as follows:

$$\mathcal{Q}'_C = \big((x_1, a_1, b_1, y_1), \ldots, (x_q, a_q, b_q, y_q)\big).$$

With this new list, a colliding query is defined as a construction query $(x, y, a, b) \in \mathcal{Q}'_C$ as follows:

1. there exists an integer $i \in \{1, \ldots, w\}$ such that $(a \oplus k_1)[i] \in U_2^{(0)}$.
2. there exists an integer $i \in \{1, \ldots, w\}$ such that $\big(b \oplus T^{-1}(k_3)\big)[i] \in V_3^{(0)}$.
3. there exist a construction query $(a', b') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(a, b, i) \neq (a', b', j)$ and $(a \oplus k_1)[i] = (a' \oplus k_1)[j]$.
4. there exist a construction query $(a', b') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(a, b, i) \neq (a', b', j)$ and $i \in \{1, \ldots, w\}$ such that $\big(b \oplus T^{-1}(k_3)\big)[i] = \big(b' \oplus T^{-1}(k_3)\big)[j]$.

Now we further introduce a new set $\mathcal{Q}'_S$ of S-box evaluations to complete the transcript extension. In detail, for each colliding query $(x, a, b, y) \in \mathcal{Q}'_C$, we will add tuples $(2, (a \oplus k_1)[i], v')_{1 \leq i \leq w}$ (if (a, b) collides at the input of S_2) or $\big(3, u', (b \oplus T^{-1}(k_3))[i]\big)_{1 \leq i \leq w}$ (if (a, b) collides at the output of S_3) to $\mathcal{Q}'_S$ by lazy sampling $v' = S_2((a \oplus k_1)[i])$ or $u' = S_3^{-1}((b \oplus k_3)[i])$, as long as it has not been determined by any existing query in $\mathcal{Q}_S$.

An extended transcript of τ includes all the above additional information, i.e.,

$$\tau' = (\mathcal{Q}'_C, \mathcal{Q}_S, \mathcal{Q}'_S, S_1, S_4, \mathbf{k}).$$

For each collision between a construction query and a primitive query, or between two construction queries, the extended transcript will contain enough information to compute a complete round of the evaluation of the SPN. This will be useful to lower bound the probability to get the transcript τ in the real world.

Below in Sect. 3.2, we will show that the number of bad extended transcripts is small enough; then in Sect. 3.3, we show that the probability to obtain good extension in the real world is sufficiently close to that in the ideal world. These will complete the proof.

3.2 Bad Transcript Extensions and Probability

The first step is to define the set of bad extended transcripts. Consider an attainable extended transcript $\tau' = (\mathcal{Q}'_C, \mathcal{Q}_S, \mathcal{Q}'_S, S_1, S_4, \mathbf{k})$. Let

$$\mathcal{Q}_{S_2}^{(1)} = \{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (2, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_S\}$$
$$\mathcal{Q}_{S_3}^{(1)} = \{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (3, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_S\}.$$

In words, $\mathcal{Q}_{S_i}^{(1)}$ summarizes each constraint that is forced on S_i by $\mathcal{Q}_S$ and $\mathcal{Q}'_S$. Let

$$U_2^{(1)} = \left\{u_2 \in \{0,1\}^n : (2, u_2, v_2) \in \mathcal{Q}_{S_2}^{(1)}\right\}, \quad V_2^{(1)} = \left\{v_2 \in \{0,1\}^n : (2, u_2, v_2) \in \mathcal{Q}_{S_2}^{(1)}\right\},$$
$$U_3^{(1)} = \left\{u_3 \in \{0,1\}^n : (3, u_3, v_3) \in \mathcal{Q}_{S_3}^{(1)}\right\}, \quad V_3^{(1)} = \left\{v_3 \in \{0,1\}^n : (3, u_3, v_3) \in \mathcal{Q}_{S_3}^{(1)}\right\}.$$

be the domains and ranges of $\mathcal{Q}_{S_2}^{(1)}$ and $\mathcal{Q}_{S_3}^{(1)}$ respectively.

Definition 1. *We say an extended transcript τ' is bad if at least one of the following conditions is fulfilled. The conditions are classified into two categories depending on the relevant randomness. In detail, regarding k_0, k_1, k_3, k_4:*

- *(B-1) there exist (not necessarily distinct) $(x, a, b, y), (x', a', b', y'), (x'', a'', b'', y'') \in \mathcal{Q}'_C$ and three distinct indices $i, i', i'' \in \{1, \ldots, w\}$ such that:*
  - $(x \oplus k_0)[i] = (x' \oplus k_0)[i'] = (x'' \oplus k_0)[i'']$*, or*
  - $(a \oplus k_1)[i] = (a' \oplus k_1)[i'] = (a'' \oplus k_1)[i'']$*, or*
  - $(b \oplus T^{-1}(k_3))[i] = (b' \oplus T^{-1}(k_3))[i'] = (b'' \oplus T^{-1}(k_3))[i'']$*, or*
  - $(y \oplus k_4)[i] = (y' \oplus k_4)[i'] = (y'' \oplus k_4)[i'']$.
- *(B-2) there exist $(x, a, b, y) \in \mathcal{Q}'_C$ and distinct indices $i, i' \in \{1, \ldots, w\}$ such that:*
  - $(x \oplus k_0)[i] \in U_1^{(0)}$ *and* $(x \oplus k_0)[i'] \in U_1^{(0)}$*, or*
  - $(a \oplus k_1)[i] \in U_2^{(0)}$ *and* $(a \oplus k_1)[i'] \in U_2^{(0)}$*, or*
  - $\big(b \oplus T^{-1}(k_3)\big)[i] \in V_3^{(0)}$ *and* $\big(b' \oplus T^{-1}(k_3)\big)[i'] \in V_3^{(0)}$*, or*
  - $(y \oplus k_4)[i] \in V_4^{(0)}$ *and* $(y \oplus k_4)[i'] \in V_4^{(0)}$.
- *(B-3) there exist $(x, a, b, y) \in \mathcal{Q}'_C$ and $i, j \in \{1, \ldots, w\}$ such that:*
  - $(x \oplus k_0)[i] \in U_1^{(0)}$ *and* $(y \oplus k_4)[j] \in V_4^{(0)}$*, or*
  - $(x \oplus k_0)[i] \in U_1^{(0)}$ *and* $(a \oplus k_1)[j] \in U_2^{(1)}$*, or*
  - $(y \oplus k_4)[j] \in V_4^{(0)}$ *and* $\big(b \oplus T^{-1}(k_3)\big)[i] \in V_3^{(1)}$.

Regarding k_2, S_1, S_4, and $\mathcal{Q}'_S$:

- *(B-7) there exist $(x, a, b, y) \in \mathcal{Q}'_C$ and $i, j \in \{1, \ldots, w\}$ such that:*
  - $(a \oplus k_1)[i] \in U_2^{(1)}$ *and* $(b \oplus T^{-1}(k_3))[j] \in V_3^{(1)}$*, or*
  - $(a \oplus k_1)[i] \in U_2^{(1)}$ *and* $(T(\overline{S_2}(a \oplus k_1)) \oplus k_2)[j] \in U_3^{(1)}$*, or*
  - $(T^{-1}(\overline{S_3^{-1}}(b \oplus T^{-1}(k_3)) \oplus k_2))[i] \in V_2^{(1)}$ *and* $(b \oplus T^{-1}(k_3))[j] \in V_3^{(1)}$.
- *(B-8) there exist $(x, a, b, y), (x', a', b', y') \in \mathcal{Q}'_C$ and $i, i', j, j' \in \{1, \ldots, w\}$, $(a, b, j) \neq (a', b', j')$, such that $(a \oplus k_1)[i] \in U_2^{(1)}, (a' \oplus k_1)[i'] \in U_2^{(1)}$, and*

$$\big(T(\overline{S_2}(a \oplus k_1)) \oplus k_2\big)[j] = \big(T(\overline{S_2}(a' \oplus k_1)) \oplus k_2\big)[j'].$$

- *(B-9) there exist $(x, a, b, y), (x', a', b', y') \in \mathcal{Q}'_C$ and $i, i', j, j' \in \{1, \ldots, w\}$, $(a, b, j) \neq (a', b', j')$, such that $\big(b \oplus T^{-1}(k_3)\big)[i] \in V_3^{(1)}, \big(b' \oplus T^{-1}(k_3)\big)[i'] \in V_3^{(1)}$, and*

$$\big(T^{-1}(\overline{S_3^{-1}}(b \oplus T^{-1}(k_3)) \oplus k_2)\big)[j] = \big(T^{-1}(\overline{S_3^{-1}}(b' \oplus T^{-1}(k_3)) \oplus k_2)\big)[j'].$$

Any extended transcript that is not bad will be called good. Given an original transcript τ, we denote $\Theta_{\text{good}}(\tau)$ (resp. $\Theta_{\text{bad}}(\tau)$) the set of good (resp. bad) extended transcripts of τ and $\Theta'(\tau)$ the set of all extended transcripts of τ.

We will rely on the following lemma, which characterizes the properties of linear SPNs.

