IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2020, No. 3, pp. 305–326. DOI:10.13154/tosc.v2020.i3.305-326

Beyond-Birthday-Bound Security for 4-round Linear Substitution-Permutation Networks

Yuan Gao[1,2], Chun Guo[1,2,3](✉), Meiqin Wang[1,2],
Weijia Wang[1,2,3] and Jiejing Wen[1,2](✉)

[1] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, 266237, China, gaoyuanwangan@mail.sdu.edu.cn, chun.guo@sdu.edu.cn, mqwang@sdu.edu.cn, wjwang@sdu.edu.cn, jjwen@sdu.edu.cn

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

[3] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract. Recent works of 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.

In this paper, we overcome this birthday barrier and prove that a 4-round SPN with linear diffusion layers and independent round keys is secure up to $2^{2n/3}$ queries. For this, we identify conditions on the linear layers that are sufficient for such security, which, unsurprisingly, turns out to be slightly stronger than Cogliati et al.'s conditions for birthday security. These provides additional theoretic supports for real world SPN blockciphers.

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

1 Introduction

Modern blockciphers roughly fall into two classes (with some rare exceptions such as IDEA [LM91] and KATAN [DDK09]), namely *Feistel networks and their generalizations*, and *substitution-permutation networks* (SPNs). A Feistel round applies a domain-preserving function on half of the data, and then executes XOR and swap operations. This paradigm may be generalized to using compression functions, expansion functions, and smaller functions. Popular examples include many blockcipher standards such as DES [oS77], GOST [GOS89], and Camellia [ISO16]. On the other hand, the latter paradigm 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. *Substitution step*: break down the wn-bit state into w disjoint chunks of n bits, and evaluate an S-box on each chunk;

2. *Permutation step*: apply a keyed permutation to the whole wn-bit state (which is also applied to the plaintext before the first round).

Received: 2020-06-01 Accepted: 2020-08-01 Published: 2020-09-28

S-boxes are typically highly non-linear, and, in fact, serve as the only source of non-linearity in many blockciphers. There is no a priori restriction on the (non-)linearity of the *Permutation step*, and the use and advantages of non-linear permutations was recently explored [LRL18]. Though, modern blockciphers still tend to use linear or affine mappings for the *Permutation step* [Bir11], which involves a simple key-mixing step followed by an invertible linear or affine transformation. More precisely, their permutation steps are *linear* or affine with respect to additions on GF(2^n), where n is the size of the S-box. Various popular blockciphers including the AES [DR02], Serpent [ABK98], and the ISO/IEC lightweight standard PRESENT [BKL$^+$07] follow this approach. Furthermore, a subset of them using maximum distance separable linear transformations allows for effective provable security against certain types of attacks [DR01, PSC$^+$02, PSLL03, MV15, SLG$^+$16].

The traditional security notion for blockciphers is (strong) pseudorandomness: for any adversary with reasonable resources, the blockcipher with *a random and secret key* should be indistinguishable from a truly random permutation. Proving such security for concrete blockciphers such as AES seems out of the reach of current techniques. The usual approach is to idealize some underlying primitives and prove that the high-level structure is sound, in the sense of being a strong pseudorandom permutation (SPRP) or others. Typically, to prove security for Feistel networks, the Feistel round functions are idealized, resulting in schemes such as the seminal Luby-Rackoff model [LR88, MP03, Pat03, Pat04, HR10, CHK$^+$16]. To prove security for SPNs, the "S-boxes" may be idealized as secret random functions or permutations, leaving the permutation layers as efficient "non-cryptographic" functions [IK01, MV15]. In this case, the S-boxes act as the only source of cryptographic hardness, while the permutation layers only supply auxiliary *combinatorial* properties. This limits the provable security to the domain-size of the S-boxes, which is unfortunately as small as 8 bits in, e.g., the AES. Consequently, provable results on SPNs do not relate to any concrete SPN-based block ciphers. Instead, they should be viewed as theoretical support for the SPN approach to constructing blockciphers.[1]

Recently, initiated by Dodis et al. [DSSL16, DKS$^+$17], a series of works investigated a new model of SPNs, in which the S-boxes are small *public* ideal primitives and the permutation layers remain non-cryptographic. In detail, it was [DSSL16] that for the first time investigated the *indifferentiability* [MRH04] of confusion-diffusion networks or keyless SPN models combining public random S-boxes and non-cryptographic permutation layers. It was also [DSSL16] that for the first time confirmed (in a widely recognized theoretical model) that, the use of non-linear permutation layers ensures more security than linear ones. The SPRP security of *keyed* SPN models has to be deferred to later in [DKS$^+$17, CDK$^+$18]. In detail, regarding the (more common) SPN model with linear permutation layers, Dodis et al. [DKS$^+$17] exhibited a chosen-ciphertext boomerang attack against 2 rounds using only 4 queries. On the positive side, they proved that 3 rounds ensure the classical birthday-bound security, i.e., security up to $2^{n/2}$ adversarial queries, where n is the size of the idealized S-boxes. These characterized its SPRP security. To ensure this birthday-bound security, the linear permutation layers shall satisfy a quite mild condition of "zero-freeness", meaning that all entries in the matrix representations of the linear permutation layers and their inverses shall be non-zero.

Regarding the SPN model with non-linear permutation layers, Dodis et al. [DKS$^+$17] identified a combinatorial property on the permutations that suffices for security in this case, named blockwise universality. Informally, a keyed permutation π_k is blockwise universal if, for any distinct inputs x, x' and any constant c, the probability (taken over uniform k) of each of the following events is low: (i) a block of $\pi(k, x)$ is equal to a block of $\pi(k, x')$, (ii) two different blocks of $\pi(k, x)$ are equal, (iii) a block of $\pi(k, x)$ is equal to c. Using such non-linear permutations, they showed that even one round is already

[1] Similar limitation exists in Feistel schemes, though it appears more acceptable, being, e.g., 32 bits in DES.

sufficient for birthday-bound. Later, Cogliati and Lee improved this result by: (i) adding *tweaks* into the non-linear transformations to obtain *tweakable non-linear SPNs*, and (ii) proving beyond-birthday-bound results [CL18]. They showed that two rounds of such tweakable non-linear SPNs are secure tweakable blockciphers [LRW11] up to roughly $2^{2n/3}$ adversarial queries. They also provided a (non-tight) asymptotic security bound improving as the number of rounds grows.

1.1 Our Results

As briefed before, with more than two rounds, non-linear SPNs could ensure beyond-birthday-bound security. Though, practitioners prefer linear SPNs, the security of which is only proved up to birthday-bound at 3 rounds. Observing this gap, we ask whether it is possible to achieve security beyond the birthday barrier with linear SPN structures. For this, 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 well investigated (see the related works below). For such linear SPNs, we answer our main question positively and prove the first beyond-birthday-bound (BBB) $2n/3$-bit security result on 4 rounds.

Concretely, we first characterize conditions on the linear layers that are sufficient for $2n/3$-bit security. For a linear transformation T to meet this, it has to be "zero-free" in the aforementioned sense. In addition, in both T and T^{-1}, the sum of every 2 entries from the same row shall be non-zero. Thus, the conditions are slightly stronger than that for birthday-bound, and may be viewed as a second order extension of the aforementioned "zero-freeness" condition.

With this, we show that a 4-round linear SPN is beyond-birthday-bound secure, if: (i) 4 independent public random S-boxes are used in the four rounds respectively, and (ii) such a "second order zero-free" linear permutation layer is used in every round, and (iii) the round keys are uniform and independent. Our proof employs the H-coefficient technique [Pat09]. Moreover, we prove the notion of *point-wise proximity* [HT16], thus establishing $2n/3$-bit *multi-user security* for 4-round linear SPNs as well. We refer to Table 1 for the position of our result.

