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

Yuan Gao[1,2], Chun Guo[1,2(✉)], and Meiqin Wang[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
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 security analysis of Substitution-Permutation Networks (SPNs), one of the most popular approach to construct modern blockciphers. In this theoretical model, the diffusion layers may be *non-linear*, which enables beyond-birthday-bound provable security. Though, for the SPN model with *linear diffusion layers*, which is closer to real world blockciphers, existing provable results are capped at the birthday barrier.
This paper solves this open problem, and proves that a 4-round SPN with linear diffusion layers is secure up to $2^{2n/3}$ adversarial queries. Besides, we show how to incorporate tweaks into linear SPNs, and prove that 6-round tweakable linear SPN is beyond birthday security. This provides additional insights into the real world SPN ciphers.

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

1 Introduction

Substitution-Permutation Networks. Nowadays block ciphers are mainly built around 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 $\mathbf{k}$ and the tweak $\mathbf{t}$ (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

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

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 $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$ obtained by $\mathcal{D}$, one has

$$\mathsf{p}_2\left(\mathcal{Q}_C | \mathcal{Q}_S\right) \geq (1 - \varepsilon(p, q))\mathsf{p}_1\left(\mathcal{Q}_C | \mathcal{Q}_S\right).$$

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 $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$ obtained by $\mathcal{D}$, one has

$$\mathsf{p}_2\left(\mathcal{Q}_C | \mathcal{Q}_S\right) \geq (1 - \varepsilon(p + wq, q))\mathsf{p}_1\left(\mathcal{Q}_C | \mathcal{Q}_S\right).$$

For any extended transcript $\tau' = (\mathcal{Q}_C, \mathcal{Q}_S, \mathcal{Q}'_S, k)$, where $\mathcal{Q}_S^{(1)} = \mathcal{Q}_S \cup \mathcal{Q}'_S$, denote

$$\mathrm{p}\left(\tau'\right) = \Pr\left[\mathcal{S} \xleftarrow{s} \mathrm{Perm}(n)^2 : \mathrm{SP}_k^T[\mathcal{S}] \vdash \mathcal{Q}_C | \left(S_1 \vdash \mathcal{Q}_{S_1}^{(1)}\right) \wedge \left(S_2 \vdash \mathcal{Q}_{S_2}^{(1)}\right)\right].$$

Then we will get the following lemma:

Lemma 3. *For any good extended transcript τ', one has*

$$(2^{wn})_q \, \mathrm{p}\left(\tau'\right) \geq 1 - \frac{q^2}{2^{wn}} - \frac{q\left(2wp + 6w^2q\right)^2}{2^{2n}}.$$

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.,

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

We show that SP^T is an SPRP as long as: (i) the linear layer T contains no zero entries (Miles and Viola [MV15] show that matrices with maximal branch number [Dae95] satisfy this property), and (ii) the round keys $\{k_i\}(i = 0, 1, 2, 3, 4)$ 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*

$$\mathrm{Adv}_{\mathsf{SP}^T}^{\mathrm{su}}(p, q) \leq \frac{q^2}{2^{nw}} + \frac{8w^2q(p + wq)^2 + w^2q}{2^n} \tag{3}$$

$$+ \frac{16w^2q(p + wq)(p + wq + 3q) + 4w^2q(p + 3wq)^2 + w^2q(p + wq)(3p + wq)}{2^{2n}}. \tag{4}$$

The proof of Theorem 4 relies on the following lemma and on Lemma 1 and Lemma 2.

Lemma 4. *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 and S_2 and makes q construction queries. Then for any attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, one has*

$$\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq 1 - xxx. \tag{5}$$

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 let

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

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

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

Recall that the domains and ranges of $\mathcal{Q}_{S_2}^{(0)}$ and $\mathcal{Q}_{S_3}^{(0)}$ are denoted by $U_2^{(0)}, V_2^{(0)}, U_3^{(0)}$, and $V_3^{(0)}$ respectively. 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.

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 transcripts. Let $\tau' = (\mathcal{Q}'_C, \mathcal{Q}_S, \mathcal{Q}'_S, S_1, S_4, \mathbf{k})$ be an attainable extended transcript. Let

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

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

$$U^{(1)}_2 = \left\{u_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}^{(1)}_{S_2}\right\}, \quad V^{(1)}_2 = \left\{v_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}^{(1)}_{S_2}\right\},$$
$$U^{(1)}_3 = \left\{u_3 \in \{0,1\}^n : (3,u_3,v_3) \in \mathcal{Q}^{(1)}_{S_3}\right\}, \quad V^{(1)}_3 = \left\{v_3 \in \{0,1\}^n : (3,u_3,v_3) \in \mathcal{Q}^{(1)}_{S_3}\right\}.$$

be the domains and ranges of $\mathcal{Q}^{(1)}_{S_1}, \ldots, \mathcal{Q}^{(1)}_{S_4}$, 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 exists $(x,a,b,y) \in \mathcal{Q}'_C, u_1 \in U^{(0)}_1, v_4 \in V^{(0)}_4$, and index $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0)[i] = u_1$ and $(y \oplus k_4)[j] = v_4$.
(B-2) there exists $(x,a,b,y) \in \mathcal{Q}'_C, u_1 \in U^{(0)}_1, u_2 \in U^{(0)}_2$, and index $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0)[i] = u_1$ and $(a \oplus k_1)[j] = u_2$.
(B-3) there exists $(x,a,b,y) \in \mathcal{Q}'_C, v_3 \in V^{(0)}_3, v_4 \in V^{(0)}_4$, and index $i,j \in \{1,\ldots,w\}$ such that $(y \oplus k_4)[j] = v_4$ and $\left(b \oplus T^{-1}(k_3)\right)[i] = v_3$.
(B-4) there exists $(x,a,b,y) \in \mathcal{Q}'_C$ and distinct indices $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0)[i] = (x \oplus k_0)[j]$, or $(y \oplus k_4)[i] = (y \oplus k_4)[j]$.