Lemma 4. *Define*

$$\mathsf{pcoll}_1^+(t,z,z',j,j') := \Pr\Big[\big(T\big(\overline{S_t}(z\oplus k_{t-1})\big)\oplus k_t\big)[j] = \big(T\big(\overline{S_t}(z'\oplus k_{t-1})\big)\oplus k_t\big)[j']$$
$$\Big|\ (z\oplus k)[i]\notin U_t^{(0)}\Big],$$
$$\mathsf{pcoll}_2^+(t,z,z',i,i',j,j') := \Pr_{S_t}\Big[\big(T\big(\overline{S_t}(z\oplus k_{t-1})\big)\oplus k_t\big)[j] = \big(T\big(\overline{S_t}(z'\oplus k_{t-1})\big)\oplus k_t\big)[j']$$
$$\Big|\ (z\oplus k)[i]\notin U_t^{(0)}\wedge (z\oplus k)[i]\notin U_t^{(0)}\Big],$$
$$\mathsf{pcoll}_1^-(t,z,z',j,j') := \Pr_{S_t}\Big[T\big(\overline{S_t^{-1}}(z\oplus k)\big)[j] = T\big(\overline{S_t^{-1}}(z'\oplus k)\big)[j']$$
$$\Big|\ (z\oplus k)[i]\notin V_t^{(0)}\Big],$$
$$\mathsf{pcoll}_2^-(t,z,z',i,i',j,j') := \Pr_{S_t}\Big[T\big(\overline{S_t^{-1}}(z\oplus k_{t-1})\big)[j] = T\big(\overline{S_t^{-1}}(z'\oplus k_{t-1})\big)[j']$$
$$\Big|\ (z\oplus k)[i]\notin V_t^{(0)}\wedge (z\oplus k)[i]\notin V_t^{(0)}\Big].$$

Then it holds

$$\Pr_{S_t}\Big[\big(T\big(\overline{S_t}(z\oplus k_{t-1})\big)\oplus k_t\big)[j]=\delta\ \Big|\ \forall\ell\in\{1,\ldots,w\}:(z\oplus k)[\ell]\notin U_t^{(0)}\Big]\le\frac{1}{N},$$
$$\Pr_{S_t}\Big[\big(T^{-1}\big(\overline{S_t}(z\oplus k_t)\big)\oplus k_{t-1}\big)[j]=\delta\ \Big|\ \forall\ell\in\{1,\ldots,w\}:(z\oplus k)[\ell]\notin V_t^{(0)}\Big]\le\frac{1}{N},$$
$$\mathsf{pcoll}_1^+(t,z,z',j)\le\frac{1}{N-p-wq},\qquad \mathsf{pcoll}_2^+(t,z',i,i',j)\le\frac{1}{N-p-wq},$$
$$\mathsf{pcoll}_1^-(t,z,z',j)\le\frac{1}{N-p-wq},\qquad \mathsf{pcoll}_2^-(t,z,z',i,i',j)\le\frac{1}{N-p-wq}.$$

Proof. First, since $k_t[j]$ is uniform and independent of k_{t-1} and S_t, it immediately holds

$$\Pr_{S_t}\Big[\big(T\big(\overline{S_t}(z\oplus k_{t-1})\big)\oplus k_t\big)[j]=\delta\ \Big|\ \forall\ell\in\{1,\ldots,w\}:(z\oplus k)[\ell]\notin U_t^{(0)}\Big]=\frac{1}{N}.$$

Similarly,

$$\Pr_{S_t}\Big[\big(T^{-1}\big(\overline{S_t}(z\oplus k_t)\big)\oplus k_{t-1}\big)[j]=\delta\ \Big|\ \forall\ell\in\{1,\ldots,w\}:(z\oplus k)[\ell]\notin V_t^{(0)}\Big]=\frac{1}{N}.$$

Then, consider $\mathsf{pcoll}_1^+(t,z,z',j,j')$. When $j\ne j'$, the probability to have $\big(T\big(\overline{S_t}(z\oplus k_{t-1})\big)\oplus k_t\big)[j]=\big(T\big(\overline{S_t}(z'\oplus k_{t-1})\big)\oplus k_t\big)[j']$ is $1/N\le 1/(N-p-wq)$, since $k_t[j]$ and $k_t[j']$ are uniform and independent. In the remaining we focus on the case of $j=j'$, which means $T\big(\overline{S_t}(z\oplus k_{t-1})\big)[j]=T\big(\overline{S_t}(z'\oplus k_{t-1})\big)[j]$. Note that $z\ne z'$ implies there exists i_0 such that $(z\oplus k_{t-1})[i_0]\ne(z'\oplus k_{t-1})[i_0]$. By the assumption, $(z\oplus k_{t-1})[i_0]\notin U_1^{(0)}$. By construction, we have

$$\begin{aligned}&T(\overline{S_t}(z\oplus k_{t-1}))[j]\oplus T(\overline{S_t}(z'\oplus k_{t-1}))[j]\\&=\Big(\bigoplus_{1\le\ell\le w}t_{j,\ell}\cdot S_t\big((z\oplus k_{t-1})[\ell]\big)\Big)\oplus\Big(\bigoplus_{1\le\ell\le w}t_{j,\ell}\cdot S_t\big((z'\oplus k_{t-1})[\ell]\big)\Big).\end{aligned}$$

Below we distinguish 3 cases:

Case 1: $\boldsymbol{(z \oplus k_{t-1})[i_0]}$ is "unique", i.e., $(z \oplus k_{t-1})[i_0] \neq (z' \oplus k_{t-1})[\ell]$ for all $\ell \in \{1, \ldots, w\}$, and $(z \oplus k_{t-1})[i_0] \neq (z \oplus k_{t-1})[\ell]$ for any $\ell \neq i_0$. Then, conditioned on $S_t \vdash \mathcal{Q}^{(0)}_{S_t}$ and on the $2w-1$ values $\{S_t((z \oplus k_{t-1})[\ell])\}_{1 \leq \ell \leq w, \ell \neq i_0} \cup \{S_t((z' \oplus k_{t-1})[\ell])\}_{1 \leq \ell \leq w}$, the value of $S_t\big((z \oplus k_{t-1})[i_0]\big)$ remains uniform in *at least* $N - p - wq$ possibilities. Moreover, the coefficient t_{j,i_0} is non-zero as per our assumption. Therefore, in this case we have

$$\Pr\big[T(\overline{S_t}(z \oplus k_{t-1}))[j] \oplus T(\overline{S_t}(z' \oplus k_{t-1}))[j] = 0\big] \leq \frac{1}{N - p - wq}. \tag{4}$$

Case 2: $\boldsymbol{(z \oplus k_{t-1})[i_0] = (z \oplus k_{t-1})[i_1]}$ for some $\boldsymbol{i_1 \neq i_0}$. Then by $\neg$(B-1), $(z \oplus k_{t-1})[i_0] \neq (z \oplus k_{t-1})[\ell]$ and $(z \oplus k_{t-1})[i_0] \neq (z' \oplus k_{t-1})[\ell]$ for any $\ell \neq i_0, i_1$. We further distinguish two subcases:

- Subcase 2.1: $(z \oplus k_{t-1})[i_1] = (z' \oplus k_{t-1})[i_1]$. Then, with the two terms $t_{j,i_1} \cdot S_t\big((z \oplus k_{t-1})[i_1]\big)$ and $t_{j,i_1} \cdot S_t\big((z' \oplus k_{t-1})[i_1]\big)$ canceled, it can be seen

  $$\begin{aligned}&T(\overline{S_t}(z \oplus k_{t-1}))[j] \oplus T(\overline{S_t}(z' \oplus k_{t-1}))[j]\\ =&\Big(\bigoplus_{1 \leq \ell \leq w, \ell \neq i_1} t_{j,\ell} \cdot S_t\big((z' \oplus k_{t-1})[\ell]\big)\Big) \oplus \Big(\bigoplus_{1 \leq \ell \leq w, \ell \neq i_1} t_{j,\ell} \cdot S_t\big((z' \oplus k_{t-1})[\ell]\big)\Big).\end{aligned}$$

  Conditioned on $S_t \vdash \mathcal{Q}^{(0)}_{S_t}$ and on the $2w-3$ values $\{S_t((z' \oplus k_{t-1})[\ell])\}_{1 \leq \ell \leq w, \ell \neq i_1} \cup \{S_t((z \oplus k_{t-1})[\ell])\}_{1 \leq \ell \leq w, \ell \neq i_0, \ell \neq i_1}$, the value of $S_t((z \oplus k_{t-1})[i_0])$ remains uniform in *at least* $N - p - wq$ possibilities. Therefore, in this case Eq. (4) still holds.
- Subcase 2.2: $(z \oplus k_{t-1})[i_1] \neq (z' \oplus k_{t-1})[i_1]$. Then we write

  $$\begin{aligned}&T(\overline{S_t}(z \oplus k_{t-1}))[j] \oplus T(\overline{S_t}(z \oplus k_{t-1}))[j]\\ =&\underbrace{\Big(t_{j,i_0} \cdot S_t\big((z \oplus k_{t-1})[i_0]\big) \oplus t_{j,i_1} \cdot S_t\big((z \oplus k_{t-1})[i_1]\big)\Big)}_{\big(t_{j,i_0} \oplus t_{j,i_1}\big) \cdot S_t\big((z \oplus k_{t-1})[i_0]\big)}\\ &\qquad \oplus \Big(\bigoplus_{1 \leq \ell \leq w} t_{j,\ell} \cdot S_t\big((z' \oplus k_{t-1})[\ell]\big)\Big) \oplus \Big(\bigoplus_{\ell \neq i_0, \ell \neq i_1} t_{j,\ell} \cdot S_t\big((z \oplus k_{t-1})[\ell]\big)\Big).\end{aligned}$$

  Conditioned on $S_t \vdash \mathcal{Q}^{(0)}_{S_t}$ and on the $2w-2$ values $\{S_t((z' \oplus k_{t-1})[\ell])\}_{1 \leq \ell \leq w} \cup \{S_t((x \oplus k_{t-1})[\ell])\}_{1 \leq \ell \leq w, \ell \neq i_0, \ell \neq i_1}$, $S_t((z \oplus k_{t-1})[i_0])$ remains uniform in at least $N - p - wq$ possibilities. Moreover, the coefficient $t_{j,i_0} \oplus t_{j,i_1}$ is non-zero as per our assumption. Therefore, Eq. (4) remains.