Our proof crucially relies on a technical lemma of Cogliati and Lee [CL18] on two SPN rounds. In some sense, in our 4-round linear SPNs, the 1st and 4th round play similar role as the so-called blockwise universal permutations in the 2-round non-linear SPNs of Cogliati and Lee. The situation somewhat resembles that of tweakable Even-Mansour ciphers [CLS15, CS15]. See Section 3 for details.

Interpretation. We view our result as extending a sound theory for constructing ciphers from small S-boxes and providing additional theoretical support for the SPN approach (particularly for the real world "linear SPNs"). As mentioned before, the n-bit idealized S-boxes are the only cryptographic hardness in the current SPN models with non-cryptographic permutation layers, and this enforces the inherent "2^n provable barrier". Neither this 2^n bound nor our inferior $2^{2n/3}$ bound (though improved upon $2^{n/2}$ of [CDK+18]) is meaningful for regular SPN blockciphers, in which very low values of n are typically chosen for the S-boxes. For example, the S-box of the AES is based on the inverse of GF(2^8), and has $n = 8$. Though, this series of theoretic results should be viewed as important complementary to the more coarse iterated Even-Mansour model [BKL+12].

On the other hand, as provable security (mostly against differential and linear properties) of the ARX ciphers advances, recent works have put forward practical choices of 11- [BDMD+20] or even 64-bit [BBdS+19] bigger S-boxes. The bound becomes more meaningful with such parameters.

Table 1: Summary of provable result on SP-Networks. The first column presents the number of rounds in the model. The second column indicates how many S-boxes are used in the model & whether they are secret or public. Regarding security, PRF, PRP, SPRP, and TSPRP (tweakable strong pseudorandom permutation) indicate the security model, su and mu indicates if it's in the single- or multi-user setting, while the header term indicates the concrete provable bounds. We remark that concrete security was not the focus of [MV15].

Rounds	S-boxes	Permutation layers	Security	Ref.
1	1 public	Non-linear	$n/2$, su TSPRP	[CDK+18]
2	2 public	Non-linear	$2n/3$, mu TSPRP	[CL18]
$2t$	$2t$ public	Non-linear	$\frac{tn}{t+1}$, mu TSPRP	[CL18]
3	3 secret	Linear, Serpent-like	$n/2$, su PRP	[IK01]
3	1 public	Linear, "zero-free"	$n/2$, su SPRP	[DKS+17]
t	t secret	Linear, "zero-free"	$n/3$, su PRF	[MV15]
4	4 public	Linear, "2nd order zero-free"	**$\mathbf{2n/3}$, mu SPRP**	**Sect. 3**

1.2 Other Related Work

Here we survey some other related works besides the aforementioned ones on SPNs with *public* S-boxes [DSSL16, DKS+17, CL18, CDK+18]. First, when $w = 1$,

- Linear SPNs collapse to the iterated Even-Mansour construction, the SPRP security of which was first studied in [EM97] and subsequently extended to multiple rounds [BKL+12, Ste12, LPS12, CS14, CLL+18, HT16] and multi-user setting [HT16]. In detail, with t rounds, the n-bit iterated Even-Mansour cipher is tightly secure up to $2^{\frac{tn}{t+1}}$ adversarial queries [BKL+12, CS14, HT16];

- Non-linear tweakable SPNs collapse to *tweakable Even-Mansour ciphers* with non-linear tweaking functions [CLS15] (with follow-ups such as [CS15, GJMN16, Men16]).

Provable security of the earlier non-linear SPN models with *secret, key-dependent S-boxes* were (partly) addressed by Naor and Reingold [NR99], Chakraborty and Sarkar [CS06], and Halevi [Hal07]. Security of linear SPN models with such secret S-boxes were proved by Iwata and Kurosawa [IK01], though for specific permutation layers and birthday-bound security only. Subsequently, Miles and Viola [MV15] proved chosen-plaintext security for linear SPNs with PRF S-boxes, "zero-free" permutations, and more than 2 rounds.

Finally, on the cryptanalytic side, attacks against SPNs could be found in [Jou03, HR04, BS10, BBK14, BK15, BK15], while provable security has been addressed by [DR01, PSC+02, PSLL03, MV15] against differential/linear cryptanalysis and [SLG+16] against others such as impossible differential attacks, etc. In addition, it was shown in [LRL18] that the use of non-linear permutation layers may indeed increase security against differential/linear attacks.

2 Preliminaries

Throughout this work, we fix positive integers w and n, and let $N = 2^n$. Let $\mathbb{F} := \mathrm{GF}(2^n)$, which is identified with $\{0,1\}^n$. 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. For an integer $m \geq 1$, the set of all permutations on $\{0,1\}^m$ will be denoted $\mathsf{Perm}(m)$.

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, an r-round SPN taking inputs of length wn is defined by $r+1$ round keys $\mathbf{k} = (k_0, k_1, \ldots, k_r) \in (\{0,1\}^{wn})^{r+1}$, r permutations $S_1, \ldots, S_r : \{0,1\}^n \to \{0,1\}^n$, and an invertible linear permutation $T \in \mathbb{F}^{w\times w}$. Define

$$\overline{S_i}(x[1] \oplus k_{i-1}[1] \| \ldots \| x[w] \oplus k_{i-1}[w]) \overset{\text{def}}{=} S_i(x[1] \oplus k_{i-1}[1]) \| \ldots \| S_i(x[w] \oplus k_{i-1}[w]).$$

Then, given an input $x \in \{0,1\}^{wn}$, the output of the SPN $\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}]$ is computed as follows:

- Let $x_1 := x$.
- For $i = 1$ to $r-1$ do:
  1. $y_i := \overline{S_i}(x_i \oplus k_{i-1})$.
  2. $x_{i+1} := T \cdot y_i$.
- $x_{r+1} := \overline{S_r}(x_r \oplus k_{r-1}) \oplus k_r$.
- The output is x_{r+1}.

Note that this model matches the structure of popular SPN ciphers such as the AES, Serpent, and PRESENT. Also note that our model follows [CDK+18, Sect. 4.2] and uses different S-boxes in different rounds. We remark that some other [CDK+18, Sect. 3] assumed the same S-box in every round. Finally, we refer to [DKS+17, Sect. 2.1] for a more general model of SPNs and its connection to the above model.

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

In the multi-user setting, let ℓ denote the number of users. In the real world, ℓ secret keys $\mathbf{k}_1, \ldots, \mathbf{k}_\ell \in (\{0,1\}^{wn})^{r+1}$ 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 permutations $\mathcal{P} = (P_1, \ldots, P_\ell) \in \text{Perm}(wn)^\ell$ 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 $(P_1, \ldots, P_\ell, \mathcal{S})$ 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

$$\begin{aligned}\text{Adv}^{\text{mu}}_{\mathsf{SP}^T}(\mathcal{D}) = \Pr&\left[P_1, \ldots, P_\ell \xleftarrow{\$} \mathsf{Perm}(wn)^\ell, \mathcal{S} \xleftarrow{\$} \mathsf{Perm}(n)^r : 1 \leftarrow \mathcal{D}^{\mathcal{S}, P_1, \ldots, P_\ell}\right] \\ - \Pr&\left[\mathbf{k}_1, \ldots, \mathbf{k}_\ell \xleftarrow{\$} \left((\{0,1\}^{wn})^{r+1}\right)^\ell, \mathcal{S} \xleftarrow{\$} \text{Perm}(n)^r : 1 \leftarrow \mathcal{D}^{\mathcal{S}, \mathsf{SP}^T_{\mathbf{k}_1}[\mathcal{S}], \ldots, \mathsf{SP}^T_{\mathbf{k}_\ell}[\mathcal{S}]}\right].\end{aligned}$$

For $p, q > 0$, we define

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

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 ℓ outer permutations in total (thus $\ell \le q$). In the single-user setting with $\ell = 1$, $\text{Adv}^{\text{mu}}_{\mathsf{SP}^T}(\mathcal{D})$ and $\text{Adv}^{\text{mu}}_{\mathsf{SP}^T}(p, q)$ will also be written as $\text{Adv}^{\text{su}}_{\mathsf{SP}^T}(\mathcal{D})$ and $\text{Adv}^{\text{su}}_{\mathsf{SP}^T}(p, q)$, respectively.

