Beyond-birthday Security for 4-round Linear SP-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,
183408234180163.com,chun.guo@sdu.edu.cn

[2] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China

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 tweak linear SPNs and prove the 6-round tweakable linear SPN is beyond birthday security. This provides additional insights into the real world SPN ciphers.

Keywords: Blockcipher · Provable security · Key-alternating cipher · Substitution-Permutation networks · domain extension of block ciphers · beyond-birthday-bound

1 Introduction

Further Related Work. Various MACs ...

2 Preliminaries

2.1 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. Formally, an r-round SPN taking inputs of length wn where $w \in \mathcal{N}$ is the width of the network, is defined by $r+1$ keyed permutations $\{\pi_i : K_i \times \{0,1\}^{wn} \to \{0,1\}^{wn}\}_{i=0}^{r}$, a distribution $\mathcal{K}$ over $\mathcal{K}_0 \times \cdots \times \mathcal{K}_r$, and a permutation $\mathcal{S} : \{0,1\}^n \to \{0,1\}^n$. Given round keys $(k_0, \ldots, k_r) \in \mathcal{K}_0 \times \cdots \times \mathcal{K}_r$ and an input $x \in \{0,1\}^{wn}$, the output of the SPN is computed as follows

- Let $x_1 := \pi_0(k_0, x)$.
- For $i = 1$ to r do:
  1. $y_i := \bar{S}(x_i)$, where $\bar{S}(x[1]\| \cdots \|x[w]) \stackrel{\text{def}}{=} S(x[1])\| \cdots \|S(x[w])$.
  2. $x_{i+1} := \pi_i(k_i, y_i)$.
- The output is x_{r+1}.

If $\mathcal{S}$ is efficiently invertible and each π_i is efficiently invertible (given the appropriate key), then the above process is reversible given the round keys $k_0, \ldots, k_r$. In our definition of an SPN, we apply a fixed permutation $\mathcal{S}$ to all w blocks of the intermediate state in each round. More generally, one could consider using w different functions $S_1, \ldots, S_w$ in each round, or even different S-boxes in different rounds. Our positive results hold even when a single permutation $\mathcal{S}$ is used, and our negative result holds even if multiple permutations are used.

2.2 Linear SPNs

We are interested in understanding the security of both linear and non-linear SPNs. We now define what we mean by these terms.

Definition 1.A *keyed permutation* $\pi : \mathbb{F}^w \times \mathbb{F}^w \to \mathbb{F}^w$ *is* **linear** *if*

$$\pi(k, x) = (T_k \cdot k) + (T_x \cdot x) + \Delta,$$

where $T_k, T_x \in \mathbb{F}^{w \times w}$ *are linear transformations,* T_x *is invertible, and* $\Delta \in \mathbb{F}^w$*. An SPN is* **linear** *if all its round permutations* $\{\pi_i\}_{i=0}^r$ *are linear.*

If $\pi(k, x) = (T_k \cdot k) + (T_x \cdot x) + \Delta$ is linear, then we may write

$$\pi(k, x) = T \cdot ((T^{-1}T_k \cdot k) + (T^{-1} \cdot \Delta) + x);$$

thus, by setting $k' = (T^{-1}T_k \cdot k) + (T^{-1} \cdot \Delta)$ we can express π as

$$\pi(k', x) = T \cdot (k' + x). \tag{1}$$

In other words, if an SPN is linear, then we may assume (by redefining the distribution $\mathcal{K}$ on keys appropriately) that each of its permutations π_i takes the form (1). This matches what is often done in practice (e.g., in AES, Serpent,PRESENT, etc.), where round permutations are computed by first performing a key-mixing step followed by an invertible linear transformation. Since the linear transformation and key mixing commute, and the adversary can compute T and T^{-1} on its own (as T is public), we may further assume without loss of generality that the first and last permutations involve only a key-mixing step. In other words, we may set $\pi_i(k_i, x) = k_i + x$ for $i \in \{0, r\}$.

2.3 Tweakable linear Substitution-Permutation Networks

Tweakable Permutations. For an integer $m \geq 1$, the set of all permutations on $\{0,1\}^m$ will be denoted $\mathrm{Perm}(m)$. 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 $\widetilde{\mathrm{Perm}}(\mathcal{T}, m)$. 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 SPNs. For fixed parameters w and n, let $\mathcal{K}$ and $\mathcal{T}$ be two wn-bit blocks, we denote $f(k, t) = k \oplus t$ with $k \in \mathcal{K}$ and $t \in \mathcal{T}$, then let

$$T : f(k, t) \times \{0,1\}^{wn} \to \{0,1\}^{wn}$$

be a keyed tweakable linear permutation with key space $\mathcal{K}$, tweak space $\mathcal{T}$ and message space $\{0,1\}^{wn}$.We simply write $T(k,t,x)$ as $T_{f(k,t)}(x)$For a fixed number of rounds r, an r-round linear substitution-permutation network (SPN) based on T, denoted SP^T, takes as input a set of n-bit permutations $\mathcal{S} = (S_1, \ldots, S_r)$, and defines a keyed tweakable linear permutation $\mathrm{SP}^T[S]$ operating on wn-bit blocks with key space $\mathcal{K}^{r+1}$ and tweak space $\mathcal{T}$: on input $x \in \{0,1\}^{wn}$, key $\mathbf{k} = (k_0, k_1, \ldots, k_r) \in \mathcal{K}^{r+1}$ and tweak $t \in \mathcal{T}$, the output of $\mathrm{SP}^T[\mathcal{S}]$ is computed as follows.