Case 3: $\boldsymbol{(z \oplus k_{t-1})[i_0] = (z' \oplus k_{t-1})[i_1]}$ for some $\boldsymbol{i_1 \neq i_0}$. the subcase and discussion are similar to Case 2.

By the above, in any case, the probability to have $T(\overline{S_t}(z \oplus k_{t-1}))[j] = T(\overline{S_t}(z \oplus k_{t-1}))[j]$ is at most $1/(N-p-wq)$, which establishes $\mathsf{pcoll}^+_1(t, z, z', j) \leq 1/(N - p - wq)$. Similarly by symmetry, $\mathsf{pcoll}^-_1(t, z, z', j) \leq 1/(N - p - wq)$.

The analysis of $\mathsf{pcoll}_2^+(t, z', i, i', j, j')$ bears some resemblance. In particular, we focus on the case of $j = j'$, as otherwise the uniformness of $k_t[j]$ and $k_t[j']$ is sufficient for $\mathsf{pcoll}_2^+(t, z', i, i', j, j') = 1/N$.

First, consider $\mathsf{pcoll}_2^+(t, z', i, i', j, j')$ with $i \neq i'$. Since $z \neq z'$, there exists i_0 such that $(z \oplus k_{t-1})[i_0] \neq (z' \oplus k_{t-1})[i_0]$. Then either $i \neq i_0$ or $i' \neq i_0$. Wlog assume $i \neq i_0$. Note that this means $(z \oplus k_{t-1})[i] \neq (z' \oplus k_{t-1})[i_0]$, as otherwise both $(z \oplus k_{t-1})[i]$ and $(z \oplus k_{t-1})[i_0]$ fall in $U_1^{(0)}$ and it contradicts ¬(B-2). We then distinguish three cases as the analysis of $\mathsf{pcoll}_1^+(t, z, z', j)$. In detail,

- Case 1: $(z \oplus k_{t-1})[i_0] \neq (z' \oplus k_{t-1})[\ell]$ for all $\ell \in \{1, \ldots, w\}$, and $(z \oplus k_{t-1})[i_0] \neq (z \oplus k_{t-1})[\ell]$ for any $\ell \neq i_0$. Then the analysis is similar to Case 1 in the analysis of $\mathsf{pcoll}_1^+(t, z, z', j)$.
- Case 2: $(z \oplus k_{t-1})[i_0] = (z \oplus k_{t-1})[i_1]$ for some $i_1 \neq i_0$. Then, if $(z \oplus k_{t-1})[i_1] = (z' \oplus k_{t-1})[i_1]$, then the two terms $t_{j,i_1} \cdot S_t\big((z \oplus k_{t-1})[i_1]\big)$ and $t_{j,i_1} \cdot S_t\big((z' \oplus k_{t-1})[i_1]\big)$ cancel, and the remaining term $t_{j,i_0} \cdot S_t\big((z \oplus k_{t-1})[i_0]\big)$ ensures that the probability is at most $1/(N - p - wq)$; otherwise, the term $(t_{j,i_0} \oplus t_{j,i_1}) \cdot S_t((z \oplus k_{t-1})[i_0])$ ensures that the probability is at most $1/(N - p - wq)$.
- Case 3: $(z \oplus k_{t-1})[i_0] = (z' \oplus k_{t-1})[i_1]$ for some $i_1 \neq i_0$. This subcase is similar to Case 2.

In all, the uniformness of $S_t((z \oplus k_{t-1})[i_0])$ is sufficient to ensure $\Pr\big[T(\overline{S_t}(z \oplus k_{t-1}))[j] = T(\overline{S_t}(z \oplus k_{t-1}))[j]\big] \leq 1/(N - p - wq)$.

Then, consider the case of $i = i'$, i.e., $\mathsf{pcoll}_2^+(t, z, z', i, i, j, j)$. Assume that $S_t((z \oplus k_{t-1})[i]) = u_t$ and $S_t((z' \oplus k_{t-1})[i]) = u'_t$ for $(u_t, v_t), (u'_t, v'_t) \in \mathcal{Q}_{S_t}^{(0)}$. Then it holds

$$
\begin{aligned}
&T(\overline{S_t}(z \oplus k_{t-1}))[j] \oplus T(\overline{S_t}(z \oplus k_{t-1}))[j] \\
=&(t_{j,i} \cdot v_1) \oplus (t_{j,i} \cdot v'_1) \oplus \Big(\bigoplus_{1 \leq \ell \leq w, \ell \neq i} t_{j,\ell} \cdot \big(S_1((x \oplus k_0)[\ell]) \oplus S_1((x' \oplus k_0)[\ell])\big)\Big). \qquad (5)
\end{aligned}
$$

Now:

- If $x[\ell] = x'[\ell]$ for any $\ell \neq i$, then $z \neq z'$ implies $v_1 \neq v'_1$. In this case, Eq. (5) collapses to $t_{j,i} \cdot v_1 = t_{j,i} \cdot v'_1$ which is not possible since $t_{j,i} \neq 0$;
- Else, there exists $i_0 \neq i$ such that $(z \oplus k_{t-1})[i_0] \neq (z' \oplus k_{t-1})[i_0]$. This means $(z' \oplus k_{t-1})[i] \notin U_t^{(0)}$ (and thus $(z' \oplus k_{t-1})[i] \neq (z \oplus k_{t-1})[i_0]$) by ¬(B-2). The remaining analysis just follows the previous one for $\mathsf{pcoll}_1^+(t, z, z', j)$, establishing that the uniformness of $S_t((z \oplus k_{t-1})[i_0])$ is sufficient to ensure that $T(\overline{S_t}(z \oplus k_{t-1}))[j]$ equals $T(\overline{S_t}(z \oplus k_{t-1}))[j]$ with probability at most $1/(N - p - wq)$.

Therefore, it still holds $\mathsf{pcoll}_2^+(t, z, z', i, i, j, j) \leq 1/(N - p - wq)$. All the above cases show that $\mathsf{pcoll}_2^+(t, z, z', i, i', j, j') \leq 1/(N - p - wq)$ for any parameters. Similarly by symmetry, $\mathsf{pcoll}_2^-(t, z, z', i, i', j, j') \leq 1/(N - p - wq)$. □

We start by upper bounding the probability of getting bad transcripts in the ideal world.

Lemma 5. *Assuming $p + wq \le N/2$, then it holds*

$$\Pr\big[\tau' \in \mathit{\Theta}_{\mathrm{bad}}(\tau)\big] \le \frac{3w^2q\,(p+wq)^2}{N^2} + \frac{w^2q}{N} + \frac{9w^2q(p+wq)^2}{N^2} + \frac{16w^3q^2p}{N^2}. \tag{6}$$

Proof. We upper bound the probabilities of the conditions in turn.