The H-coefficient technique. Suppose that a distinguisher $\mathcal{D}$ makes p queries to each of the S-boxes, and in 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

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

for $j = 1, ..., \ell$, where q_j is the number of queries made to C_j and $(j, x_{j,i}, y_{j,i})$ represents the evaluation obtained by the ith query to C_j. So according to the instantiation, it implies either $\mathsf{SP}^T_{\mathbf{k}_j}[\mathcal{S}](x_{j,i}) = y_{j,i}$ or $P_j(x_{j,i}) = y_{j,i}$. 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 and does not make 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 $\mathbf{k} \in (\{0,1\}^{wn})^{r+1}$, a permutation $P \in \mathsf{Perm}(wn)$, 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 $\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}](x_{j,i}) = y_{j,i}$ (resp. $P(x_{j,i}) = y_{j,i}$) for every $i = 1, ..., q_j$, then we will write $\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_{C_j}$ (resp. $P \vdash \mathcal{Q}_{C_j}$).

Let $\mathbf{k}_1, \ldots, \mathbf{k}_\ell \in \left((\{0,1\}^{wn})^{r+1}\right)^\ell$ and $\mathcal{P} = (P_1, \ldots, P_\ell) \in \mathsf{Perm}(wn)^\ell$, if $\mathsf{SP}^T_{\mathbf{k}_j}[\mathcal{S}] \vdash \mathcal{Q}_{C_j}$ (resp. $P_j \vdash \mathcal{Q}_{C_j}$) 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. $P \vdash \mathcal{Q}_C$). If there exist $\mathcal{P} \in \mathsf{Perm}(wn)^\ell$ and $\mathcal{S} \in \mathsf{Perm}(\underline{n})^r$ 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 $\mathcal{P} \in \mathsf{Perm}(wn)^\ell$ and $\mathcal{S} \in \mathsf{Perm}(n)^r$ such that $\mathcal{P} \vdash \mathcal{Q}_C$ and $\mathcal{S} \vdash \mathcal{Q}_S$. For an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, let

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

$$\mathsf{p}_2(\tau) = \Pr\left[\mathbf{k}_1, \ldots, \mathbf{k}_\ell \xleftarrow{\$} \left((\{0,1\}^{wn})^{r+1}\right)^\ell, \mathcal{S} \xleftarrow{\$} \mathsf{Perm}(n)^r : (\mathsf{SP}^T_{\mathbf{k}_j}[\mathcal{S}])_j \vdash \mathcal{Q}_C \bigwedge \mathcal{S} \vdash \mathcal{Q}_S\right].$$

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

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

$$\mathsf{p}_2(\tau) \ge (1-\varepsilon)\mathsf{p}_1(\tau). \tag{2}$$

Then one has

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

The lower bound (2) 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 [HT16].

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

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

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

$$\mathsf{p}_2(\tau) \geq (1 - 2\varepsilon(p + wq, q))\mathsf{p}_1(\tau).$$

3 Beyond-Birthday-Bound Security for 4-Round SPNs

Concretely, let $\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}]$ be the 4-round SPN using any linear transformations T. I.e.,

$$\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}](x) := \oplus_{k_4} \circ \overline{S_4} \circ \oplus_{k_3} \circ T \circ \overline{S_3} \circ \oplus_{k_2} \circ T \circ \overline{S_2} \circ \oplus_{k_1} \circ T \circ \overline{S_1} \circ \oplus_{k_0}(x), \tag{3}$$

where $\oplus_{k_i}$ is the operation of xoring with the wn-bit round-key k_i, and $\circ$ stands for function composition. We define good linear transformations to characterize their properties that are sufficient for $2n/3$-bit security.

Definition 1. We say that a linear transformation

$$T = \begin{pmatrix} t_{1,1} & t_{1,2} & \cdots & t_{1,w} \\ t_{2,1} & t_{2,2} & \cdots & t_{2,w} \\ \vdots & \vdots & \ddots & \vdots \\ t_{w,1} & t_{w,2} & \cdots & t_{w,w} \end{pmatrix}, \qquad T^{-1} = \begin{pmatrix} t'_{1,1} & t'_{1,2} & \cdots & t'_{1,w} \\ t'_{2,1} & t'_{2,2} & \cdots & t'_{2,w} \\ \vdots & \vdots & \ddots & \vdots \\ t'_{w,1} & t'_{w,2} & \cdots & t'_{w,w} \end{pmatrix},$$

is *good*, if:

1. T contains no zero entries, i.e., $t_{i,j} \neq 0$ for all $i, j \in \{1, \ldots, w\}$, and
2. No row of T contains redundant entries, i.e., for every i, $t_{i,j} \neq t_{i,j'}$ for all distinct indices $j, j' \in \{1, \ldots, w\}$; and
3. T^{-1} contains no zero entries, i.e., $t'_{i,j} \neq 0$ for all $i, j \in \{1, \ldots, w\}$, and
4. No row of T^{-1} contains redundant entries, i.e., for every i, $t'_{i,j} \neq t'_{i,j'}$ for all distinct indices $j, j' \in \{1, \ldots, w\}$.

The 1st and 3rd conditions are also required for the birthday security of 3-round linear SPNs [DKS+17, Sect. 3]. As mentioned in the Introduction, the 2nd and 4th conditions can be seen as a "second order" extension of the 1st and 3rd ones. To justify the soundness of this definition, we list several candidates in Appendix A. Using such a good linear transformation T and uniform and independent round keys, SP^T is beyond-birthday-bound secure.

Theorem 1. *Assume $w \geq 2$, and $p + wq \leq N/2$. Let $\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}]$ be a 4-round, linear SPN as defined by Eq. (3). If the round keys $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4)$ are uniform and independent, and T is good as per Definition 1, then*

$$\mathrm{Adv}^{\mathrm{su}}_{\mathsf{SP}^T}(p,q) \leq \frac{3w^4q^2(p+2wq)}{N^2} + \frac{9w^2q(p+3wq)^2}{N^2} + \frac{q^2}{N^w},$$

$$\mathrm{Adv}^{\mathrm{mu}}_{\mathsf{SP}^T}(p,q) \leq \frac{6w^4q^2(p+3wq)}{N^2} + \frac{18w^2q(p+4wq)^2}{N^2} + \frac{2q^2}{N^w}.$$

The proof of Theorem 1 relies on the following point-wise proximity result 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*

$$\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq 1 - \frac{3w^4q^2(p+2wq)}{N^2} - \frac{9w^2q(p+3wq)^2}{N^2} - \frac{q^2}{N^w}. \tag{4}$$

3.1 Terminology, and 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 by $\mathcal{D}$. As we focus on the single-user setting, we drop the user indices from Eq. (1) and assume $\mathcal{Q}_C = (x_i, y_i)_{1 \leq i \leq q}$. Then, let