- $y \leftarrow x$
- For $i \leftarrow 1$ to r do:
  1. $y \leftarrow T_{f(k_{i-1},t)}(y)$.
  2. Break $y = y_1 \| \cdots \| y_w$ into n-bit blocks.
  3. $y \leftarrow S_i(y_1) \| \cdots \| S_i(y_w)$.
- $y \leftarrow T_{f(k_r,t)}(y)$.

2.4 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 construction oracle denoted $\mathcal{C}$, are recorded in a query history

$$\mathcal{Q}_C = (x_i, y_i)_{1 \le i \le q}$$

where q is the number of queries made to $\mathcal{C}$, and (x_i, y_i) represents the evaluation obtained by the i -th query to $\mathcal{C}$, So according to the instantiation, it implies either $\mathrm{SP}_k[\mathcal{S}](x_i) = y_i$ or $\mathcal{P}(x_i) = y_i$. For $j = 1, \cdots, r$, 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 i -th query to S_j. Let

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

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 $\mathcal{D}(\mathcal{Q}_C, \mathcal{Q}_S)$.

The adversarial goal is to tell apart the two worlds $(\mathrm{SP}_{\mathbf{k}}[\mathcal{S}], \mathcal{S})$, and $(\mathcal{P}, \mathcal{S})$ 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

$$\begin{aligned} \mathrm{Adv}_{\mathrm{SP}}(\mathcal{D}) = &\Pr\left[\mathcal{P} \xleftarrow{s} \widehat{\mathrm{Perm}}(wn), \mathcal{S} \xleftarrow{s} \mathrm{Perm}(n)^r : 1 \leftarrow \mathcal{D}^{\mathcal{S},\mathcal{P}}\right] \\ &- \Pr\left[\mathbf{k} \xleftarrow{s} \mathcal{K}^{r+1}, \mathcal{S} \xleftarrow{s} \mathrm{Perm}(n)^r : 1 \leftarrow \mathcal{D}^{\mathcal{S},\mathrm{SP}_{\mathbf{k}}[\mathcal{S}]}\right] \end{aligned} \tag{2}$$

for $p, q > 0$,we define

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

We use the H-coefficient technique [**?**, **?**] to prove various indistinguishability results. We provide a quick overview of its main ingredients here. Our presentation is essentially that of Chen and Steinberger [**?**]; for further details, refer there or to the tutorial by Patarin [**?**]. Fix a distinguisher $\mathcal{D}$ that makes at most q queries to its oracles. As in the security definition presented above, $\mathcal{D}$'s aim is to distinguish between two worlds: a "real world" and an "ideal world". Assume without loss of generality that $\mathcal{D}$ is deterministic. The execution of $\mathcal{D}$ defines a transcript that includes the sequence of queries and answers received from its oracles; $\mathcal{D}$'s output is a deterministic function of its transcript. Thus if X, Y denote the probability distributions on transcripts induced by the real and ideal worlds, respectively, then $\mathcal{D}$'s distinguishing advantage is upper bounded by the statistical distance

$$\Delta(X,Y) := \frac{1}{2}\sum_{\tau} |\Pr[X=\tau] - \Pr[Y=\tau]|$$

where the sum is taken over all possible transcripts τ. Let $\mathcal{T}$ denote the set of all transcripts that can be generated by $\mathcal{D}$ in either world. We look for a partition of $\mathcal{T}$ into two sets $\mathcal{T}_1$ and $\mathcal{T}_2$ of "good" and "bad" transcripts, respectively, along with a constant $\epsilon_1 \in [0,1)$ such that

$$\tau \in \mathcal{T}_1 \Longrightarrow \Pr[X=\tau]/\Pr[Y=\tau] \geq 1-\epsilon_1$$

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

$$\Delta(X,Y) \leq \epsilon_1 + \Pr[Y \in \mathcal{T}_2]$$

For a transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, a key $k \in \mathcal{K}^{r+1}$, a permutation $\mathcal{P} \in \mathrm{Perm}(wn)$, a set of S-boxes $\mathcal{S} = (S_1, \ldots, S_r) \in \mathrm{Perm}(n)^r$ and $j \in \{1, \ldots, r\}$: if $S_j(u_i) = v_i$ for every $i = 1, \ldots, p$, 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 $j \in \{1, \ldots, r\}$. Similarly, if $\mathrm{SP}_{\mathbf{k}}[\mathcal{S}](x_i) = y_i$ (resp.$\mathcal{P}(x_i) = y_i$) for every $i = 1, \ldots, q$, then we will write $\mathrm{SP}_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_C$(resp.$\mathcal{P} \vdash \mathcal{Q}_C$).