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

(B-5) there exist $(x,a,b,y) \in \mathcal{Q}'_C$, $i,j \in \{1,\ldots,w\}$, $u_2 \in U_2$ and $v_3 \in V_3$ such that $(a \oplus k_1)[i] = u_2$ and $(b \oplus T^{-1}(k_3))[j] = v_3$.
(B-6) there exist $(x,a,b,y) \in \mathcal{Q}'_C$, $i,j \in \{1,\ldots,w\}$, $u_2 \in U_2$ and $u_3 \in U_3$ such that $(a \oplus k_1)[i] = u_2$ and $(T(\overline{S_2}(a \oplus k_1)) \oplus k_2)[j] = u_3$.
(B-7) there exist $(x,a,b,y) \in \mathcal{Q}'_C$, $i,j \in \{1,\ldots,w\}$, $v_2 \in V_2$ and $v_3 \in V_3$ such that $(b \oplus T^{-1}(k_3))[j] = v_3$ and $\left(T^{-1}(b \oplus T^{-1}(k_3)) \oplus T^{-1}(k_2)\right)[j] = v_2$.
(B-8) there exist $(x,a,b,y) \in \mathcal{Q}'_C$, distinct $i,i' \in \{1,\ldots,w\}$, $u_2, u'_2 \in U^{(0)}_2$ such that

$$(a \oplus k_1)[i] = u_2, \text{ and } (a \oplus k_1)[i'] = u'_2.$$

(C-5) there exist distinct $(a,b),(a',b') \in \mathcal{Q}^*_C(S_1,S_4)$, distinct $i,i' \in \{1,\ldots,w\}$, $u_2 \in U_2$ such that

$$\left(T\left(a \oplus k_1\right)\right)[i] = u_2, \text{ and } \left(T\left(a \oplus k_1\right)\right)[i'] = \left(T\left(a' \oplus k_1\right)\right)[i'].$$

(B-9) *there exist* $(x,a,b,y),(x',a',b',y') \in \mathcal{Q}'_C$, $i,i',j,j' \in \{1,\ldots,w\}$, *with* $(a,b,j) \neq (a',b',j')$, $u_2,u'_2 \in U_2$ *such that* $(a \oplus k_1)[i] = u_2, (a' \oplus k_1)[i'] = u'_2$, *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-10) *there exist* $(x,a,b,y) \in \mathcal{Q}'_C$, *distinct* $i,i' \in \{1,\ldots,w\}$, $v_3,v'_3 \in V_3$ *such that*

$$\left(T^{-1}(b) \oplus k_3\right)[i] = v_3, \text{ and } \left(T^{-1}(b) \oplus k_3\right)[i'] = v'_3.$$

(C-8) *there exist distinct* $(a,b),(a',b') \in \mathcal{Q}^*_C(S_1,S_4)$, *distinct* $i,i' \in \{1,\ldots,w\}$, $v_3 \in V_3$ *such that*

$$\left(T^{-1}(b) \oplus k_3\right)[i] = v_3, \text{ and } \left(T^{-1}(b) \oplus k_3\right)[i] = \left(T^{-1}(b') \oplus k_3\right)[i'].$$

(B-11) *there exist* $(x,a,b,y),(x',a',b',y') \in \mathcal{Q}'_C$, $i,i',j,j' \in \{1,\ldots,w\}$, *with* $(a,b,j) \neq (a',b',j')$, $v_3,v'_3 \in V_3$ *such that* $\big(b \oplus T^{-1}(k_3)\big)[i] = v_3, \big(b' \oplus T^{-1}(k_3)\big)[i'] = v'_3$, *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 start by upper bounding the probability of getting bad transcripts in the ideal world.

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

$$\Pr[\tau' \in \Theta_{\text{bad}}(\tau)] \leq \frac{3w^2q\,(p+wq)^2}{N^2} + \frac{w^2q}{N} + \frac{9w^2q(p+wq)^2}{N^2} + \frac{16w^3q^2p}{N^2}. \quad (6)$$

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

(B-1), (B-2), AND (B-3). For each fixed choice of $(x,a,b,y) \in \mathcal{Q}'_C, (u_1,v_1) \in \mathcal{Q}^{(0)}_{S_1}, (u_4,v_4) \in \mathcal{Q}^{(0)}_{S_4}$ and indices $i,j \in \{1,\ldots,w\}$, since k_0 and k_4 are uniform and independent, the probability to have $(x \oplus k_0)[i] = u_1$ and $(y \oplus k_4)[j] = v_4$ is $1/N^2$. Since we have at most w^2qp^2 such choices, we have

$$\Pr[\text{(B-1)}] \leq \frac{w^2q\,(p+wq)^2}{N^2}.$$

Similarly, since k_0 and k_1 are uniform and independent, and we have at most $w^2qp\,(p+wq)$ for $(x,a,b,y) \in \mathcal{Q}'_C, (u_1,v_1) \in \mathcal{Q}^{(0)}_{S_1}, (u_2,v_2) \in \mathcal{Q}^{(0)}_{S_2}$ and indices $i,j \in \{1,\ldots,w\}$, we have $\Pr[\text{(B-2)}] \leq \frac{w^2qp(p+wq)}{N^2} \leq \frac{w^2q(p+wq)^2}{N^2}$; since k_3 and k_4 are uniform and independent, we have $\Pr[\text{(B-3)}] \leq \frac{w^2q(p+wq)^2}{N^2}$ by symmetry.

(B-4). Since k_0 and k_4 are uniform, for each $(x,a,b,y) \in \mathcal{Q}'_C$ and $i,j \in \{1,\ldots,w\}$, the probability to have $(x \oplus k_0)[i] = (x \oplus k_0)[j]$ or $(y \oplus k_4)[i] = (y \oplus k_4)[j]$ is $2/N$. Since the number of such choices is $q\binom{w}{2} \leq w^2q/2$, we have $\Pr[\text{(B-4)}] \leq \frac{w^2q}{N}$.

For the remaining, define event

$\mathsf{Coll}_2(x,a,b,y) \Leftrightarrow$ there exist $i \in \{1,\ldots,w\}$ and $u_2 \in U_2$ such that $(a \oplus k_1)[i] = u_2$.

This event can be broken down into the following two subevents:

- $\mathsf{Coll}_{21}(x,a,b,y)$: there exist $i \in \{1,\ldots,w\}$, $(u_2,v_1) \in \mathcal{Q}_{S_2}^{(0)}$ such that $(a \oplus k_1)[i] = u_2$;
- $\mathsf{Coll}_{22}(x,a,b,y)$: there exist $(x',a',b',y') \in \mathcal{Q}'_C$, $i,i' \in \{1,\ldots,w\}$ such that $(a,b,i) \neq (a',b',i')$ and $(a \oplus k_1)[i] = (a' \oplus k_1)[i']$.