(B-1). Consider each of the $\binom{w}{3} \cdot q^3 \le w^3q^3/6$ choices of $(x,a,b,y), (x',a',b',y'), (x'',a'',b'',y'') \in \mathcal{Q}'_C$ and distinct $i, i', i'' \in \{1,\ldots,w\}$. Since $k_0[i]$, $k_0[i']$, and $k_0[i'']$ are uniform and independent, the probability to have $(x \oplus k_0)[i] = (x' \oplus k_0)[i'] = (x'' \oplus k_0)[i'']$ is $1/N^2$. Similarly, the probability to have $(a \oplus k_1)[i] = (a' \oplus k_1)[i'] = (a'' \oplus k_1)[i'']$, *or* $(b \oplus k_3)[i] = (b' \oplus k_3)[i'] = (b'' \oplus k_3)[i'']$, *or* $(y \oplus k_4)[i] = (y' \oplus k_4)[i'] = (y'' \oplus k_4)[i'']$, is $3/N^2$. Thus

$$\Pr\left[\text{(B-1)}\right] \le \frac{4w^3q^3}{6N^2} \le \frac{w^3q^3}{N^2}.$$

(B-2). For each of the $q\binom{w}{2} \le w^2q/2$ choices of $(x,a,b,y) \in \mathcal{Q}'_C$ and distinct $i, i' \in \{1,\ldots,w\}$, since $k_0[i]$ and $k_0[i']$ are uniform and independent, the probability to have $(x \oplus k_0)[i] \in U_1^{(0)}$ and $(x \oplus k_0)[i'] \in U_1^{(0)}$ is at most p^2/N^2. The same bound holds for the other three conditions. Thus

$$\Pr\left[\text{(B-2)}\right] \le \frac{w^2q}{2} \cdot \frac{4p^2}{N^2} \le \frac{2w^2qp^2}{N^2}.$$

(B-3). For each of the w^2q choices of $(x,a,b,y) \in \mathcal{Q}'_C$ and indices $i, j \in \{1,\ldots,w\}$, since k_0 and k_4 are uniform and independent, the probability to have $(x \oplus k_0)[i] \in U_1^{(0)}$ and $(y \oplus k_4)[j] \in V_4^{(0)}$ is p^2/N^2. Thus

$$\Pr\left[\text{(B-3)}\right] \le \frac{w^2qp^2}{N^2}.$$

(B-4) and (B-5). Note that (B-4) consists of four subevents:

- (B-41) there exists $(x,a,b,y) \in \mathcal{Q}'_C$ and indices $i, j \in \{1,\ldots,w\}$ such that $(x \oplus k_0)\,[i] \in U_1^{(0)}$ and $(a \oplus k_1)\,[j] \in U_2^{(0)}$;
- (B-42) there exists $(x,a,b,y), (x',a',b',y') \in \mathcal{Q}'_C$, and $i, j, j' \in \{1,\ldots,w\}$ such that $(x,j) \ne (x',j')$, $(x' \oplus k_0)[i'] \notin U_1^{(0)}$ for all $i' \in \{1,\ldots,w\}$, while $(x \oplus k_0)\,[i] \in U_1^{(0)}$ and $(a \oplus k_1)[j] = (a' \oplus k_1)[j']$.
- (B-43) there exists $(x,a,b,y), (x',a',b',y') \in \mathcal{Q}'_C$, and $i, i', j, j' \in \{1,\ldots,w\}$ such that $(x,j) \ne (x',j')$, while $(x \oplus k_0)\,[i] \in U_1^{(0)}$, $(x' \oplus k_0)\,[i'] \in U_1^{(0)}$, and $(a \oplus k_1)[j] = (a' \oplus k_1)[j']$.

Since k_0 and k_1 are uniform and independent, it holds $\Pr\big[(x \oplus k_0)[i] \in U_1^{(0)} \wedge (a \oplus k_1)[j] \in U_2^{(0)}\big] = p^2/N^2$. Thus $\Pr[\text{(B-41)}] \le w^2qp^2/N^2$.

For (B-42), we have $\mathsf{pcoll}_1^{+}(1, x, x', j, j') \le 1/(N - p - wq)$ by Lemma 4. Thus

$$\begin{aligned}\Pr[\text{(B-42)}] \le & \sum_{(x,a,b,y),(x',a',b',y'),j,j'} \mathsf{pcoll}_1^{+}(1, x, x', j, j') \times \Pr[(x \oplus k_0)\,[i] \in U_1^{(0)}] \\ \le & \binom{wq}{2} \cdot \frac{1}{N-p-wq} \cdot \frac{w}{N} \le \frac{w^3q^2p}{2N(N-p-wq)}.\end{aligned}$$

For (B-43), we have

$$\begin{aligned}\Pr[\text{(B-43)}] = \sum_{(x,a,b,y),(x',a',b',y')} \sum_{i,i',j,j'} \Big(& \underbrace{\Pr[(x \oplus k_0)[i] \in U_1^{(0)}]}_{\le p/N} \\ & \times \underbrace{\Pr[(x' \oplus k_0)[i'] \in U_1^{(0)} | (x \oplus k_0)[i] \in U_1^{(0)}]}_{\le 1} \times \underbrace{\mathsf{pcoll}_2^+(1, x, x', i, i', j, j')}_{\le 1/(N-p-wq)} \Big) \\ \le & \binom{wq}{2} \cdot w^2 \cdot \frac{p}{N} \cdot \frac{1}{N-p-wq} \le \frac{w^4pq^2}{2N(N-p-wq)}.\end{aligned}$$

Summing over the above and using $p + wq \le N/2$, we reach

$$\Pr\big[\text{(B-3)} \mid \neg\text{(B-1)}\big] \le \frac{w^2qp^2}{N^2} + \frac{w^4pq^2}{2N(N-p-wq)} + \frac{w^4pq^2}{2N(N-p-wq)} \le \frac{w^2qp^2}{N^2} + \frac{2w^4pq^2}{N^2}.$$

Similarly, $\Pr\big[\text{(B-4)} \mid \neg\text{(B-1)}\big] \le \frac{w^2qp^2 + 2w^4pq^2}{N^2}$ by symmetry.

(B-6). **For any construction query $(x, a, b, y) \in \mathcal{Q}'_C$, to have $(a \oplus k_1)[i] \in U_2^{(1)}$, it has to be $(x \oplus k_0)[i_0] \notin U_1^{(0)}$ for any $i_0 \in \{1, \ldots, w\}$, as otherwise it contradicts $\neg$(B-4).**

For any $(x, a, b, y) \in \mathcal{Q}'_C$ and any i, j, it holds

$$\begin{aligned}\Pr\big[(a \oplus k_1)[j] \in U_2^{(1)}\big] \le & \sum_{u_2 \in U_2^{(0)}} \underbrace{\Pr\big[\big(T(\overline{S_1}(x \oplus k_0)) \oplus k_1\big)[i] = u_2\big]}_{=1/N \text{ (Lemma 4)}} \\ & + \sum_{(x',a',b',y') \in \mathcal{Q}'_C} \sum_{i',i} \underbrace{\Pr\big[(a \oplus k_1)[i] = (a' \oplus k_1)[i']\big]}_{\le 1/(N-p-wq) \text{ (Lemma 4)}} \\ \le & \frac{p}{N} + \frac{w^2q}{N-p-wq} \le \frac{p + 2w^2q}{N}.\end{aligned}$$

Similarly, $\Pr\big[(b \oplus T^{-1}(k_3))[j] \in V_3^{(1)}\big] \le (p + 2w^2q)/N$. Since we have at most w^2q choices for (x, a, b, y) and $i, j \in \{1, \ldots, w\}$, we have

$$\Pr\big[\text{(B-6)} \mid \neg\text{(B-3)} \wedge \neg\text{(B-4)}\big] \le w^2q \cdot \Big(\frac{2(p+wq)}{N}\Big)^2 \le \frac{4w^2q(p+wq)^2}{N}.$$

(B-7). Following the analysis of (B-6), for any $(x, a, b, y) \in \mathcal{Q}'_C$ and i, the probability to have $(a \oplus k_1)[i] \in U_2^{(1)}$ is at most $2(p+wq)/N$. On the other hand, since k_2 is uniform and independent from the queries and from k_0, k_1, the probability to have $(T(\overline{S_2}(a \oplus k_1)) \oplus k_2)[j] \in U_3^{(1)}$ is $(p + wq)/N$. Similarly by symmetry, the probability to have both $(T^{-1}(\overline{S_3^{-1}}(b \oplus T^{-1}(k_3)) \oplus k_2))[i] \in V_2^{(1)}$ and $(b \oplus T^{-1}(k_3))[j] \in V_3^{(1)}$ is at most $2(p + wq)^2/N^2$. Since we have at most w^2q choices for (x, a, b, y) and $i, j \in \{1, \ldots, w\}$, we have

$$\Pr\big[\text{(B-7)} \mid \neg\text{(B-3)}\big] \le \frac{4w^2q(p+wq)^2}{N^2}.$$

(B-8) AND (B-9). Consider (B-8) first.

$$\begin{aligned}\Pr[\text{(B-8)}] = &\sum_{(x,a,b,y),(x',a',b',y')\in\mathcal{Q}'_C}\ \sum_{i,i',j,j'} \Bigg(\underbrace{\Pr\big[(a\oplus k_1)[i]\in U_2^{(1)}\big]}_{\leq (p+wq)/(N-p-wq)} \\ &\times \underbrace{\Pr\big[(a'\oplus k_1)[i]\in U_2^{(1)} | (a\oplus k_1)[i]\in U_2^{(1)}\big]}_{\leq 1} \times \underbrace{\mathsf{pcoll}_2^{+}(2,a,a',i,i',j,j')}_{\leq 1/(N-p-wq)} \Bigg) \\ \leq &\binom{wq}{2}\cdot w^2\cdot\frac{p+wq}{N-p-wq}\cdot\frac{1}{N-p-wq}\leq\frac{w^4q^2(p+wq)}{2(N-p-wq)^2}.\end{aligned}$$