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

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

$$U^{(0)}_1 = \left\{u_1 \in \{0,1\}^n : (1,u_1,v_1) \in \mathcal{Q}^{(0)}_{S_1}\right\}, \quad V^{(0)}_1 = \left\{v_1 \in \{0,1\}^n : (1,u_1,v_1) \in \mathcal{Q}^{(0)}_{S_1}\right\},$$
$$U^{(0)}_2 = \left\{u_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}^{(0)}_{S_2}\right\}, \quad V^{(0)}_2 = \left\{v_2 \in \{0,1\}^n : (2,u_2,v_2) \in \mathcal{Q}^{(0)}_{S_2}\right\},$$
$$U^{(0)}_3 = \left\{u_3 \in \{0,1\}^n : (3,u_3,v_3) \in \mathcal{Q}^{(0)}_{S_3}\right\}, \quad V^{(0)}_3 = \left\{v_3 \in \{0,1\}^n : (3,u_3,v_3) \in \mathcal{Q}^{(0)}_{S_3}\right\},$$
$$U^{(0)}_4 = \left\{u_4 \in \{0,1\}^n : (4,u_4,v_4) \in \mathcal{Q}^{(0)}_{S_4}\right\}, \quad V^{(0)}_4 = \left\{v_4 \in \{0,1\}^n : (4,u_4,v_4) \in \mathcal{Q}^{(0)}_{S_4}\right\}.$$

3.1.1 Extending the transcripts

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 [CDK+18, 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 first extended in the following manner:

- At the end of the interaction between $\mathcal{D}$ and the real world $(\mathcal{S}, \mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}])$, 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 $(x, y, a, b) \in \mathcal{Q}'_C$ that fulfills any of the following conditions:

1. there exists an index $i \in \{1, \ldots, w\}$ such that $(a \oplus k_1)\,[i] \in U_2^{(0)}$.
2. there exists an index $i \in \{1, \ldots, w\}$ such that $\big(b \oplus T^{-1}(k_3)\big)\,[i] \in V_3^{(0)}$.
3. there exist a construction query $(x', a', b', y') \in \mathcal{Q}'_C$ and two indices $i, j \in \{1, \ldots, w\}$ such that $(x, a, i) \neq (x', a', j)$ and $(a \oplus k_1)\,[i] = (a' \oplus k_1)\,[j]$.
4. there exist a construction query $(x', a', b', y') \in \mathcal{Q}'_C$ and two indices $i, j \in \{1, \ldots, w\}$ such that $(x, a, i) \neq (x', a', j)$ 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 $u' = S_3^{-1}((b \oplus T^{-1}(k_3))[i])$, as long as it has not been determined by any existing query in $\mathcal{Q}_S$.

We remark that S_1, S_4, and $\mathcal{Q}'_S$ are *auxiliary variables* rather than something given to the distinguisher at the end of the interaction. The latter paradigm was used in [CS14], but it appears incompatible with point-wise proximity.

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

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

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 $\mathcal{Q}^{(1)}_{S_2}$ and $\mathcal{Q}^{(1)}_{S_3}$ 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_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 $i, i', i'' \in \{1, \dots, w\}$ 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 $i, i' \in \{1, \dots, w\}$ such that:

- $(x \oplus k_0)[i] \in U^{(0)}_1$ and $(x \oplus k_0)[i'] \in U^{(0)}_1$, or
- $(a \oplus k_1)[i] \in U^{(0)}_2$ and $(a \oplus k_1)[i'] \in U^{(0)}_2$, or
- $(b \oplus T^{-1}(k_3))[i] \in V^{(0)}_3$ and $(b' \oplus T^{-1}(k_3))[i'] \in V^{(0)}_3$, or
- $(y \oplus k_4)[i] \in V^{(0)}_4$ and $(y \oplus k_4)[i'] \in V^{(0)}_4$.

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

(B-3) there exist $(x, a, b, y) \in \mathcal{Q}'_C$ and $i, j \in \{1, \dots, w\}$ such that:

- $(a \oplus k_1)[i] \in U^{(1)}_2$ and $(b \oplus T^{-1}(k_3))[j] \in V^{(1)}_3$, or
- $(a \oplus k_1)[i] \in U^{(1)}_2$ and $(T(\overline{S_2}(a \oplus k_1)) \oplus k_2)[j] \in U^{(1)}_3$, or
- $(T^{-1}(\overline{S_3^{-1}}(b \oplus T^{-1}(k_3)) \oplus k_2))[i] \in V^{(1)}_2$ and $(b \oplus T^{-1}(k_3))[j] \in V^{(1)}_3$.

(B-4) 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 $(a \oplus k_1)[i] \in U^{(1)}_2, (a' \oplus k_1)[i'] \in U^{(1)}_2$, 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-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 $\big(b \oplus T^{-1}(k_3)\big)[i] \in V^{(1)}_3, \big(b' \oplus T^{-1}(k_3)\big)[i'] \in V^{(1)}_3$, 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 4. *Assuming $p+wq \leq N/2$, then the probability to obtain bad extended transcripts in the ideal world is bounded to*

$$\Pr\big[\tau' \in \Theta_{\text{bad}}(\tau)\big] \leq \frac{5w^2q(p+2wq)^2}{N^2} + \frac{3w^4q^2(p+2wq)}{N^2}. \tag{5}$$

The remaining of this subsection is devoted to establish Eq. (5). To this end, we analyze the conditions in turn.

3.2.1 Conditions (B-1) and (B-2)

For (B-1), consider each of the $q^3w(w-1)(w-2)/3! \leq w^3q^3/6$ choices $(x,a,b,y),(x',a',b',y')$, $(x'',a'',b'',y'') \in \mathcal{Q}'_C$ 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

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

Regarding (B-2), for each of the $q\binom{w}{2} \leq w^2q/2$ 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 $\big|U_1^{(0)}\big|^2/N^2 = p^2/N^2$. The same bound holds for the other three conditions. Thus

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

3.2.2 Useful intermediate results

To analyze the remaining conditions, we will rely on the following lemma, which characterizes some useful properties of the t-th round of the linear SPN.

Lemma 5. *For any $t \in \{1,2\}$, $r \in \{3,4\}$, $z,z',\delta \in \{0,1\}^n$, and $i,i',j,j' \in \{1,\ldots,w\}$,* *define*

$$\begin{aligned}
&\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'] \\
&\qquad \Big|\ \neg\textit{(B-1)}\wedge\neg\textit{(B-2)}\wedge S_t\vdash\mathcal{Q}^{(0)}_{S_t}\wedge\forall\ell\in\{1,\ldots,w\}:(z\oplus k_{t-1})[\ell]\notin U_t^{(0)}\Big],\\
&\mathsf{pcoll}_2^+(t,z,z',i,i',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'] \\
&\qquad \Big|\ \neg\textit{(B-1)}\wedge\neg\textit{(B-2)}\wedge S_t\vdash\mathcal{Q}^{(0)}_{S_t}\wedge(z\oplus k_{t-1})[i]\in U_t^{(0)}\wedge(z'\oplus k_{t-1})[i']\in U_t^{(0)}\Big],\\
&\mathsf{pcoll}_3^+(t,z,i,\delta) := \Pr\Big[\big(T\big(\overline{S_t}(z\oplus k_{t-1})\big)\oplus k_t\big)[i] = \delta \\
&\qquad \Big|\ \neg\textit{(B-1)}\wedge\neg\textit{(B-2)}\wedge S_t\vdash\mathcal{Q}^{(0)}_{S_t}\wedge\forall\ell\in\{1,\ldots,w\}:(z\oplus k_{t-1})[\ell]\notin U_t^{(0)}\Big],\\
&\mathsf{pcoll}_1^-(r,z,z',j,j') := \Pr\Big[\big(T^{-1}\big(\overline{S_r^{-1}}(z\oplus k_r)\big)\oplus k_{r-1}\big)[j] = \big(T^{-1}\big(\overline{S_r^{-1}}(z'\oplus k_r)\big)\oplus k_{r-1}\big)[j'] \\
&\qquad \Big|\ \neg\textit{(B-1)}\wedge\neg\textit{(B-2)}\wedge S_r\vdash\mathcal{Q}^{(0)}_{S_r}\wedge\forall\ell\in\{1,\ldots,w\}:(z\oplus k_r)[\ell]\notin V_r^{(0)}\Big],\\
&\mathsf{pcoll}_2^-(r,z,z',i,i',j,j') := \Pr\Big[\big(T^{-1}\big(\overline{S_r^{-1}}(z\oplus k_r)\big)\oplus k_{r-1}\big)[j] = \big(T^{-1}\big(\overline{S_r^{-1}}(z'\oplus k_r)\big)\oplus k_{r-1}\big)[j'] \\
&\qquad \Big|\ \neg\textit{(B-1)}\wedge\neg\textit{(B-2)}\wedge S_r\vdash\mathcal{Q}^{(0)}_{S_r}\wedge(z\oplus k_r)[i]\in V_r^{(0)}\wedge(z'\oplus k_r)[i']\in V_r^{(0)}\Big],\\
&\mathsf{pcoll}_3^-(r,z,i,\delta) := \Pr\Big[\big(T^{-1}\big(\overline{S_r^{-1}}(z\oplus k_r)\big)\oplus k_{r-1}\big)[i] = \delta \\
&\qquad \Big|\ \neg\textit{(B-1)}\wedge\neg\textit{(B-2)}\wedge S_r\vdash\mathcal{Q}^{(0)}_{S_r}\wedge\forall\ell\in\{1,\ldots,w\}:(z\oplus k_r)[\ell]\notin V_r^{(0)}\Big],
\end{aligned}$$