Consider the subevent $\mathsf{Coll}_{21}(x,a,b,y)$ first. To have $(a \oplus k_1)[i] = u_2$, 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-2). Thus conditioned on $S_1 \vdash \mathcal{Q}_{S_1}$, the value of $S_1((x \oplus k_0)[i_0])$ remains uniform in $\{0,1\}^n \backslash V_1^{(1)}$ for any fixed i_0. Because every entry in the i_0th column of T is nonzero, we have

$$\Pr\left[\mathsf{Coll}_{21}(x,a,b,y)\right] = \Pr\left[\exists i, u_2 : (T(\overline{S_1}(x \oplus k_0)) \oplus k_1)[i] = u_2\right] \leq \frac{wp}{N-p-wq}.$$

For the subevent $\mathsf{Coll}_{22}(x,a,b,y)$, note that

$$\Pr\left[\mathsf{Coll}_{22}(x,a,b,y)\right] = \underbrace{\sum_{(x',a',b',y') \in \mathcal{Q}'_C} \sum_{i \neq i' \in \{1,\ldots,w\}} \Pr\left[(a \oplus k_1)[i] = (a' \oplus k_1)[i']\right]}_{\leq w^2 q/2N} \quad (7)$$

$$+ \sum_{(x',a',b',y') \in \mathcal{Q}'_C, x' \neq x} \sum_{i \in \{1,\ldots,w\}} \Pr\left[a[i] = a'[i]\right], \quad (8)$$

where (7) follows from that $k_1[i]$ and $k_1[i']$ are uniform and independent. For the term (8),

- 0
- 0
- 0
- 0
- 0

Similarly, define

$\mathsf{Coll}_3(x,a,b,y) \Leftrightarrow$ there exist $i \in \{1,\ldots,w\}$ and $v_3 \in V_3$ such that $(b \oplus T^{-1}(k_3))[i] = v_3$.

Then it holds

by symmetry. With these, we are able to analyze the remaining conditions.
(C-1). Consider the probability that a construction query $(x,a,b,y) \in \mathcal{Q}'_C$ fulfills (C-1). If $(a \oplus k_1)[i] \in U_2$, then 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-2). Thus conditioned on $S_1 \vdash \mathcal{Q}_{S_1}$, the value of $S_1((x \oplus k_0)[i_0])$ remains uniform in $\{0,1\}^n \backslash V_1^{(1)}$ for any fixed i_0. Because every entry in the i_0th column of T is nonzero, the probability to have

$(a \oplus k_1)[i] = (T(\overline{S_1}(x \oplus k_0)) \oplus k_1)[i] = u_2$ is at most $1/(N-p-wq)$. Similarly, the probability of $(b \oplus T^{-1}(k_3))[j] = v_3$ is at most $1/(N-p-wq)$. Since we have at most $q(p+wq)^2w^2$ choices for (x,a,b,y), $i,j \in \{1,\ldots,w\}$, $u_2 \in U_2$ and $v_3 \in V_3$, we have

$$\Pr[\text{(C-1)}] \leq \frac{w^2q(p+wq)^2}{(N-p-wq)^2}.$$

(C-2) AND (C-3). Following the analysis of (C-1), for any $(x,a,b,y) \in \mathcal{Q}'_C$, the probability to have $(a \oplus k_1)[i] = u_2$ is at most $1/(N-p-wq)$. On the other hand, since k_2 is uniform and independent from the queries and from k_0, k_1, the probability to have $(T(\overline{S_2}(a \oplus k_1)) \oplus k_2)[j] = u_3$ is $1/N$. Since we have at most $q(p+wq)^2w^2$ choices for (x,a,b,y), $i,j \in \{1,\ldots,w\}$, $u_2 \in U_2$ and $u_3 \in U_3$, we have

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

Similarly,

$$\Pr[\text{(C-3)}] \leq \frac{w^2q(p+wq)^2}{N(N-p-wq)}.$$

(C-4) AND (C-7). For any of the $qw^2p^2/2$ choices of $(x,a,b,y) \in \mathcal{Q}'_C$, distinct $i,i' \in \{1,\ldots,w\}$, and $u_2,u'_2 \in U_2^{(0)}$, the probability to have $(a \oplus k_1)[i] = u_2$ and $(a \oplus k_1)[i'] = u'_2$ is $1/N^2$, since k_1 is uniform and independent of S_1. By these, we have

$$\Pr[\text{(C-4)}] \leq \frac{w^2qp^2}{2N^2}.$$

Similarly, using the uniformness of k_3, we have

$$\Pr[\text{(C-7)}] \leq \frac{w^2qp^2}{2N^2}.$$

CONDITIONS (C-6) AND (C-9). Consider (C-6) first. For any choice of $(x,a,b,y),(x',a',b',y') \in \mathcal{Q}'_C, i,i',j,j' \in \{1,\ldots,w\}$, with $(x,j) \neq (x',j')$, $u_2,u'_2 \in U_2$, denote by $\mathsf{Coll}(x,x',i,i',j,j',u_2,u'_2)$ the event that

$$(a \oplus k_1)[i] = u_2 \bigwedge (a' \oplus k_1)[i'] = u'_2 \bigwedge \big(T(\overline{S_2}(a \oplus k_1)) \oplus k_2\big)[j] = \big(T(\overline{S_2}(a' \oplus k_1)) \oplus k_2\big)[j'].$$

With this, we derive the probability via the following calculations.

$$\begin{aligned}\Pr[\text{(C-6)}] = &\underbrace{\sum_{(a,b),(a',b')}\sum_{i,i'}\sum_{(u_2,v_2),(u_2',v_2')}\sum_{j\neq j'}\Pr[\mathsf{Coll}(x,x',i,i',j,j',u_2,u_2')]}_{A_1}\\ &+\underbrace{\sum_{(a,b)\neq(a',b')}\sum_{i,i'}\sum_{(u_2,v_2)}\sum_{j}\Pr[\mathsf{Coll}(x,x',i,i',j,j',u_2,u_2')]}_{A_2}\\ &+\underbrace{\sum_{(a,b)\neq(a',b')}\sum_{i\neq i'}\sum_{(u_2,v_2)\neq(u_2',v_2')}\sum_{j}\Pr[\mathsf{Coll}(x,x',i,i',j,j',u_2,u_2')]}_{A_3}\\ &+\underbrace{\sum_{(a,b)\neq(a',b')}\sum_{i}\sum_{(u_2,v_2)\neq(u_2',v_2')}\sum_{j}\Pr[\mathsf{Coll}(x,x',i,i',j,j',u_2,u_2')]}_{A_4}.\end{aligned}$$