Similarly by symmetry,

$$\Pr[\text{(B-9)}]\leq\frac{w^4q^2(p+wq)}{2(N-p-wq)^2}.$$

Summing over the above yields

$$\begin{aligned}&\Pr\left[\tau'\in\Theta_{\text{good}}\left(\tau\right)\right]\leq\sum_{i=1}^{9}\Pr[\text{(B-}i\text{)}] \\ \leq&\frac{w^2q(p+wq)^2}{(N-p-wq)^2}+\frac{2w^2q(p+wq)^2}{N(N-p-wq)}+\frac{w^2qp^2}{N^2}+\frac{8w^3q^2p}{N(N-p-wq)} \\ \leq&\frac{9w^2q(p+wq)^2}{N^2}+\frac{16w^3q^2p}{N^2}.\end{aligned}$$

as claimed. □

3.3 Analyzing Good Transcript Extensions

We are now ready for the second step of the reasoning. Define

$$\mathcal{C}_{\mathbf{k}}^{T}[\mathcal{S}](a) := \overline{S_3}(T(\overline{S_2}(a\oplus k_1))\oplus k_2)\oplus T^{-1}(k_3).$$

For any attainable transcript τ, the ideal world probability is easy to calculate:

$$\begin{aligned}\mathsf{p}_1(\tau) =&\Pr\left[(\widetilde{P},\mathcal{S})\xleftarrow{\$}\widetilde{\mathsf{Perm}}(\mathcal{T},wn)\times\mathsf{Perm}(n)^4 : (\mathcal{S}\vdash\mathcal{Q}_S)\wedge(\widetilde{P}\vdash\mathcal{Q}_C)\right] \\ =&\frac{1}{(N^w)_q}\cdot\left(\frac{1}{(N)_p}\right)^4.\end{aligned}$$

To reach the real world probability $\mathsf{p}_2(\tau)$, for any transcript extension $\tau'=(\mathcal{Q}'_C,\mathcal{Q}_S,\mathcal{Q}'_S,S_1^*,S_4^*,\mathbf{k})$ from τ, denote

$$\begin{aligned}\mathsf{p}_{\text{re}}(\tau') =&\Pr\Big[\big(\mathbf{k}',\mathcal{S}\big)\xleftarrow{\$}\big(\{0,1\}^{wn}\big)^5\times\mathsf{Perm}(n)^4 : \Big(\big(S_1=S_1^*\big)\wedge\big(S_4=S_4^*\big)\wedge \\ &\big(S_2\vdash\mathcal{Q}_{S_2}^{(1)}\big)\wedge\big(S_3\vdash\mathcal{Q}_{S_3}^{(1)}\big)\wedge\big(\mathcal{C}_{\mathbf{k}'}^{T}[\mathcal{S}]\vdash\mathcal{Q}'_C\big)\wedge\big(\mathbf{k}'=\mathbf{k}\big)\Big)\Big] \\ \mathsf{p}_{\text{mid}}(\tau') =&\Pr\Big[\mathcal{S}\xleftarrow{\$}\mathsf{Perm}(n)^4 : (\mathcal{C}_{\mathbf{k}}^{T}[\mathcal{S}]\vdash\mathcal{Q}'_C)\ \Big|\ (S_1=S_1^*)\wedge(S_4=S_4^*)\wedge \\ &(S_2\vdash\mathcal{Q}_{S_2}^{(1)})\wedge(S_3\vdash\mathcal{Q}_{S_3}^{(1)})\Big].\end{aligned}$$

and let $\alpha_1 = |\mathcal{Q}_{S_2}^{(1)}| - |\mathcal{Q}_{S_2}^{(0)}| = |\mathcal{Q}_{S_2}^{(1)}| - p$ and $\alpha_2 = |\mathcal{Q}_{S_3}^{(1)}| - p$. With these, we have

$$\begin{aligned}\mathsf{p}_2(\tau) &= \Pr\left[(\mathbf{k}, \mathcal{S}) \xleftarrow{\$} \left(\{0,1\}^{wn}\right)^5 \times \mathsf{Perm}(n)^4 : \left(\mathsf{SP}_{\mathbf{k}}^T[\mathcal{S}] \vdash \mathcal{Q}_C\right) \wedge \left(\mathcal{S} \vdash \mathcal{Q}_S\right)\right] \\ &\geq \sum_{\tau' \in \Theta_{\text{good}}(\tau)} \mathsf{p}_{\text{re}}(\tau') \geq \sum_{\tau' \in \Theta_{\text{good}}(\tau)} \frac{1}{N^{5w}\left((N)_N\right)^2 (N)_{p+\alpha_1} (N)_{p+\alpha_2}} \cdot \mathsf{p}_{\text{mid}}(\tau').\end{aligned}$$

Therefore,

$$\begin{aligned}\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} &\geq \sum_{\tau' \in \Theta_{\text{good}}(\tau)} \frac{(N^w)_q \cdot \left((N)_p\right)^4}{N^{5w}\left((N)_N\right)^2 (N)_{p+\alpha_1} (N)_{p+\alpha_2}} \cdot \mathsf{p}_{\text{mid}}(\tau') \\ &\geq \min_{\tau' \in \Theta_{\text{good}}(\tau)} \left((N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau')\right) \underbrace{\sum_{\tau' \in \Theta_{\text{good}}(\tau)} \frac{1}{N^{5w}\left((N-p)_{N-p}\right)^2 (N-p)_{\alpha_1} (N-p)_{\alpha_2}}}_{B}.\end{aligned}$$

Note that, the exact probability of observing the extended transcript τ' is

$$\frac{1}{N^{5w}\left((N-p)_{N-p}\right)^2 (N-p)_{\alpha_1} (N-p)_{\alpha_2}},$$

since:

1. sample keys $k_0, \ldots, k_4 \in \{0,1\}^{wn}$ uniformly and independently at random;
2. sample two random permutations S_1, S_4 from $\mathsf{Perm}(n)$ at uniform, such that $S_1 \vdash \mathcal{Q}_{S_1}^{(0)}, S_4 \vdash \mathcal{Q}_{S_4}^{(0)}$.
3. choose the partial extension of the S-box queries based on the new collisions $\mathcal{Q}'_S$ uniformly at random (meaning that each possible u or v is chosen uniformly at random in the set of its authorized values).

This means the term B captures the probability of good transcript extensions:

$$B = \sum_{\tau' \in \Theta_{\text{good}}(\tau)} \frac{1}{N^{5w}\left((N-p)_{N-p}\right)^2 (N-p)_{\alpha_1} (N-p)_{\alpha_2}} = \Pr\left[\tau' \in \Theta_{\text{good}}\ (\tau)\right],$$

which further implies

$$\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq \Pr\left[\tau' \in \Theta_{\text{good}}\ (\tau)\right] \cdot \min_{\tau' \in \Theta_{\text{good}}(\tau)} \left((N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau')\right). \tag{7}$$

The term $\mathsf{p}_{\text{mid}}(\tau')$ captures the probability that $\mathcal{C}_{\mathbf{k}'}^T[\mathcal{S}] \vdash \mathcal{Q}'_C$, i.e., the inner two SPN rounds are consistent with the pairs of inputs/outputs (a, b) defined in $\mathcal{Q}'_C$. We appeal to [**?**] to have a concrete bound on $(N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau')$.

Lemma 6. *Assume $p + wq \leq N/2$, then*

$$(N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau') \geq 1 - \frac{q^2}{N^w} - \frac{q(2wp + 6w^2q)^2}{N^2}. \tag{8}$$

Proof. It can be checked that, the transcript $(\mathcal{Q}'_C, \mathcal{Q}^{(1)}_{S_2}, \mathcal{Q}^{(1)}_{S_3})$ satisfies exactly the conditions defining a good transcript as per [**?**, page 740]. Moreover, the ratio $\mathsf{p}_{\mathrm{mid}}(\tau')/(1/(N^w)_q)$ is exactly the ratio of the probabilities to get τ' in the real and in the ideal world. The result thus immediately follows from [**?**, Lemma 9]. □

Gathering Eqs. (6), (7), and (8), we obtain

$$\begin{aligned}\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq & \left(1-\frac{3w^2q\,(p+wq)^2}{N^2}-\frac{w^2q}{N}-\frac{9w^2q(p+wq)^2}{N^2}-\frac{16w^3q^2p}{N^2}\right)\cdot\left(1-\frac{q^2}{N^w}-\frac{q(2wp+6w^2q)^2}{N^2}\right)\\ \geq & 1-\frac{3w^2q\,(p+wq)^2}{N^2}-\frac{w^2q}{N}-\frac{9w^2q(p+wq)^2}{N^2}-\frac{16w^3q^2p}{N^2}-\frac{q^2}{N^w}-\frac{q(2wp+6w^2q)^2}{N^2}\end{aligned}$$

as claimed in Eq. (3).

4 TSPRP Security of 6-Round Tweakable Linear SPNs

In this section, we prove beyond-birthday-bound STPRP security for 6-round tweakable linear SPNs. Concretely, let $\mathsf{SP}_{\mathbf{k}}[\mathcal{S}]$ be the 6-round SPN using any linear transformations T. I.e.,

$$\begin{aligned}\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}](x) := k_6 \oplus t \oplus \overline{S_6}(k_5 \oplus t \oplus T(\overline{S_5}(k_4 \oplus t \oplus \overline{S_4}(k_3 \oplus t \oplus T(\overline{S_3}(k_2 \oplus t \oplus T(\\ \overline{S_2}(k_1 \oplus t \oplus T(\overline{S_1}(k_0 \oplus t \oplus x))))))))))). \qquad (9)\end{aligned}$$

We show that SP^T is an STPRP as long as: (i) the linear layer T contains no zero entries, and (ii) the round keys $\{k_i\}(i=0,\ldots,6)$ are uniform and independent, and (iii) the tweak t is directly xored into each round key.