where the probabilities are taken over the random choices of S_t, k_{t-1}, k_t, S_r, k_{r-1}, and k_r. Then, as long as $(z,j)\neq(z',j')$, it holds

$$\begin{aligned}
&\mathsf{pcoll}_1^+(t,z,z',j,j')\le\frac{1}{N-p-wq}, &&\mathsf{pcoll}_2^+(t,z,z',i,i',j,j')\le\frac{1}{N-p-wq},\\
&\mathsf{pcoll}_1^-(r,z,z',j,j')\le\frac{1}{N-p-wq}, &&\mathsf{pcoll}_2^-(r,z,z',i,i',j,j')\le\frac{1}{N-p-wq}.\\
&\mathsf{pcoll}_3^+(t,z,i,\delta)\le\frac{1}{N}, &&\mathsf{pcoll}_3^-(r,z,i,\delta)\le\frac{1}{N}.
\end{aligned}$$

Proof. First, consider $\mathsf{pcoll}_1^+(t,z,z',j,j')$. When $j\neq j'$, 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 $z\neq z'$ while $T\big(\overline{S_t}(z\oplus k_{t-1})\big)[j]=T\big(\overline{S_t}(z'\oplus k_{t-1})\big)[j]$. Note that $z\neq z'$ implies there exists i_0 such that $(z\oplus k_{t-1})[i_0]\neq(z'\oplus k_{t-1})[i_0]$. 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: $(z\oplus k_{t-1})[i_0]$ 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 all $\ell\neq i_0$. Then, conditioned on $S_t\vdash\mathcal{Q}^{(0)}_{S_t}$ and on the $2w-1$ values $\{S_t((z\oplus k_{t-1})[\ell])\}_{1\le\ell\le w,\ell\neq i_0}\cup\{S_t((z'\oplus k_{t-1})[\ell])\}_{1\le\ell\le w}$, 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

$$\Pr\big[T(\overline{S_t}(z\oplus k_{t-1}))[j]\oplus T(\overline{S_t}(z'\oplus k_{t-1}))[j]=0\big]\le\frac{1}{N-p-wq}. \tag{6}$$

Case 2: $(z \oplus k_{t-1})[i_0] = (z \oplus k_{t-1})[i_1]$ for some $i_1 \neq i_0$. Then by ¬(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. (6) still holds.

- Subcase 2.2: $(z \oplus k_{t-1})[i_1] \neq (z' \oplus k_{t-1})[i_1]$. Then we write
$$\begin{aligned}&T(\overline{S_t}(z \oplus k_{t-1}))[j] \oplus T(\overline{S_t}(z' \oplus k_{t-1}))[j]\\ =&\underbrace{\Big(t_{j,i_0} \cdot S_t\big((z \oplus k_{t-1})[i_0]\big) \oplus t_{j,i_1} \cdot S_t\big((z \oplus k_{t-1})[i_1]\big)\Big)}_{\big(t_{j,i_0}\oplus t_{j,i_1}\big)\cdot S_t\big((z\oplus k_{t-1})[i_0]\big)}\\ &\oplus \Big(\bigoplus_{1\leq \ell\leq w} t_{j,\ell} \cdot S_t\big((z' \oplus k_{t-1})[\ell]\big)\Big) \oplus \Big(\bigoplus_{\ell\neq i_0, \ell\neq i_1} t_{j,\ell} \cdot S_t\big((z \oplus k_{t-1})[\ell]\big)\Big).\end{aligned}$$
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. (6) remains.

Case 3: $(z \oplus k_{t-1})[i_0] = (z' \oplus k_{t-1})[i_1]$ for some $i_1 \neq i_0$. 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 $\mathsf{pcoll}^+_1(t, z, z', j, j') \leq 1/(N-p-wq)$. Similarly by symmetry, $\mathsf{pcoll}^-_1(r, z, z', j, j') \leq 1/(N-p-wq)$.

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

First, consider $\mathsf{pcoll}^+_2(t, z, z', i, i', j, j)$ 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 $U^{(0)}_1$ and it contradicts ¬(B-2). In the same vein as the analysis of $\mathsf{pcoll}^+_1(t, z, z', j, j')$, we then distinguish three cases. 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 $\mathsf{pcoll}^+_1(t, z, z', j, j')$.

- 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

$$\begin{aligned} & T(\overline{S_t}(z \oplus k_{t-1}))[j] \oplus T(\overline{S_t}(z \oplus k_{t-1}))[j] \\ =& (t_{j,i} \cdot v_1) \oplus (t_{j,i} \cdot v_1') \oplus \Big(\bigoplus_{1 \leq \ell \leq w, \ell \neq i} t_{j,\ell} \cdot \big(S_1((x \oplus k_0)[\ell]) \oplus S_1((x' \oplus k_0)[\ell])\big)\Big). \end{aligned} \tag{7}$$

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. (7) 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, $\mathsf{pcoll}_2^-(r, z, z', i, i', j, j') \leq 1/(N - p - wq)$.

Finally, since $k_t[i]$ is uniform and independent of k_{t-1} and S_t, it immediately holds

$$\mathsf{pcoll}_3^+(t, z, i, \delta) = \frac{1}{N}.$$

Similarly, $\mathsf{pcoll}_3^-(r, z, i, \delta) = \frac{1}{N}$. These complete the proof. □

3.2.3 Conditions (B-3), (B-4), and (B-5)

Regarding (B-3), consider any choice of (x, a, b, y) and i, j. Consider the probability to have $(a \oplus k_1)[i] \in U_2^{(1)}$ first. Note that this consists of three subevents:

- (B-31) $(a \oplus k_1)[i] \in U_2^{(0)}$;

- (B-32) there exists $(x', a', b', y') \in \mathcal{Q}_C'$, and $j' \in \{1, \ldots, w\}$ such that $(x, j) \neq (x', j')$, while $(a \oplus k_1)[j] = (a' \oplus k_1)[j']$.

Since k_1 is uniform and independent of S_1, it holds $\Pr[\text{(B-31)}] \leq p/N$.

For (B-32), consider each $((x', a', b', y'), j')$ such that $(x, j) \neq (x', j')$, we distinguish three cases.