Regarding the term A_1, which captures the case of $j \neq j'$, we have

$$\begin{aligned}&\Pr\left[\mathsf{Coll}(x,x',i,i',j,j',u_2,u_2')\right]\\ =&\Pr\Big[\big(T(\overline{S_2}(a\oplus k_1))\oplus k_2\big)[j] = \big(T(\overline{S_2}(a'\oplus k_1))\oplus k_2\big)[j'] \;\Big|\\ &\qquad\underbrace{(T(\overline{S_1}(x'\oplus k_0))\oplus k_1)[i]=u_2 \bigwedge (T(\overline{S_1}(x\oplus k_0))\oplus k_1)[i]=u_2\Big]}_{=1/N} \qquad (9)\\ &\times\underbrace{\Pr\left[(T(\overline{S_1}(x'\oplus k_0))\oplus k_1)[i]=u_2 \;\middle|\; (T(\overline{S_1}(x\oplus k_0))\oplus k_1)[i]=u_2\right]}_{\leq 1} \qquad (10)\\ &\times\underbrace{\Pr\left[(T(\overline{S_1}(x\oplus k_0))\oplus k_1)[i]=u_2\right]}_{\leq 1/(N-p-wq)} \qquad (11)\\ \leq&\frac{1}{N(N-p-wq)}, \qquad (12)\end{aligned}$$

where (9) follows from that $k_2[j]$ and $k_2[j']$ are uniform and independent, while (11) has been argued before. Summing over all the possible choices, we reach

$$\Pr[A_1] \leq \frac{w^4q^2p^2}{N(N-p-wq)^2} \leq \frac{w^4q^2p}{N(N-p-wq)}.$$

Regarding the term A_2, since the number of choices for $(a,b),(a',b') \in \mathcal{Q}_C^*(S_1,S_4)$, $i,i',j,j' \in \{1,\ldots,w\}$, with $(a,j) \neq (a',j')$, $u_2 = u_2' \in U_2$ is at most w^4q^2p, we have

$$\Pr[A_2] \leq \frac{w^4q^2p}{N(N-p-wq)}.$$

Regarding the term A_3, since $(a\oplus k_1)[i] \in U_2^{(0)}$, it holds $(a\oplus k_1)[i'] \notin U_2^{(0)}$ by $\neg$(C-4). Therefore, a random output v_2^* will be sampled during the extension

process, so that $((a \oplus k_1)[i'], v_2^*) \in \mathcal{Q}_{S_2}^{(1)}$. Conditioned on the values in $V_2^{(0)}$ (which includes v_2'), v_2^* is uniform in *at least* $N - p - wq$ possibilities. This means the probability to have $T(\overline{S_2}(a \oplus k_1))[j] = T(\overline{S_2}(a' \oplus k_1))[j]$ is at most $1/(N-p-wq)$, as every entry in the i'th column of T is nonzero. Moreover, as argued before, the probability to have $(T(\overline{S_1}(x \oplus k_0)) \oplus k_1)[i] = u_2$ is at most $1/(N - p - wq)$. By this,

$$\Pr[A_3] \leq \frac{w^3q^2p^2}{N(N-p-wq)^2} \leq \frac{w^3q^2p}{N(N-p-wq)}.$$

Finally, consider the term A_4. Assume that $\overline{S_2}(a \oplus k_1) = \mathbf{v}_1 \| v_1 \| \mathbf{v}_2$ and $\overline{S_2}(a \oplus k_1) = \mathbf{v}_1' \| v_1' \| \mathbf{v}_2'$ after the extension process.

Then the equality $T(\overline{S_2}(a \oplus k_1))[j] = T(\overline{S_2}(a' \oplus k_1))[j]$ implies

$$\mathbf{t}_1^* \cdot \mathbf{v}_1 \oplus t^* \oplus v_1 \oplus \mathbf{t}_2^* \cdot \mathbf{v}_2 = \mathbf{t}_1^* \cdot \mathbf{v}_1' \oplus t^* \oplus v_1' \oplus \mathbf{t}_2^* \cdot \mathbf{v}_2'. \tag{13}$$

for two vectors $\mathbf{t}_1^*, \mathbf{t}_2^*$ and $t^* \in \{0,1\}^n$. Now:

- If $\mathbf{v}_1 = \mathbf{v}_1'$ and $\mathbf{v}_2 = \mathbf{v}_2'$, then Eq. (13) collapses to $t^* \oplus v_1 = t^* \oplus v_1'$ which is not possible;
- Else, Eq. (13) holds with probability at most $1/(N - p - wq)$.

Moreover, as argued before, the probability to have $(T(\overline{S_1}(x \oplus k_0)) \oplus k_1)[i] = u_2$ is at most $1/(N - p - wq)$. By this,

$$\Pr[A_4] \leq \frac{w^3q^2p^2}{N(N-p-wq)^2} \leq \frac{w^3q^2p}{N(N-p-wq)}.$$

Summing over the above, we reach

$$\Pr[\text{(C-5)}] \leq \frac{4w^3q^2p}{N(N-p-wq)}.$$

The analysis of (C-7) is similar by symmetry, resulting in

$$\Pr[\text{(C-7)}] \leq \frac{4w^3q^2p}{N(N-p-wq)}.$$

Summing over the above yields

$$\begin{aligned}
&\Pr\left[\tau' \in \Theta_{\text{good}}\ (\tau)\right] \leq \sum_{i=1}^{11} \Pr[\text{(B-}i\text{)}] \\
\leq &\frac{w^2q(p+wq)^2}{(N-p-wq)^2} + \frac{2w^2q(p+wq)^2}{N(N-p-wq)} + \frac{w^2qp^2}{N^2} + \frac{8w^3q^2p}{N(N-p-wq)} \\
\leq &\frac{9w^2q(p+wq)^2}{N^2} + \frac{16w^3q^2p}{N^2}.
\end{aligned}$$

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:

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

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

$$\begin{aligned}\mathsf{p}_{\mathrm{re}}(\tau') =& \Pr\Big[\left(\mathbf{k}', \mathcal{S}\right) \xleftarrow{\$} (\{0,1\}^{wn})^4 \times \mathsf{Perm}(n)^4 : \Big((S_1 = S_1^*) \wedge (S_4 = S_4^*) \wedge \\ & (S_2 \vdash \mathcal{Q}_{S_2}^{(1)}) \wedge (S_3 \vdash \mathcal{Q}_{S_3}^{(1)}) \wedge (\mathcal{C}_{\mathbf{k}}^{T}[\mathcal{S}] \vdash \mathcal{Q}'_C) \wedge (\mathbf{k}' = \mathbf{k})\Big)\Big] \quad (14) \\ \mathsf{p}_{\mathrm{mid}}(\tau') =& \Pr\Big[\mathcal{S} \xleftarrow{\$} \mathsf{Perm}(n)^4 : (\mathcal{C}_{\mathbf{k}}^{T}[\mathcal{S}] \vdash \mathcal{Q}'_C) \Big| (S_1 = S_1^*) \wedge (S_4 = S_4^*) \wedge \\ & (S_2 \vdash \mathcal{Q}_{S_2}^{(1)}) \wedge (S_3 \vdash \mathcal{Q}_{S_3}^{(1)})\Big]. \quad (15)\end{aligned}$$

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

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

Therefore,

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

The term B captures the probability that a random extended transcript is good when it is sampled as follows:

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).