Theorem 2. *Assume $w \geq 2$, and $p+wq \leq N/2$. Let $\mathsf{SP}_{\mathbf{k}}[\mathcal{S}]$ be a 6-round, tweakable linear SPN as defined by Eq. (9). If round keys $\mathbf{k}=(k_0,\ldots,k_6)$ are uniform and independent, and T contains no zero entries, then*

$$\begin{aligned}\mathrm{Adv}^{\mathrm{su}}_{\mathsf{SP}^T}(p,q) \leq & \frac{q^2}{2^{nw}}+\frac{8w^2q(p+wq)^2+w^2q}{2^n}.\\ \mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(p,q) \leq & \frac{q^2}{2^{nw}}+\frac{8w^2q(p+wq)^2+w^2q}{2^n}\\ & +\frac{16w^2q(p+wq)(p+wq+3q)+4w^2q(p+3wq)^2}{2^{2n}}.\end{aligned}$$

For the proof, we rely on the following lemma and Lemmas 1 and 2.

Lemma 7. *Assume $p+wq \leq N/2$. Let $\mathcal{D}$ be a distinguisher in the single-user setting that makes p primitive queries to each of $S_1,\ldots,S_6$, and makes q construction queries. Then for any attainable transcript $\tau=(\mathcal{Q}_C,\mathcal{Q}_S)$, one has*

$$\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq 1-xxx. \qquad (10)$$

Similar to the 4-round case, we will first define the notion of extended transcripts. We then define bad extensions and bound their probability. The ratio $\mathsf{p}_2(\tau)/\mathsf{p}_1(\tau)$ is then derived similarly to the 4-round case.

Transcript Extension for 6 rounds. Fix a distinguisher $\mathcal{D}$ as described in the statement and fix an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$ obtained $\mathcal{D}$. For $i \in \{1, \cdots, 6\}$, let

$$\mathcal{Q}_{S_i}^{(0)} = \{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (i, u, v) \in \mathcal{Q}_S\},$$

and let

$$\begin{aligned} U_i^{(0)} &= \left\{u_i \in \{0,1\}^n : (i, u_i, v_i) \in \mathcal{Q}_{S_i}^{(0)}\right\} \\ V_i^{(0)} &= \left\{v_i \in \{0,1\}^n : (i, u_i, v_i) \in \mathcal{Q}_{S_i}^{(0)}\right\}, \end{aligned}$$

denote the domains and ranges of $\mathcal{Q}_{S_i}^{(0)}, i \in \{1, \cdots, 6\}$, respectively.

In detail, a transcript τ is extended in the following manner:

– At the end of the interaction between $\mathcal{D}$ and the real world $(\mathcal{S}, \mathsf{SP}_{\mathbf{k}}^{T}[\mathcal{S}])$, we append τ with the keys $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4)$ and the two random permutations S_1, S_4 in use;

– At the end of the interaction between $\mathcal{D}$ and the ideal world $(\mathcal{S}, \widetilde{P})$, we append τ with randomly sampled keys $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4)$ and the two random permutations S_1, S_4 in use.

Note that, in either case, it is equivalent to sampling two new random permutations S_1, S_4 such that $S_1 \vdash \mathcal{Q}_{S_1}$ and $S_4 \vdash \mathcal{Q}_{S_4}$ and appending them to τ. With the above, for any $(x, y) \in \mathcal{Q}_C$ we define

$$\begin{aligned} a &= T\big(\overline{S_1}\,(x \oplus k_0)\,\big), & c &= T\big(\overline{S_2}\,(a \oplus k_1)\,\big), \\ d &= T^{-1}\big(\overline{S_3^{-1}}\,(b \oplus k_3)\,\big), & b &= T^{-1}\big(\overline{S_4^{-1}}\,(y \oplus k_4)\,\big). \end{aligned}$$

This extends the list $\mathcal{Q}_C$ into $\mathcal{Q}_C' = \big((x_1, a_1, c_1, d_1, b_1, y_1), \ldots, (x_q, a_q, c_q, d_q, b_q, y_q)\big)$. Then, a colliding query is defined as a construction query $(x, a, c, d, b, y) \in \mathcal{Q}_C'$ as follows:

1. there exist an S-box query $(u, v) \in \mathcal{Q}_{S_2}^{(0)}$ and an integer $i \in \{1, \ldots, w\}$ such that $(a \oplus k_1)[i] = u$.
2. there exist an S-box query $(u, v) \in \mathcal{Q}_{S_3}^{(0)}$ and an integer $i \in \{1, \ldots, w\}$ such that $\big(b \oplus T^{-1}(k_3)\big)[i] = v$.
3. there exist a construction query $(a', b') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(a, b, i) \neq (a', b', j)$ and $(a \oplus k_1)[i] = (a' \oplus k_1)[j]$.
4. there exist a construction query $(a', b') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(a, b, i) \neq (a', b', j)$ and $i \in \{1, \ldots, w\}$ such that $\big(b \oplus T^{-1}(k_3)\big)[i] = \big(b' \oplus T^{-1}(k_3)\big)[j]$.

Now we further introduce a new set $\mathcal{Q}'_S$ of S-box evaluations to complete the transcript extension. In detail, for each colliding query $(x, a, b, y) \in \mathcal{Q}'_C$, we will add tuples $(2, (a \oplus k_1)[i], v')_{1 \le i \le w}$ (if (a, b) collides at the input of S_2) or $\big(3, u', (b \oplus T^{-1}(k_3))[i]\big)_{1 \le i \le w}$ (if (a, b) collides at the output of S_3) to $\mathcal{Q}'_S$ by lazy sampling $v' = S_2((a \oplus k_1)\,[i])$ or $u' = S_3^{-1}((b \oplus k_3)\,[i])$, as long as it has not been determined by any existing query in $\mathcal{Q}_S$.

An extended transcript of τ includes all the above additional information, i.e.,

$$\tau' = (\mathcal{Q}'_C, \mathcal{Q}_S, \mathcal{Q}'_S, S_1, S_4, \mathbf{k}).$$

For each collision between a construction query and a primitive query, or between two construction queries, the extended transcript will contain enough information to compute a complete round of the evaluation of the SPN. This will be useful to lower bound the probability to get the transcript τ in the real world.

Bad Extension for 6 rounds. Consider an attainable extended transcript $\tau' = (\mathcal{Q}'_C, \mathcal{Q}_S, \mathcal{Q}'_S, S_1, S_2, S_5, S_6, \mathbf{k})$. Let

$$\begin{aligned} \mathcal{Q}^{(1)}_{S_3} &= \{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (2, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_S\} \\ \mathcal{Q}^{(1)}_{S_4} &= \{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (3, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_S\}\,. \end{aligned}$$

In words, $\mathcal{Q}^{(1)}_{S_i}$ summarizes each constraint that is forced on S_i by $\mathcal{Q}_S$ and $\mathcal{Q}'_S$. Let

$$\begin{aligned} U_3^{(1)} &= \left\{u_2 \in \{0,1\}^n : (2, u_2, v_2) \in \mathcal{Q}^{(1)}_{S_2}\right\}, \quad V_3^{(1)} = \left\{v_2 \in \{0,1\}^n : (2, u_2, v_2) \in \mathcal{Q}^{(1)}_{S_2}\right\}, \\ U_4^{(1)} &= \left\{u_3 \in \{0,1\}^n : (3, u_3, v_3) \in \mathcal{Q}^{(1)}_{S_3}\right\}, \quad V_4^{(1)} = \left\{v_3 \in \{0,1\}^n : (3, u_3, v_3) \in \mathcal{Q}^{(1)}_{S_3}\right\}. \end{aligned}$$

be the domains and ranges of $\mathcal{Q}^{(1)}_{S_3}$ and $\mathcal{Q}^{(1)}_{S_4}$ respectively.

Definition 2. *We say an extended transcript τ' is bad if at least one of the following conditions is fulfilled. The conditions are classified into two categories depending on the relevant randomness. In detail, regarding $k_0, k_1, k_2, k_4, k_5, k_6$:*

(C-1) there exist (not necessarily distinct) $(t, x, a, c, d, b, y), (t', x', a', c', d', b', y'), (t'', x'', a'', b'', y'') \in \mathcal{Q}'_C$ and distinct $i, i', i'' \in \{1, \ldots, w\}$ such that any of the following holds:

- $(x \oplus t \oplus k_0)[i] = (x' \oplus t' \oplus k_0)[i'] = (x'' \oplus t'' \oplus k_0)[i'']$*;*
- $(a \oplus t \oplus k_1)[i] = (a' \oplus t' \oplus k_1)[i'] = (a'' \oplus t'' \oplus k_1)[i'']$*;*
- $(c \oplus t \oplus k_2)[i] = (c' \oplus t' \oplus k_2)[i'] = (c'' \oplus t'' \oplus k_2)[i'']$*;*
- $(d \oplus t \oplus T^{-1}(k_4))[i] = (c' \oplus t' \oplus T^{-1}(k_4))[i'] = (c'' \oplus t'' \oplus T^{-1}(k_4))[i'']$*;*
- $(b \oplus t \oplus T^{-1}(k_5))[i] = (b' \oplus t' \oplus T^{-1}(k_5))[i'] = (b'' \oplus t'' \oplus T^{-1}(k_5))[i'']$*;*
- $(y \oplus t \oplus k_6)[i] = (y' \oplus t' \oplus k_6)[i'] = (y'' \oplus t'' \oplus k_6)[i'']$.