- Case 1: $(x \oplus k_0)[\ell] \notin U_1^{(0)}$ for all $\ell \in \{1, \ldots, w\}$. Then we have $\mathsf{pcoll}_1^+(1, x, x', j, j') \leq 1/(N - p - wq)$ by Lemma 5.

- Case 2: there exists i_1 such that $(x \oplus k_0)[i_1] \in U_1^{(0)}$, though $(x' \oplus k_0)[\ell] \notin U_1^{(0)}$ for all $\ell \in \{1, \ldots, w\}$. Then we have $\mathsf{pcoll}_1^+(1, x', x, j', j) \leq 1/(N - p - wq)$ by Lemma 5.

- Case 3: there exists i_1, i_2 such that $(x \oplus k_0)[i_1] \in U_1^{(0)}$ and $(x' \oplus k_0)[i_2] \in U_1^{(0)}$. Then we have $\mathsf{pcoll}_2^+(1, x, x', i_1, i_2, j, j') \leq 1/(N - p - wq)$ by Lemma 5.

Therefore, for any $((x', a', b', y'), j')$, the probability to have $(a \oplus k_1)[j] = (a' \oplus k_1)[j']$ never exceeds $1/(N - p - wq)$. By this, $\Pr[\text{(B-32)}] \leq wq/(N - p - wq)$. Using $p + wq \leq N/2$, we reach

$$\Pr\big[(a \oplus k_1)[i] \in U_2^{(1)}\big] \leq \Pr[\text{(B-31)}] + \Pr[\text{(B-32)}] \leq \frac{p}{N} + \frac{wq}{(N - p - wq)} \leq \frac{p + 2wq}{N}.$$

Via deriving one round further in a similar vein, we reach,

$$\Pr\big[(T(\overline{S_2}(a \oplus k_1)) \oplus k_2)[j] \in U_3^{(1)}\big] \leq \frac{p + 2wq}{N},$$

and similarly by symmetry,

$$\begin{aligned} &\Pr\big[(b \oplus T^{-1}(k_3))[j] \in V_3^{(1)}\big] \leq \frac{p + 2wq}{N}, \\ &\Pr\big[(T^{-1}(\overline{S_3^{-1}}(b \oplus T^{-1}(k_3)) \oplus k_2))[i] \in V_2^{(1)}\big] \leq \frac{p + 2wq}{N}. \end{aligned}$$

By this, the probability that (B-3) is fulfilled with respect to each choice of $((x, a, b, y), i, j)$ is at most $3(p + 2wq)^2/N^2$. As there are at most w^2q choices for (x, a, b, y) and i, j, we eventually obtain

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

(B-4) AND (B-5). For (B-4), we have

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

Similarly by symmetry,

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

3.2.4 Summary for bad transcripts

Summing over the above and using $\frac{w^3q^3}{N^2} \leq \frac{w^4q^2(p+2wq)}{N^2}$ and $\frac{2w^2qp^2}{N^2} \leq \frac{2w^2q(p+2wq)^2}{N^2}$ yield Eq. (5):

$$\begin{aligned} &\Pr\big[\tau' \in \Theta_{\text{bad}}\ (\tau)\big] \leq \sum_{i=1}^{5} \Pr[\text{(B-}i\text{)}] \\ \leq\ &\frac{w^3q^3}{N^2} + \frac{2w^2qp^2}{N^2} + \frac{3w^2q(p + 2wq)^2}{N^2} + \frac{w^4q^2(p + 2wq)}{N^2} + \frac{w^4q^2(p + 2wq)}{N^2} \\ \leq\ &\frac{5w^2q(p + 2wq)^2}{N^2} + \frac{3w^4q^2(p + 2wq)}{N^2}. \end{aligned}$$

3.3 Analyzing Good Transcript Extensions

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

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

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

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

To reach the real world probability $\mathsf{p}_2(\tau)$, consider any transcript extension $\tau' = (\mathcal{Q}'_C, \mathcal{Q}_S, \mathcal{Q}'_S, S^*_1, S^*_4, \mathbf{k})$ from τ. Denote

$$\begin{aligned}\mathsf{p}_{\mathrm{re}}(\tau') =& \Pr\Big[(\mathbf{k}', \mathcal{S}) \xleftarrow{\$} \left(\{0,1\}^{wn}\right)^5 \times \mathsf{Perm}(n)^4 : \Big(\left(S_1 = S^*_1\right) \wedge \left(S_4 = S^*_4\right) \wedge \\ & \left(S_2 \vdash \mathcal{Q}^{(1)}_{S_2}\right) \wedge \left(S_3 \vdash \mathcal{Q}^{(1)}_{S_3}\right) \wedge \left(\mathcal{C}^T_{\mathbf{k}'}[\mathcal{S}] \vdash \mathcal{Q}'_C\right) \wedge \left(\mathbf{k}' = \mathbf{k}\right)\Big)\Big]\\ \mathsf{p}_{\mathrm{mid}}(\tau') =& \Pr\Big[\mathcal{S} \xleftarrow{\$} \mathsf{Perm}(n)^4 : (\mathcal{C}^T_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}'_C) \;\Big|\; (S_1 = S^*_1) \wedge (S_4 = S^*_4) \wedge \\ & (S_2 \vdash \mathcal{Q}^{(1)}_{S_2}) \wedge (S_3 \vdash \mathcal{Q}^{(1)}_{S_3})\Big].\end{aligned}$$

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

$$\begin{aligned}\mathsf{p}_2(\tau) =& \Pr\left[(\mathbf{k}, \mathcal{S}) \xleftarrow{\$} \left(\{0,1\}^{wn}\right)^5 \times \mathsf{Perm}(n)^4 : \left(\mathsf{SP}^T_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_C\right) \wedge \left(\mathcal{S} \vdash \mathcal{Q}_S\right)\right]\\ \geq & \sum_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \mathsf{p}_{\mathrm{re}}(\tau') \geq \sum_{\tau' \in \Theta_{\mathrm{good}}(\tau)} \frac{1}{N^{5w}\left((N)_N\right)^2 (N)_{p+\alpha_1} (N)_{p+\alpha_2}} \cdot \mathsf{p}_{\mathrm{mid}}(\tau').\end{aligned}$$

Therefore,

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

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 $S_1 \vdash \mathcal{Q}^{(0)}_{S_1}, S_4 \vdash \mathcal{Q}^{(0)}_{S_4}$.
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:

$$\begin{aligned}B = &\sum_{\tau' \in \Theta_{\text{good}}(\tau)} \frac{1}{N^{5w}\big((N-p)_{N-p}\big)^2 (N-p)_{\alpha_1}(N-p)_{\alpha_2}} \\ =&\Pr\big[\tau' \in \Theta_{\text{good}}\ (\tau)\big] \geq 1 - \Pr\big[\tau' \in \Theta_{\text{bad}}\ (\tau)\big],\end{aligned}$$

which further implies

$$\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq \Pr\big[\tau' \in \Theta_{\text{good}}\ (\tau)\big] \cdot \min_{\tau' \in \Theta_{\text{good}}(\tau)} \big((N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau')\big). \tag{8}$$

The term $\mathsf{p}_{\text{mid}}(\tau')$ captures the probability that $\mathcal{C}^T_{\mathbf{k}'}[\mathcal{S}] \vdash \mathcal{Q}'_C$, 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 [CL18] to have a concrete bound on $(N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau')$.