Thus, the exact probability of observing the extended transcript τ' is

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

which means

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

and further

$$\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq \Pr\left[\tau' \in \Theta_{\text{good}}\ (\tau)\right] \cdot \min_{\tau' \in \Theta_{\text{good}}(\tau)} \big((N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau')\big). \tag{16}$$

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 $(a,b) \in \mathcal{Q}'_C$. 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*

$$(N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau') \geq 1 - \frac{q^2}{N^w} - \frac{q(2wp + 6w^2q)^2}{N^2}. \tag{17}$$

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 $\mathsf{p}_{\text{mid}}(\tau')/(1/(N^w)_q)$ 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), (16), and (17), 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. (5).

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.,

$$\begin{aligned}\mathsf{SP}_{\mathbf{k}}^T[\mathcal{S}](x) := k_6 \oplus t \oplus \overline{S_6}(k_5 \oplus t \oplus T(\overline{S_5}(k_4 \oplus t \oplus \overline{S_4}(k_3 \oplus t \oplus T(\overline{S_3}(k_2 \oplus t \oplus T(\\ \overline{S_2}(k_1 \oplus t \oplus T(\overline{S_1}(k_0 \oplus t \oplus x)))))))))).\end{aligned} \tag{18}$$

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. (18). If round keys $\mathbf{k} = (k_0, \ldots, k_6)$ are uniform and independent, and T contains no zero entries, then*

$$\mathrm{Adv}_{\mathcal{C}}(p, q) \leq \frac{q^2}{2^{nw}} + \frac{8w^2q(p+wq)^2 + w^2q}{2^n} \tag{19}$$

$$+ \frac{16w^2q(p+wq)(p+wq+3q) + 4w^2q(p+3wq)^2 + w^2q(p+wq)(3p+wq)}{2^{2n}}. \tag{20}$$

Outline of Proof of Theorem 2. 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

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

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

Similar to the 4-round SPN, we will first define what we mean by an extension of the transcript τ. Next, we will define bad extensions and explain the link between good extended transcripts and the ratio $\frac{p_2}{p_1}$. Finally, we will show that the number of bad extended transcripts is small enough, and then show that the probability to obtain any good extension in the real world is sufficiently close to the probability to obtain τ the ideal world. We stress that extended transcripts are completely virtual and are not disclosed to the adversary. They are just an artificial intermediate step to lower bound the probability to observe transcript τ in the real world.

EXTENSION OF A TRANSCRIPT(OUTER FOUR ROUNDS). We will extend the transcript τ of the attack via a certain randomized process. We begin with choosing a pair of keys $(k_0, k_6) \in \mathcal{K}^2$ uniformly at random. Once these keys have been chosen, some construction queries will become involved in collisions. Then a colliding query is defined as a construction query $(t, x, y) \in \mathcal{Q}_C$ such that one of the following conditions holds:

1. there exist an S-box query $(1, u, v) \in \mathcal{Q}_S$ and an integer $i \in \{1, \ldots, w\}$ such that $(x \oplus k_0 \oplus t)[i] = u$.
2. there exist an S-box query $(6, u, v) \in \mathcal{Q}_S$ and an integer $i \in \{1, \ldots, w\}$ such that $(y \oplus k_6 \oplus t)[i] = v$.

We are now going to build a new set $\mathcal{Q}'_{S_{outmost}}$ of S-box evaluations that will play the role of an extension of $\mathcal{Q}_S$. For each colliding query $(t, x, y) \in \mathcal{Q}_C$, we

will add tuples $(1, (x \oplus k_0 \oplus t)[i], v'_1)_{1 \le i \le w}$ (if $(t, x,\ y)$ collides at the input of S_1), or (if (t, x, y) collides at the output of S_6) $(6, u'_6, (y \oplus k_6 \oplus t)[i])_{1 \le i \le w}$, by lazy sampling $v'_1 = S_1((x \oplus k_0 \oplus t)[i])$, or $u'_6 = S_6^{-1}((y \oplus k_6 \oplus t)[i])$, as long as it has not been determined by any existing query in $\mathcal{Q}_S$. Then we choose the key k_1, k_2, k_3, k_4, k_5 uniformly at random. An extended transcript of τ will be defined as a tuple $\tau' = \left(\mathcal{Q}_C, \mathcal{Q}_S, \mathcal{Q}'_{S_{outmost}}, \mathbf{k}\right)$ where $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4, k_5, k_6)$. 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.

Let

$$\mathcal{Q}_{S_1}^{(1)} = \left\{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (1, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_{S_{outmost}}\right\}$$
$$\mathcal{Q}_{S_6}^{(1)} = \left\{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (6, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_{S_{outmost}}\right\}$$

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

$$U_1 = \left\{u_1 \in \{0,1\}^n : (1, u_1, v_1) \in \mathcal{Q}_{S_1}^{(1)}\right\}, \quad V_1 = \left\{v_1 \in \{0,1\}^n : (1, u_1, v_1) \in \mathcal{Q}_{S_1}^{(1)}\right\},$$
$$U_6 = \left\{u_6 \in \{0,1\}^n : (6, u_6, v_6) \in \mathcal{Q}_{S_6}^{(1)}\right\}, \quad V_6 = \left\{v_6 \in \{0,1\}^n : (6, u_6, v_6) \in \mathcal{Q}_{S_6}^{(1)}\right\}$$

be the domains and ranges of $\mathcal{Q}_{S_1}^{(1)}$, $\mathcal{Q}_{S_6}^{(1)}$ respectively. We define two quantities characterizing an extended transcript τ', namely

$$\alpha_1 \stackrel{\text{def}}{=} |\left\{(t, x, y) \in \mathcal{Q}_C : (x \oplus k_0 \oplus t)[i] \in U_1 \text{ for some } i \in \{1, \ldots, w\}\right\}|$$
$$\alpha_6 \stackrel{\text{def}}{=} |\left\{(t, x, y) \in \mathcal{Q}_C : (y \oplus k_6 \oplus t)[i] \in V_6 \text{ for some } i \in \{1, \ldots, w\}\right\}|$$

In words, α_1 (resp. α_6) is the number of queries $(t, x, y) \in \mathcal{Q}_C$ which collide with a query $(u_1, v_1) \in \mathcal{Q}_{S_1}^{(1)}$ (resp. $(u_6, v_6) \in \mathcal{Q}_{S_6}^{(1)}$) in the extended transcript. This corresponds to the number of queries $(t, x, y) \in \mathcal{Q}_C$ which collide with either an original query $(u_1, v_1) \in \mathcal{Q}_{S_1}^{(0)}$ (resp. which collide with a query $(u_6, v_6) \in \mathcal{Q}_{S_6}^{(0)}$) or with a query $(t'x', y') \in \mathcal{Q}_C$ at an input of S_1 (resp. at the output of S_6), once the choice of (k_0, k_6) has been made. We will also denote

$$\beta_i = \left|\mathcal{Q}_{S_i}^{(1)}\right| - \left|\mathcal{Q}_{S_i}^{(0)}\right| = \left|\mathcal{Q}_{S_i}^{(1)}\right| - p.$$

for $i = 1, 6$ the number of additional queries included in the extended transcript.