(C-2) there exist $(t, x, a, b, y) \in \mathcal{Q}'_C$ and distinct indices $i, i' \in \{1, \ldots, w\}$ such that:

- $(x \oplus t \oplus k_0)[i] \in U_1^{(0)}$ *and* $(x \oplus t \oplus k_0)[i'] \in U_1^{(0)}$, *or*
- $(a \oplus t \oplus k_1)[i] \in U_2^{(0)}$ *and* $(a \oplus t \oplus k_1)[i'] \in U_2^{(0)}$, *or*
- $(c \oplus t \oplus k_2)[i] \in U_3^{(1)}$ *and* $(c \oplus t \oplus k_2)[i'] \in U_3^{(1)}$, *or*

- $(d \oplus t \oplus T^{-1}(k_4))[i] \in V_4^{(1)}$ *and* $(d \oplus t \oplus T^{-1}(k_4))[i'] \in V_4^{(1)}$*, or*
- $(b \oplus t \oplus T^{-1}(k_5))[i] \in V_5^{(0)}$ *and* $(b \oplus t \oplus T^{-1}(k_5))[i'] \in V_5^{(0)}$*, or*
- $(y \oplus t \oplus k_6)[i] \in V_6^{(0)}$ *and* $(y \oplus t \oplus k_6)[i'] \in V_6^{(0)}$*.*

(C-3) there exist $(t, x, a, b, y) \in \mathcal{Q}'_C$ *and* $i, j \in \{1, \dots, w\}$ *such that:*

- $(x \oplus t \oplus k_0)[i] \in U_1^{(0)}$ *and* $(y \oplus t \oplus k_6)[j] \in V_6^{(0)}$*, or*
- $(x \oplus t \oplus k_0)[i] \in U_1^{(0)}$ *and* $(a \oplus t \oplus k_1)[j] \in U_2^{(0)}$*, or*
- $(a \oplus t \oplus k_1)[i] \in U_2^{(0)}$ *and* $(c \oplus t \oplus k_2)[j] \in U_3^{(1)}$*, or*
- $(d \oplus t \oplus T^{-1}(k_4))[i] \in V_4^{(1)}$ *and* $(b \oplus t \oplus T^{-1}(k_5))[j] \in V_5^{(0)}$*, or*
- $(b \oplus t \oplus T^{-1}(k_5))[i] \in V_5^{(0)}$ *and* $(y \oplus t \oplus k_6)[j] \in V_6^{(0)}$*.*

Regarding $k_2, S_1, S_4,$ *and* $\mathcal{Q}'_S$*:*

(C-4) there exist $(x, a, b, y) \in \mathcal{Q}'_C$ *and* $i, j \in \{1, \dots, w\}$ *such that:*

- $(c \oplus k_2 \oplus t)[i] \in U_3^{(1)}$ *and* $(d \oplus T^{-1}(k_4 \oplus t))[j] \in V_4^{(1)}$*, or*
- $(c \oplus k_2 \oplus t)[i] \in U_3^{(1)}$ *and* $(T(\overline{S_3}(c \oplus k_2 \oplus t)) \oplus k_3 \oplus t)[j] \in U_4^{(1)}$*, or*
- $(T^{-1}(\overline{S_4^{-1}}(d \oplus T^{-1}(k_4 \oplus t)) \oplus k_3 \oplus t))[i] \in V_3^{(1)}$ *and* $(d \oplus T^{-1}(k_4 \oplus t))[j] \in V_4^{(1)}$*.*

(C-5) there exist $(x, a, b, y), (x', a', b', y') \in \mathcal{Q}'_C$ *and* $i, i', j, j' \in \{1, \dots, w\}$*,* $(a, b, j) \neq (a', b', j')$*, such that* $(a \oplus k_2 \oplus t)[i] \in U_3^{(1)}, (a' \oplus k_2 \oplus t)[i'] \in U_3^{(1)}$*, and*

$$\big(T(\overline{S_2}(a \oplus k_1 \oplus t)) \oplus k_2 \oplus t\big)[j] = \big(T(\overline{S_2}(a' \oplus k_1 \oplus t)) \oplus k_2 \oplus t\big)[j'].$$

(C-6) there exist $(x, a, b, y), (x', a', b', y') \in \mathcal{Q}'_C$ *and* $i, i', j, j' \in \{1, \dots, w\}$*,* $(a, b, j) \neq (a', b', j')$*, such that* $\big(b \oplus T^{-1}(k_3 \oplus t)\big)[i] \in V_4^{(1)}, \big(b' \oplus T^{-1}(k_3 \oplus t)\big)[i'] \in V_4^{(1)}$*, and*

$$\big(T^{-1}(\overline{S_3^{-1}}(b \oplus T^{-1}(k_3 \oplus t)) \oplus k_2 \oplus t)\big)[j] = \big(T^{-1}(\overline{S_3^{-1}}(b' \oplus T^{-1}(k_3 \oplus t)) \oplus k_2 \oplus t)\big)[j'].$$

Any extended transcript that is not bad will be called good. Given an original transcript τ*, we denote* $\Theta_{\mathrm{good}}(\tau)$ *(resp.* $\Theta_{\mathrm{bad}}(\tau)$*) the set of good (resp. bad) extended transcripts of* τ *and* $\Theta'(\tau)$ *the set of all extended transcripts of* τ*.*

Lemma 8. *One has*

$$\Pr\big[\tau' \in \Theta_{bad}(\tau)\big] \leq \frac{3w^2 q\,(p + wq)^2}{N^2} + \frac{w^2 q}{N}. \tag{11}$$

Proof. The analyses of the conditions just follow Lemma 5 and thus we omit. The crux lies in the conditions (C-4), (C-5), and (C-6).

(C-4). We consider the probability to have $(c \oplus k_2 \oplus t)[j] \in U_2^{(1)}$. Note that this consists of two subevents:

- $(c \oplus k_2 \oplus t)[j] \in U_2^{(1)}$, and
- there exists $(t', x', y', j') \neq (t, x, y, j)$ such that $(c \oplus k_2 \oplus t)[j] \neq (c' \oplus k_2 \oplus t')[j']$.

For the 1st subevent, conditioned on $\neg$(C-3), ... thus its probability is at most $1/(N-p-wq)$.

For the 2nd subevent, when $j\neq j'$, it immediately holds $\Pr\big[(c\oplus k_2\oplus t)[j]\neq (c'\oplus k_2\oplus t')[j']\big]=1/N$. Below we focus on the case of $j=j'$ meaning that $(t',x',y')\neq(t,x,y)$. We have to further distinguish **three** cases as follows.

Case 1: $x\oplus t\neq x'\oplus t'$. Then **using the previous idea, it can be show**

$$\Pr[a\oplus t=a'\oplus t'|x\oplus t\neq x'\oplus t']\le\frac{1}{N-p-wq}.$$

Similarly, it further holds

$$\Pr[(c\oplus t)[j]\neq(c'\oplus t')[j']|a\oplus t=a'\oplus t']\le\frac{1}{N-p-wq}.$$

Case 2: $x\oplus t=x'\oplus t'$. Then it necessarily holds $a\oplus t\neq a'\oplus t'$, and thus

$$\Pr[(c\oplus t)[j]\neq(c'\oplus t')[j']|a\oplus t=a'\oplus t']\le\frac{1}{N-p-wq}.$$

For any construction query $(x,a,b,y)\in\mathcal{Q}'_C$, to have $(a\oplus k_1)[i]\in U_2^{(1)}$, it has to be $(x\oplus k_0)[i_0]\notin U_1^{(0)}$ for any $i_0\in\{1,\dots,w\}$, as otherwise it contradicts $\neg$(B-4).