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

$$(N^w)_q \cdot \mathsf{p}_{\text{mid}}(\tau') \geq 1 - \frac{q^2}{N^w} - \frac{q(2wp + 6w^2q)^2}{N^2}. \tag{9}$$

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 [CL18, page 16]. 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 [CL18, Lemma 9]. □

Gathering Eqs. (5), (8), and (9), and using $\frac{q(2wp+6w^2q)^2}{N^2} \leq \frac{4w^2q(p+3wq)^2}{N^2}$, we obtain

$$\begin{aligned}\frac{\mathsf{p}_2(\tau)}{\mathsf{p}_1(\tau)} \geq &\left(1 - \frac{5w^2q(p+2wq)^2}{N^2} - \frac{3w^4q^2(p+2wq)}{N^2}\right) \cdot \left(1 - \frac{q^2}{N^w} - \frac{q(2wp+6w^2q)^2}{N^2}\right) \\ \geq &1 - \frac{5w^2q(p+2wq)^2}{N^2} - \frac{3w^4q^2(p+2wq)}{N^2} - \frac{q^2}{N^w} - \frac{4w^2q(p+3wq)^2}{N^2} \\ \geq &1 - \frac{3w^4q^2(p+2wq)}{N^2} - \frac{q^2}{N^w} - \frac{9w^2q(p+3wq)^2}{N^2}\end{aligned}$$

as claimed in Eq. (4).

4 Conclusion

We show that, with four rounds and a moderately stronger linear permutation layer, a linear substitution-permutation network is secure up to $2^{2n/3}$ adversarial queries, which overcomes the birthday barrier. This provides additional theoretic supports for the real world SPN (tweakable) blockciphers.

We conjecture that the $2^{2n/3}$ security is tight for 4 or 3 rounds. Though, we are not aware of matching attacks. Moreover, whether 3 rounds are sufficient has been open since [DKS⁺17]. We also remark that: (a) the security of t-round linear SPNs for general t remains open, and (b) whether tweaks can be mixed into the construction via xoring, like [CS15], to ensure beyond-birthday-bound security, remains unknown.

Acknowledgments

Yuan Gao and Chun Guo were partly supported by the Program of Qilu Young Scholars (Grant No. 61580089963177) of Shandong University. Meiqin Wang was supported by National Key Research and Development Project under Grant No.2018YFA0704702, and Major Scientific and Technological Innovation Project of Shandong Province, China under Grant No.2019JZZY010133, and Major Scientific and Technological Innovation Project of Shandong Province, China under Grant No.2017CXGC0704. Weijia Wang was partly supported by the Program of Qilu Young Scholars (Grant No. 61580082063088) of Shandong University.

References

[ABK98] Ross Anderson, Eli Biham, and Lars Knudsen. Serpent: A Proposal for the Advanced Encryption Standard. NIST AES Proposal, 174, 1998.

[BBdS+19] Christof Beierle, Alex Biryukov, Luan Cardoso dos Santos, Johann Großschädl, Leo Perrin, Aleksei Udovenko, Vesselin Velichkov, and Qingju Wang. Alzette: A 64-bit arx-box. Cryptology ePrint Archive, Report 2019/1378, 2019. https://eprint.iacr.org/2019/1378. To appear at CRYPTO 2020.

[BBK14] Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key (extended abstract). In Palash Sarkar and Tetsu Iwata, editors, ASIACRYPT 2014, Part I, volume 8873 of LNCS, pages 63–84. Springer, Heidelberg, December 2014.

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

[Bir11] Alex Biryukov. Substitution-Permutation (SP) Network. In Encyclopedia of Cryptography and Security, 2nd Ed, page 1268. 2011.

[BK15] Alex Biryukov and Dmitry Khovratovich. Decomposition attack on sasasasas. Cryptology ePrint Archive, Report 2015/646, 2015. https://eprint.iacr.org/2015/646.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, CHES 2007, volume 4727 of LNCS, pages 450–466. Springer, Heidelberg, September 2007.

[BKL+12] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, François-Xavier Standaert, John P. Steinberger, and Elmar Tischhauser. Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract). In David Pointcheval and Thomas Johansson, editors, EUROCRYPT 2012, volume 7237 of LNCS, pages 45–62. Springer, Heidelberg, April 2012.

[BS10] Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. Journal of Cryptology, 23(4):505–518, October 2010.

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

[CHK$^+$16] Jean-Sébastien Coron, Thomas Holenstein, Robin Künzler, Jacques Patarin, Yannick Seurin, and Stefano Tessaro. How to build an ideal cipher: The indifferentiability of the Feistel construction. Journal of Cryptology, 29(1):61–114, January 2016.

[CL18] Benoît Cogliati and Jooyoung Lee. Wide tweakable block ciphers based on substitution-permutation networks: Security beyond the birthday bound. Cryptology ePrint Archive, Report 2018/488, 2018. https://eprint.iacr.org/2018/488.

[CLL$^+$18] Shan Chen, Rodolphe Lampe, Jooyoung Lee, Yannick Seurin, and John P. Steinberger. Minimizing the two-round Even-Mansour cipher. Journal of Cryptology, 31(4):1064–1119, October 2018.

[CLS15] Benoit Cogliati, Rodolphe Lampe, and Yannick Seurin. Tweaking Even-Mansour ciphers. In Rosario Gennaro and Matthew J. B. Robshaw, editors, CRYPTO 2015, Part I, volume 9215 of LNCS, pages 189–208. Springer, Heidelberg, August 2015.

[CS06] Debrup Chakraborty and Palash Sarkar. A new mode of encryption providing a tweakable strong pseudo-random permutation. In Matthew J. B. Robshaw, editor, FSE 2006, volume 4047 of LNCS, pages 293–309. Springer, Heidelberg, March 2006.

[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 Tetsu Iwata and Jung Hee Cheon, editors, ASIACRYPT 2015, Part II, volume 9453 of LNCS, pages 134–158. Springer, Heidelberg, November / December 2015.

[DDK09] Christophe De Cannière, Orr Dunkelman, and Miroslav Knežević. KATAN and KTANTAN - a family of small and efficient hardware-oriented block ciphers. In Christophe Clavier and Kris Gaj, editors, CHES 2009, volume 5747 of LNCS, pages 272–288. Springer, Heidelberg, September 2009.

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

[DR01] Joan Daemen and Vincent Rijmen. The wide trail design strategy. In Bahram Honary, editor, 8th IMA International Conference on Cryptography and Coding, volume 2260 of LNCS, pages 222–238. Springer, Heidelberg, December 2001.

[DR02] Joan Daemen and Vincent Rijmen. The Design of Rijndael: AES - the Advanced Encryption Standar Springer, 2002.

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

[EM97] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. Journal of Cryptology, 10(3):151–162, June 1997.

[GJMN16] Robert Granger, Philipp Jovanovic, Bart Mennink, and Samuel Neves. Improved masking for tweakable blockciphers with applications to authenticated encryption. In Marc Fischlin and Jean-Sébastien Coron, editors, EUROCRYPT 2016, Part I, volume 9665 of LNCS, pages 263–293. Springer, Heidelberg, May 2016.

[GOS89] Government Committee of the USSR for Standards. GOST, Gosudarstvennyi Standard 28147-89, Cryptographic Protection for Data Processing Systems. 1989.

[Hal07] Shai Halevi. Invertible universal hashing and the TET encryption mode. In Alfred Menezes, editor, CRYPTO 2007, volume 4622 of LNCS, pages 412–429. Springer, Heidelberg, August 2007.

[HP03] W. Cary Huffman and Vera Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press, 2003.

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

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

[HT16] Viet Tung Hoang and Stefano Tessaro. Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part I, volume 9814 of LNCS, pages 3–32. Springer, Heidelberg, August 2016.

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

[ISO16] ISO/IEC 18033-3:2010. Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers, 2016.

[Jou03] Antoine Joux. Cryptanalysis of the EMD mode of operation. In Eli Biham, editor, EUROCRYPT 2003, volume 2656 of LNCS, pages 1–16. Springer, Heidelberg, May 2003.