4.1 Bad Transcript for 6-rounds tweakable linear SPN

Definition 2. *We say an extended transcript τ' is bad if at least one of the following conditions is fulfilled:*

(B-1) there exists $(t,x,y) \in \mathcal{Q}_C, (u_1,v_1) \in \mathcal{Q}_{S_1}^{(1)}, (u_6,v_6) \in \mathcal{Q}_{S_6}^{(1)}$, and index $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0 \oplus t)[i] = u_1$ and $(y \oplus k_6 \oplus t)[j] = v_6$.

(B-2) there exists $(t,x,y) \in \mathcal{Q}_C, (u_1,v_1) \in \mathcal{Q}_{S_1}^{(1)}, (u_2,v_2) \in \mathcal{Q}_{S_2}$, and index $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0 \oplus t)[i] = u_1$ and $(T_1(S_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t))[j] = u_2$.

(B-3) there exists $(t,x,y) \in \mathcal{Q}_C, (u_5,v_5) \in \mathcal{Q}_{S_5}, (u_6,v_6) \in \mathcal{Q}_{S_6}^{(1)}$, and index $i,j \in \{1,\ldots,w\}$ such that $(y \oplus k_6 \oplus t)[j] = v_6$ and $\left(T_5^{-1}\left(S_6^{-1}(y \oplus k_6 \oplus t)\right) \oplus k_5 \oplus t\right)[i] = v_5$.

(B-4) there exists $(t,x,y) \in \mathcal{Q}_C$ and distinct indices $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0 \oplus t)[i] = (x \oplus k_0 \oplus t)[j]$, or $(y \oplus k_6 \oplus t)[i] = (y \oplus k_6 \oplus t)[j]$.

Any extended transcript that is not bad will be called good.

Lemma 7. *One has*

$$\Pr[\tau' \in \Theta_{bad}(\tau)] \leq \frac{3w^2q\left(p+wq\right)^2}{N^2} + \frac{w^2q}{N}. \tag{21}$$

The proof simply follows that of Lemma 7 and thus we omit.

Similar to the outermost two round, we will extend the inner two round (the two and the five round). Pick a pair of S-box (S_1,S_6) such that $S_1 \vdash \mathcal{Q}_{S_1}^{(0)}$ and $S_6 \vdash \mathcal{Q}_{S_6}^{(0)}$, and for each $(t,x,y) \in \mathcal{Q}_C$ we set $a = S_1(x \oplus k_0 \oplus t)$, $b = S_6^{-1}(y \oplus k_6 \oplus t)$. In this way we obtain q tuples of the form (t,a,b); for convenience we denote the set of such induced tuples by $\mathcal{Q}_C^*(S_1,S_6)$. Then we choose a pair of keys $(k_1,k_5) \in \mathcal{K}^2$ uniformly at random. Once these keys have been chosen, some construction queries will become involved in collisions. A colliding query is defined as a construction query $(t,a,b) \in \mathcal{Q}_C^*(S_1,S_6)$. After that, we build a new set $\mathcal{Q}'_{S_{outer}}$ of S-box evaluations that will play the role of an extension of $\mathcal{Q}_S$. Then we choose the key k_2,k_3,k_4 uniformly at random. An extended transcript of τ will be defined as a tuple $\tau'' = \left(\mathcal{Q}_C, \mathcal{Q}_S, \mathcal{Q}'_{S_{outer}}, \mathbf{k}\right)$ where $\mathbf{k} = (k_1,k_2,k_3,k_4,k_5)$. We also let

$$\mathcal{Q}_{S_2}^{(1)} = \left\{(u,v) \in \{0,1\}^n \times \{0,1\}^n : (2,u,v) \in \mathcal{Q}_S \cup \mathcal{Q}'_{S_{outer}}\right\}$$
$$\mathcal{Q}_{S_5}^{(1)} = \left\{(u,v) \in \{0,1\}^n \times \{0,1\}^n : (5,u,v) \in \mathcal{Q}_S \cup \mathcal{Q}'_{S_{outer}}\right\}$$

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

$$U_2 = \left\{u_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}_{S_2}^{(1)}\right\}, \quad V_2 = \left\{v_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}_{S_2}^{(1)}\right\},$$
$$U_5 = \left\{u_5 \in \{0,1\}^n : (5,u_5,v_5) \in \mathcal{Q}_{S_5}^{(1)}\right\}, \quad V_5 = \left\{v_5 \in \{0,1\}^n : (5,u_5,v_5) \in \mathcal{Q}_{S_5}^{(1)}\right\}$$

be the domains and ranges of $\mathcal{Q}_{S_1}^{(1)}$, $\mathcal{Q}_{S_6}^{(1)}$ respectively. After define the extended transcript τ'' is bad,

(F-1) there exists $(t,a,b) \in \mathcal{Q}_C^*(S_1,S_6), (u_2,v_2) \in \mathcal{Q}_{S_2}^{(1)}, (u_5,v_5) \in \mathcal{Q}_{S_5}^{(1)}$, and index $i,j \in \{1,\ldots,w\}$ such that $(T_1(a \oplus k_1 \oplus t))[i] = u_2$ and $(T_5^{-1}(b) \oplus k_5 \oplus t)[j] = v_5$.