For any $(x,a,b,y)\in\mathcal{Q}'_C$ and any i,j, it holds

$$\begin{aligned}\Pr\big[(a\oplus k_1)[j]\in U_2^{(1)}\big]\le&\sum_{u_2\in U_2^{(0)}}\underbrace{\Pr\big[\big(T(\overline{S_1}(x\oplus k_0))\oplus k_1\big)[i]=u_2\big]}_{=1/N\ \text{(Lemma 4)}}\\&+\sum_{(x',a',b',y')\in\mathcal{Q}'_C}\sum_{i',i}\underbrace{\Pr\big[(a\oplus k_1)[i]=(a'\oplus k_1)[i']\big]}_{\le 1/(N-p-wq)\ \text{(Lemma 4)}}\\\le&\frac{p}{N}+\frac{w^2q}{N-p-wq}\le\frac{p+2w^2q}{N}.\end{aligned}$$

Similarly, $\Pr\big[(b\oplus T^{-1}(k_3))[j]\in V_3^{(1)}\big]\le(p+2w^2q)/N$. Since we have at most w^2q choices for (x,a,b,y) and $i,j\in\{1,\dots,w\}$, we have

$$\Pr\big[\text{(B-6)}\mid\neg\text{(B-3)}\wedge\neg\text{(B-4)}\big]\le w^2q\cdot\Big(\frac{2(p+wq)}{N}\Big)^2\le\frac{4w^2q(p+wq)^2}{N}.$$

- 0
- 0
- 0
- 0
- 0

$$
\begin{aligned}
\Pr[(\text{B-8})] = &\sum_{(x,a,b,y),(x',a',b',y')\in\mathcal{Q}'_C}\ \sum_{i,i',j,j'} \Bigg(\underbrace{\Pr\big[(a\oplus k_1)[i]\in U_2^{(1)}\big]}_{\le (p+wq)/(N-p-wq)} \\
&\times \underbrace{\Pr\big[(a'\oplus k_1)[i]\in U_2^{(1)} | (a\oplus k_1)[i]\in U_2^{(1)}\big]}_{\le 1} \times \underbrace{\mathsf{pcoll}_2^{+}(2,a,a',i,i',j,j')}_{\le 1/(N-p-wq)} \Bigg) \\
\le &\binom{wq}{2}\cdot w^2\cdot \frac{p+wq}{N-p-wq}\cdot\frac{1}{N-p-wq} \le \frac{w^4q^2(p+wq)}{2(N-p-wq)^2}.
\end{aligned}
$$

Similarly by symmetry,

$$
\Pr[(\text{B-9})] \le \frac{w^4q^2(p+wq)}{2(N-p-wq)^2}.
$$

Summing over the above yields

$$
\begin{aligned}
&\Pr\left[\tau'\in \mathit{\Theta}_{\text{good}}\,(\tau)\right] \le \sum_{i=1}^{9}\Pr[(\text{B-}i)] \\
\le &\frac{w^2q(p+wq)^2}{(N-p-wq)^2} + \frac{2w^2q(p+wq)^2}{N(N-p-wq)} + \frac{w^2qp^2}{N^2} + \frac{8w^3q^2p}{N(N-p-wq)} \\
\le &\frac{9w^2q(p+wq)^2}{N^2} + \frac{16w^3q^2p}{N^2}.
\end{aligned}
$$

as claimed. □

Analyzing Good Extensions. This part just follows the same line as Sect. 3.3. In detail, define $\mathcal{C}_{\mathbf{k}}^T[\mathcal{S}](c) := \overline{S_4}(T(\overline{S_3}(c\oplus k_2))\oplus k_3)\oplus T^{-1}(k_4)$. Then, for any attainable transcript τ, we have the following upper bound for the the ideal world probability:

$$
\begin{aligned}
\mathsf{p}_1(\tau) = &\Pr\left[(\widetilde{P},\mathcal{S}) \xleftarrow{\$} \widetilde{\mathsf{Perm}}(\mathcal{T},wn)\times\mathsf{Perm}(n)^6 : (\mathcal{S}\vdash\mathcal{Q}_S)\wedge(\widetilde{P}\vdash\mathcal{Q}_C)\right] \\
\le &\frac{1}{(N^w)_q}\cdot\left(\frac{1}{(N)_p}\right)^6.
\end{aligned}
$$

To reach the real world probability $\mathsf{p}_2(\tau)$, for any transcript extension $\tau' = (\mathcal{Q}'_C, \mathcal{Q}_S, \mathcal{Q}'_S, S_1^*, S_2^*, S_5^*, S_6^*, \mathbf{k})$ from τ, denote

$$
\begin{aligned}
\mathsf{p}_{\text{re}}(\tau') = &\Pr\Big[\big(\mathbf{k}',\mathcal{S}\big) \xleftarrow{\$} \big(\{0,1\}^{wn}\big)^7\times\mathsf{Perm}(n)^6 : \Big(\big(S_1=S_1^*\big)\wedge\big(S_2=S_2^*\big)\wedge\big(S_5=S_5^*\big) \\
&\wedge\big(S_6=S_6^*\big)\wedge\big(S_3\vdash\mathcal{Q}_{S_3}^{(1)}\big)\wedge\big(S_4\vdash\mathcal{Q}_{S_4}^{(1)}\big)\wedge\big(\mathcal{C}_{\mathbf{k}'}^T[\mathcal{S}]\vdash\mathcal{Q}'_C\big)\wedge\big(\mathbf{k}'=\mathbf{k}\big)\Big)\Big] \\
\mathsf{p}_{\text{mid}}(\tau') = &\Pr\Big[\mathcal{S}\xleftarrow{\$}\mathsf{Perm}(n)^6 : (\mathcal{C}_{\mathbf{k}}^T[\mathcal{S}]\vdash\mathcal{Q}'_C)\ \Big|\ (S_1=S_1^*)\wedge(S_2=S_2^*)\wedge\big(S_5=S_5^*\big) \\
&\wedge\big(S_6=S_6^*\big)\wedge(S_3\vdash\mathcal{Q}_{S_3}^{(1)})\wedge(S_4\vdash\mathcal{Q}_{S_4}^{(1)})\Big].
\end{aligned}
$$

and let $\beta_1 = |\mathcal{Q}^{(1)}_{S_3}| - p$ and $\beta_2 = |\mathcal{Q}^{(1)}_{S_4}| - p$. With these, we have

$$\begin{aligned}
\mathsf{p}_2(\tau) =& \Pr\left[(\mathbf{k}, \mathcal{S}) \xleftarrow{\$} \left(\{0,1\}^{wn}\right)^7 \times \mathsf{Perm}(n)^6 : \left(\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_C\right) \wedge \left(\mathcal{S} \vdash \mathcal{Q}_S\right)\right] \\
\geq& \sum_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \mathsf{p}_{\mathrm{re}}(\tau') \geq \sum_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \frac{1}{N^{7w}\left((N)_N\right)^4 (N)_{p+\beta_1}(N)_{p+\beta_2}} \cdot \mathsf{p}_{\mathrm{mid}}(\tau').
\end{aligned}$$

Therefore,

$$\begin{aligned}
\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq& \sum_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \frac{(N^w)_q \cdot \left((N)_p\right)^6}{N^{7w}\left((N)_N\right)^4 (N)_{p+\beta_1}(N)_{p+\beta_2}} \cdot \mathsf{p}_{\mathrm{mid}}(\tau') \\
\geq& \min_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \left((N^w)_q \cdot \mathsf{p}_{\mathrm{mid}}(\tau')\right) \sum_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \frac{1}{N^{7w}\left((N-p)_{N-p}\right)^4 (N-p)_{\beta_1}(N-p)_{\beta_2}} \\
\geq& \Pr\left[\tau' \in \Theta_{\mathrm{good}}\ (\tau)\right] \cdot \min_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \left((N^w)_q \cdot \mathsf{p}_{\mathrm{mid}}(\tau')\right) \\
\geq& \Pr\left[\tau' \in \Theta_{\mathrm{good}}\ (\tau)\right] \cdot \left(1 - \frac{q^2}{N^w} - \frac{q(2wp + 6w^2q)^2}{N^2}\right) \qquad \text{(by Lemma 6)} \\
\geq& \left(1 - \frac{3w^2q\,(p+wq)^2}{N^2} - \frac{w^2q}{N} - \frac{9w^2q(p+wq)^2}{N^2} - \frac{16w^3q^2p}{N^2}\right) \cdot \left(1 - \frac{q^2}{N^w} - \frac{q(2wp+6w^2q)^2}{N^2}\right) \\
\geq& 1 - \frac{3w^2q\,(p+wq)^2}{N^2} - \frac{w^2q}{N} - \frac{9w^2q(p+wq)^2}{N^2} - \frac{16w^3q^2p}{N^2} - \frac{q^2}{N^w} - \frac{q(2wp+6w^2q)^2}{N^2}
\end{aligned}$$

as claimed in Eq. (10).

References

CL18. Benoît Cogliati and Jooyoung Lee. Wide tweakable block ciphers based on substitution-permutation networks: Security beyond the birthday bound. *IACR Cryptology ePrint Archive*, 2018:488, 2018.

CLS15. Benoît Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking even-mansour ciphers. In *Annual Cryptology Conference*, pages 189–208. Springer, 2015.

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.

CS15. Benoît Cogliati and Yannick Seurin. Beyond-birthday-bound security for tweakable even-mansour ciphers with linear tweak and key mixing. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 134–158. Springer, 2015.

Dae95. Joan Daemen. *Cipher and hash function design strategies based on linear and differential cryptanalysis.* PhD thesis, Doctoral Dissertation, March 1995, KU Leuven, 1995.

HT16. Viet Tung Hoang and Stefano Tessaro. Key-alternating ciphers and key-length extension: exact bounds and multi-user security. In *Annual International Cryptology Conference*, pages 3–32. Springer, 2016.

MV15. Eric Miles and Emanuele Viola. Substitution-permutation networks, pseudorandom functions, and natural proofs. *Journal of the ACM (JACM)*, 62(6):1–29, 2015.

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.