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

[LPS12] Rodolphe Lampe, Jacques Patarin, and Yannick Seurin. An asymptotically tight security analysis of the iterated Even-Mansour cipher. In Xiaoyun Wang and Kazue Sako, editors, ASIACRYPT 2012, volume 7658 of LNCS, pages 278–295. Springer, Heidelberg, December 2012.

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

[LRL18] Yunwen Liu, Vincent Rijmen, and Gregor Leander. Nonlinear diffusion layers. Des. Codes Cryptogr., 86(11):2469–2484, 2018.

[LRW11] Moses Liskov, Ronald L. Rivest, and David Wagner. Tweakable block ciphers. Journal of Cryptology, 24(3):588–613, July 2011.

[Men16] Bart Mennink. XPX: Generalized tweakable Even-Mansour with improved security guarantees. In Matthew Robshaw and Jonathan Katz, editors, CRYPTO 2016, Part I, volume 9814 of LNCS, pages 64–94. Springer, Heidelberg, August 2016.

[MP03] Ueli M. Maurer and Krzysztof Pietrzak. The security of many-round Luby-Rackoff pseudo-random permutations. In Eli Biham, editor, EUROCRYPT 2003, volume 2656 of LNCS, pages 544–561. Springer, Heidelberg, May 2003.

[MRH04] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In Moni Naor, editor, TCC 2004, volume 2951 of LNCS, pages 21–39. Springer, Heidelberg, February 2004.

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

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

[oS77] National Bureau of Standards. Data Encryption Standard (DES). Federal Information Processing Standards Publication 46, 1977.

[Pat03] Jacques Patarin. Luby-Rackoff: 7 rounds are enough for 2n(1-epsilon)security. In Dan Boneh, editor, CRYPTO 2003, volume 2729 of LNCS, pages 513–529. Springer, Heidelberg, August 2003.

[Pat04] Jacques Patarin. Security of random Feistel schemes with 5 or more rounds. In Matthew Franklin, editor, CRYPTO 2004, volume 3152 of LNCS, pages 106–122. Springer, Heidelberg, August 2004.

[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.

[PSC^{+}02] Sangwoo Park, Soo Hak Sung, Seongtaek Chee, E-Joong Yoon, and Jongin Lim. On the security of Rijndael-like structures against differential and linear cryptanalysis. In Yuliang Zheng, editor, ASIACRYPT 2002, volume 2501 of LNCS, pages 176–191. Springer, Heidelberg, December 2002.

[PSLL03] Sangwoo Park, Soo Hak Sung, Sangjin Lee, and Jongin Lim. Improving the upper bound on the maximum differential and the maximum linear Hull probability for SPN structures and AES. In Thomas Johansson, editor, FSE 2003, volume 2887 of LNCS, pages 247–260. Springer, Heidelberg, February 2003.

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

[Ste12] John Steinberger. Improved security bounds for key-alternating ciphers via hellinger distance. Cryptology ePrint Archive, Report 2012/481, 2012. http://eprint.iacr.org/2012/481.

A Candidate Good Transformations for Definition 1

For $n = 8$, the search space is sufficiently small for a naive exhaustive search. Concretely, using the primitive polynomial $x^8 + x^4 + x^3 + x + 1$, two candidates for $n = 8$ and $w = 8$ respectively are as follows:

$$\begin{pmatrix}
\text{0x}86 & \text{0x}AF & \text{0x}57 & \text{0x}A7 & \text{0x}CE & \text{0x}42 & \text{0x}9F & \text{0x}D \\
\text{0x}1F & \text{0x}6 & \text{0x}6C & \text{0x}9A & \text{0x}DC & \text{0x}E3 & \text{0x}D7 & \text{0x}93 \\
\text{0x}85 & \text{0x}69 & \text{0x}FF & \text{0x}28 & \text{0x}DC & \text{0x}65 & \text{0x}51 & \text{0x}A7 \\
\text{0x}46 & \text{0x}B2 & \text{0x}6 & \text{0x}F0 & \text{0x}73 & \text{0x}52 & \text{0x}EC & \text{0x}29 \\
\text{0x}41 & \text{0x}BD & \text{0x}6A & \text{0x}B3 & \text{0x}DE & \text{0x}79 & \text{0x}BE & \text{0x}5C \\
\text{0x}2D & \text{0x}EB & \text{0x}8A & \text{0x}D6 & \text{0x}6C & \text{0x}6D & \text{0x}8F & \text{0x}68 \\
\text{0x}13 & \text{0x}A1 & \text{0x}B8 & \text{0x}E3 & \text{0x}FF & \text{0x}4 & \text{0x}5A & \text{0x}D8 \\
\text{0x}CF & \text{0x}C6 & \text{0x}BA & \text{0x}8 & \text{0x}8F & \text{0x}D9 & \text{0x}D0 & \text{0x}1C
\end{pmatrix},$$

$$\begin{pmatrix}
\text{0x}F8 & \text{0x}59 & \text{0x}42 & \text{0x}9C & \text{0x}ED & \text{0x}1B & \text{0x}DD & \text{0x}F2 \\
\text{0x}AF & \text{0x}FF & \text{0x}20 & \text{0x}4F & \text{0x}81 & \text{0x}17 & \text{0x}E3 & \text{0x}9A \\
\text{0x}82 & \text{0x}A8 & \text{0x}F5 & \text{0x}A7 & \text{0x}3E & \text{0x}E8 & \text{0x}35 & \text{0x}C7 \\
\text{0x}45 & \text{0x}6D & \text{0x}67 & \text{0x}A0 & \text{0x}75 & \text{0x}8B & \text{0x}A1 & \text{0x}4C \\
\text{0x}B2 & \text{0x}BD & \text{0x}78 & \text{0x}B8 & \text{0x}E7 & \text{0x}AB & \text{0x}BE & \text{0x}93 \\
\text{0x}62 & \text{0x}49 & \text{0x}44 & \text{0x}D8 & \text{0x}DA & \text{0x}87 & \text{0x}EC & \text{0x}F3 \\
\text{0x}F8 & \text{0x}D6 & \text{0x}8D & \text{0x}96 & \text{0x}4D & \text{0x}63 & \text{0x}C4 & \text{0x}E7 \\
\text{0x}12 & \text{0x}77 & \text{0x}1E & \text{0x}F1 & \text{0x}D9 & \text{0x}7E & \text{0x}32 & \text{0x}1
\end{pmatrix},$$

For $n = 16$, we resort to coding theory in order to reduce the search space. Note that, to verify the 1st and 2nd conditions for linear matrices built upon cyclic codes, it suffices to verify them for a *single row*. Moreover, the dual code of a cyclic code remains cyclic [HP03, Theorem 4.2.6], which enables efficiently verifying the 3rd and 4th conditions for its inverse. By the above, we enumerate cyclic code-based matrices and verify if they satisfy Definition 1. Below we provide a candidate for $n = 8$ and $w = 16$ using the primitive polynomial $x^8 + x^4 + x^3 + x^2 + 1$.

$$\begin{pmatrix}
\text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D \\
\text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D \\
\text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 \\
\text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE \\
\text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 \\
\text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 \\
\text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 \\
\text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 \\
\text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A \\
\text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A \\
\text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 \\
\text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 \\
\text{0x}2C & \text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 \\
\text{0x}4C & \text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C \\
\text{0x}2 & \text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C \\
\text{0x}9D & \text{0x}7D & \text{0x}10 & \text{0x}BE & \text{0x}66 & \text{0x}F7 & \text{0x}85 & \text{0x}A8 & \text{0x}6A & \text{0x}9A & \text{0x}A6 & \text{0x}87 & \text{0x}30 & \text{0x}2C & \text{0x}4C & \text{0x}9D
\end{pmatrix}.$$