(F-2) there exists $(t,a,b) \in \mathcal{Q}_C^*(S_1,S_6), (u_2,v_2) \in \mathcal{Q}_{S_2}^{(1)}, (u_3,v_3) \in \mathcal{Q}_{S_3}$, and index $i,j \in \{1,\ldots,w\}$ such that $(T_1(a \oplus k_1 \oplus t))[i] = u_2$ and

$$(T_2(S_2(T_1(a \oplus k_1 \oplus t)) \oplus k_2 \oplus t))[j] = u_3.$$

(F-3) there exists $(t,a,b) \in \mathcal{Q}_C^*(S_1,S_6), (u_4,v_4) \in \mathcal{Q}_{S_4}, (u_5,v_5) \in \mathcal{Q}_{S_5}^{(1)}$, and index $i,j \in \{1,\ldots,w\}$ such that $(T_5^{-1}(b) \oplus k_5 \oplus t)[j] = v_5$ and

$$\left(T_4^{-1}\left(S_5^{-1}\left(T_5^{-1}(b) \oplus k_5 \oplus t\right)\right) \oplus k_4 \oplus t\right)[i] = v_4.$$

(F-4) there exists $(t,x,y) \in \mathcal{Q}_C$ and distinct indices $i,j \in \{1,\ldots,w\}$ such that

$$(T_1(a \oplus k_1 \oplus t))[i] = (T_1(a \oplus k_1 \oplus t))[j], \text{ or}$$

$$(T_5^{-1}(b) \oplus k_5 \oplus t)[i] = (T_5^{-1}(b) \oplus k_5 \oplus t)[j].$$

Lemma 11 *One has*

$$\Pr[\tau'' \in \Theta_{bad}(\tau)] \leq \frac{w^2q(p+wq)(3p+wq)}{N^2} + \frac{w^2q}{N}. \tag{22}$$

The proof is similar to Lemma 10.

Let $\tau_1 = \tau' \cup \tau''$. Then combine (11), (12), we can get

$$\Pr[\tau_1 \in \Theta_{bad}(\tau)] \leq \frac{2w^2q(p+wq)(3p+wq)}{N^2} + \frac{2w^2q}{N}. \tag{23}$$

4.2 Analysis for Good Transcript

Fix a good transcript and a good round-key vector k, we are to derive a lower bound for the probability $\Pr\left[\mathcal{S} \xleftarrow{\$} (\mathcal{S}(n))^6 : \mathrm{SP}_k[\mathcal{S}] \vdash \mathcal{Q}_C | \mathcal{S} \vdash \mathcal{Q}_S\right]$. We "peel off" the outer four rounds. Then assuming (S_1,S_2,S_5,S_6) is good, we analyze the induced 2-round transcript to yield the final bounds.

PEELING OFF THE OUTER FOUR ROUNDS. Pick a pair of S-box (S_1,S_2,S_5,S_6) such that $S_1 \vdash \mathcal{Q}_{S_1}^{(0)}, S_2 \vdash \mathcal{Q}_{S_2}^{(0)}, S_5 \vdash \mathcal{Q}_{S_5}^{(0)}$ and $S_6 \vdash \mathcal{Q}_{S_6}^{(0)}$, and for each $(t,a,b) \in \mathcal{Q}_C^*(S_1,S_6)$ we set $c = S_2(T_1(a \oplus k_1 \oplus t))$, $d = S_5^{-1}\left(T_5^{-1}(b) \oplus k_5 \oplus t\right)$. In this way we obtain q tuples of the form (c,d); for convenience we denote the

set of such induced tuples by $\mathcal{Q}_C^{**}(S_2, S_5)$. Similarly, we also extended the innermost two rounds:

Then we build a new set $\mathcal{Q}'_{S_{inner}}$ of S-box evaluations that will play the role of an extension of $\mathcal{Q}_C^{**}(S_2, S_5)$. Then we choose the key k_3 uniformly at random. An extended transcript of τ_{inner} will be defined as a tuple $\tau'_{inner} = \left(\mathcal{Q}_C^{**}(S_2, S_5), \mathcal{Q}_{S_{inner}}, \mathcal{Q}'_{S_{inner}}, \mathbf{k}\right)$ where $\mathbf{k} = (k_2, k_3, k_4)$.

Lemma 12 *For any extended $S_1 \vdash \mathcal{Q}_{S_1}, S_2 \vdash \mathcal{Q}_{S_2}, S_5 \vdash \mathcal{Q}_{S_5}, S_6 \vdash \mathcal{Q}_{S_6}$, we have*

$$\Pr\left[\mathrm{Bad}\left(S_1, S_2, S_5, S_6\right) | S_i \vdash \mathcal{Q}_{S_i}, i = 1, 2, 5, 6\right] \geq \frac{2w^2q^2(p+wq)}{(N-p-wq)\cdot(N-p)} + \frac{2w^2q(p+wq)(p+wq+2q)}{N\cdot(N-p)} + \frac{w^2q(p+wq)(p+wq+2q)}{(N-p)^2} + \frac{2w^2q(p+wq)^2}{(N-p)}. \tag{24}$$

Proof: Then we define a predicate $\mathrm{Bad}\left(S_1, S_2, S_5, S_6\right)$ on the pair (S_1, S_2, S_5, S_6), which holds if the corresponding induced set $\mathcal{Q}_C^{**}(S_2, S_5)$ fulfills at least one of the following seven "collision" conditions:

(H-1) there exist $(t, c, d) \in \mathcal{Q}_C^{**}(S_2, S_5)$, $i, j \in \{1, \ldots, w\}$, $u_3 \in U_3$ and $v_4 \in V_4$ such that $\left(T_2\left(c \oplus k_2 \oplus t\right)\right)[i] = u_3$ and $\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)[i] = v_4$.

(H-2) there exist $(t, c, d) \in \mathcal{Q}_C^{**}(S_2, S_5)$, $i, j \in \{1, \ldots, w\}$, $u_3 \in U_3$ and $u_4 \in U_4$ such that $\left(T_2\left(c \oplus k_2 \oplus t\right)\right)[i] = u_3$ and $\left(T_3\left(S_3\left(T_2\left(c \oplus k_2 \oplus t\right)\right) \oplus k_3 \oplus t\right)\right)[j] = u_4$.

(H-3) there exist $(t, c, d) \in \mathcal{Q}_C^{**}(S_2, S_5)$, $i, j \in \{1, \ldots, w\}$, $v_3 \in V_3$ and $v_4 \in V_4$ such that $\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)[i] = v_4$ and $\left(T_3^{-1}\left(S_4^{-1}\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)\right) \oplus k_3 \oplus t\right)[j] = v_3$.

(H-4) there exist $(t, c, d) \in \mathcal{Q}_C^{**}(S_2, S_5)$, distinct $i, i' \in \{1, \ldots, w\}$, $u_3, u'_3 \in U_3$ such that

$$\left(T_2\left(c \oplus k_2 \oplus t\right)\right)[i] = u_3, \text{ and } \left(T_2\left(c \oplus k_2 \oplus t\right)\right)[i'] = u'_3.$$

(H-5) there exist distinct $(t, c, d), (t', c', d') \in \mathcal{Q}_C^{**}(S_2, S_5)$, distinct $i, i' \in \{1, \ldots, w\}$, $u_3 \in U_3$ such that

$$\left(T_2\left(c \oplus k_2 \oplus t\right)\right)[i] = u_3, \text{ and } \left(T_2\left(c \oplus k_2 \oplus t\right)\right)[i'] = \left(T_2\left(c' \oplus k_2 \oplus t'\right)\right)[i'].$$

(H-6) there exist $(t, c, d), (t', c', d') \in \mathcal{Q}_C^{**}(S_2, S_5)$, $i, i', j, j' \in \{1, \ldots, w\}$, with$(t, c, j) \neq (t', c', j')$, $u_3, u'_3 \in U_3$ such that $\left(T_2\left(c \oplus k_2 \oplus t\right)\right)[i] = u_3$, $\left(T_2\left(c' \oplus k_2 \oplus t'\right)\right)[i] = u'_3$ and

$$\left(T_3\left(S_3\left(T_2\left(c \oplus k_2 \oplus t\right)\right) \oplus k_3 \oplus t\right)\right)[j] = \left(T_3\left(S_3\left(T_2\left(c' \oplus k_2 \oplus t'\right)\right) \oplus k_3 \oplus t'\right)\right)[j'].$$

(H-7) there exist $(t, c, d) \in \mathcal{Q}_C^{**}(S_2, S_5)$, distinct $j, j' \in \{1, \ldots, w\}$, $v_4, v'_4 \in V_4$ such that

$$\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)[j] = v_4,$$
$$\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)[j'] = v_4.$$

(H-8) there exist distinct $(t,c,d),(t',c',d') \in \mathcal{Q}_C^{**}(S_2,S_5)$, distinct $j,j' \in \{1,\ldots,w\}$, $v_4 \in V_4$ such that

$$\begin{aligned}&\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)[j] = v_4,\\ &\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)[j] = \left(T_4^{-1}(d') \oplus k_4 \oplus t'\right)[j'].\end{aligned}$$

(H-9) there exist $(t,c,d),(t',c',d') \in \mathcal{Q}_C^{**}(S_2,S_5)$, $i,i',j,j' \in \{1,\ldots,w\}$, with$(t,d,j) \neq (t',d',j')$, $u_3 \in U_3$, $v_4, v_4' \in V_4$ such that

$$\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)[i] = v_4, \text{ and } \left(T_4^{-1}(d') \oplus k_4 \oplus t'\right)[i] = v_4'.$$

$$\begin{aligned}&\left(T_3^{-1}\left(S_4^{-1}\left(T_4^{-1}(d) \oplus k_4 \oplus t\right)\right) \oplus k_3 \oplus t\right)[j]\\ &= \left(T_3^{-1}\left(S_4^{-1}\left(T_4^{-1}(d') \oplus k_4 \oplus t'\right)\right) \oplus k_3 \oplus t'\right)[j'].\end{aligned}$$

Proof: We upper bound the probabilities of the nine conditions in turn. We denote Θ_i the set of attainable transcripts satisfying condition (H-i).

The proof of (H-1) to (H-5) and (H-7), (H-8) is similar to the Lemma 8, there are no more details. So we just consider (H-6) and (H-9) here. We first note that, if the condition is satisfied, we have $(S_2(a \oplus k_1 \oplus t))[i]$ remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_2} \cup \mathcal{Q}_{S_5} \cup \mathcal{Q}_{S_6})$. Moreover if $u_3 = u_3'$, that is $c \oplus t = c' \oplus t'$, then after oplus different tweak, the input of the S_4 must be different, so the collision would not happen. Hence we must have $u_3 \neq u_3'$. The condition can be divided into two conditions: the first concerning with $j \neq j'$, while the second concerning with $j = j'$.

For the first case, to make

$$(T_3(S_3(T_2(c \oplus k_2 \oplus t)) \oplus k_3 \oplus t))[j] = (T_3(S_3(T_2(c' \oplus k_2 \oplus t')) \oplus k_3 \oplus t'))[j'].$$

achieved, we just leverage the fact that $k_3[j]$ and $k_3[j']$ are uniform and independent, so the collision holds with probability $1/N$. Because of $a$remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_2} \cup \mathcal{Q}_{S_5} \cup \mathcal{Q}_{S_6})$, let (a',b') be the unique query such that the collision happened. Then the probability that $(T_2(c \oplus k_2 \oplus t))[i] = u_3, (T_2(c' \oplus k_2 \oplus t'))[i] = u_3'$ is at most $\frac{1}{N-p}$, because we have at most $w^2q^2(p+wq)$ such tuples, one has

$$\Pr[\tau_{inner} \in \Theta_6] \leq \frac{w^2q^2(p+wq)}{N \cdot (N-p)}.$$

For the case of $j = j'$ with distinct $(c,d),(c',d')$, that is there is only one index has different value of input and output. Because of the value $S_2(T_1(a' \oplus k_1 \oplus t))[i]$ also remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_2} \cup \mathcal{Q}_{S_5} \cup \mathcal{Q}_{S_6})$, then we leverage the randomness due to lazy sampling $S_3(T_2(c \oplus k_2 \oplus t))$. Conditioned on (F-4), for $i'' \neq i$, the value $T_2(c \oplus k_2 \oplus t)[i'']$ "does not collide with" pairs in $\mathcal{Q}_{S_3}^{(1)}$, and will be assigned a random outputs during the lazy sampling process. Simultaneously conditioned on (F-5), for distinct $i'' \neq i$, if $(T_2(c \oplus k_2 \oplus t))[i] = u_3$, it holds $(T_2(c \oplus k_2 \oplus t))[i''] \neq (T_2(c' \oplus k_2 \oplus t'))[i'']$. Since T_3 contain no zero entries, so the

value $(T_3\,(S_3\,(T_2\,(c \oplus k_2 \oplus t)) \oplus k_3 \oplus t))\,[i'']$ could not be disturbed by the value of $(T_3\,(S_3\,(T_2\,(c' \oplus k_2 \oplus t')) \oplus k_3 \oplus t'))\,[i'']$ and thus uniform in at least $\frac{1}{N-p-wq}$. One has,

$$\Pr\left[\tau_{inner} \in \Theta_6\right] \leq \frac{w^2q^2(p+wq)}{(N-p-wq)\cdot(N-p)}.$$

So, combine these two subevents, one has

$$\Pr\left[\tau_{inner} \in \Theta_6\right] \leq \frac{w^2q^2(p+wq)}{N\cdot(N-p)} + \frac{w^2q^2(p+wq)}{(N-p-wq)\cdot(N-p)}.$$

Similarly, we have

$$\Pr\left[\tau_{inner} \in \Theta_9\right] \leq \frac{w^2q^2(p+wq)}{N\cdot(N-p)} + \frac{w^2q^2(p+wq)}{(N-p-wq)\cdot(N-p)}.$$

Then combining Lemma 9, we complete the proof of Theorem 2.

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.