Then for $Y \in \mathcal{T}_2$, we have

$$\mathrm{Pr}_{re}(\tau,k) = \Pr\left[\mathbf{k} \xleftarrow{s} \mathcal{K}^{r+1}, \mathcal{S} \xleftarrow{s} \mathrm{Perm}(n)^r : \mathrm{SP}_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_C, \mathcal{S} \vdash \mathcal{Q}_S\right]$$
$$\mathrm{Pr}_{id}(\tau,k) = \Pr\left[\mathcal{P} \xleftarrow{s} \widehat{\mathrm{Perm}}(wn), \mathcal{S} \xleftarrow{s} \mathrm{Perm}(n)^r : \mathcal{P} \vdash \mathcal{Q}_C, \mathcal{S} \vdash \mathcal{Q}_S\right]$$

2.5 Indistinguishability in the Multi-user Setting

We concentrate on the MU security with m users. The SU security definition corresponds to the special case of $m = 1$. Concretely, let $\mathrm{SP}_k[\mathcal{S}]$ be an r -round SPN based on a set of S-boxes $\mathcal{S} = (S_1, \cdots, S_r)$. In the multi-user setting, let ℓ denote the number of users. In the real world ℓ secret keys $k_1, \cdots, k_\ell \in \mathcal{K}^{r+1}$ are chosen independently at random. A set of independent S-boxes $\mathcal{S} = (S_1, \cdots, S_r)$ is also randomly chosen from $\mathrm{Perm(n)}^r$. A distinguisher $\mathcal{D}$ is given oracle access to $(\mathrm{SP}_{k_1}[\mathcal{S}], \cdots, \mathrm{SP}_{k_\ell}[\mathcal{S}])$ as well as $\mathcal{S} = (S_1, \cdots, S_r)$. In the ideal world, $\mathcal{D}$ is given a set of independent random permutation $\mathcal{P} = (\mathrm{P}_1, \cdots, \mathrm{P}_\ell) \in \widetilde{\mathrm{Perm}}(wn)^l$ instead of $(\mathrm{SP}_{k_1}[\mathcal{S}], \cdots, \mathrm{SP}_{k_\ell}[\mathcal{S}])$. However, oracle access to $\mathcal{S} = (S_1, \cdots, S_r)$ is still allowed in the world.

The adversarial goal is to tell apart the two worlds, the $(\mathrm{SP}_{k_1}[\mathcal{S}], \cdots, \mathrm{SP}_{k_l}[\mathcal{S}], \mathcal{S})$ and the ideal world $(\mathrm{P}_1, \cdots, \mathrm{P}_\ell, \mathcal{S})$ 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

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

for $p, q > 0$, we define

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

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 permutations. In the single-user setting with $l = 1$. $\mathrm{Adv}^{mu}_{\mathrm{SP}}(\mathcal{D})$ and $\mathrm{Adv}^{mu}_{\mathrm{SP}}(p,q)$ will also be written as $\mathrm{Adv}^{su}_{\mathrm{SP}}(\mathcal{D})$ and $\mathrm{Adv}^{su}_{\mathrm{SP}}(p,q)$, respectively.

3 related works

Till now, for the beyond birthday security, the wide tweakable block ciphers based on 2-round nonlinear SPN was proved in [?], we will briefly recall it in this chapter.

2-ROUND NONLINEAR SPN. Fix a transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, a key $k \in \mathcal{K}^{r+1}$, a tweakable permutation $\widetilde{\mathcal{P}} \in \widetilde{\mathrm{Perm}}(\mathcal{T}, wn)$, a set of S-boxes $\mathcal{S} = (S_1, \cdots, S_r) \in \mathrm{Perm}(n)^r$ and $j \in \{1, \cdots, \ell\}$. Let $k_1, \cdots, k_\ell \in \mathcal{K}^{r+1}$ and $\mathcal{P} = (\mathrm{P}_1, \cdots, \mathrm{P}_\ell) \in \widetilde{\mathrm{Perm}}(\mathcal{T}, wn)^l$, if $\mathrm{SP}^T_{k_j}[\mathcal{S}] \vdash \mathcal{Q}_{C_j}$ (resp. $\mathcal{P}_j \vdash \mathcal{Q}_{C_j}$) for every $j = 1, \cdots, \ell$, then we will write $(\mathrm{SP}^T_{k_j}[\mathcal{S}])_{j=1,\cdots,\ell} \vdash \mathcal{Q}_C$ (resp. $\mathcal{P} \vdash \mathcal{Q}_{C_j}$).

If there exist $\widetilde{\mathcal{P}} \in \widetilde{\mathrm{Perm}}(\mathcal{T}, wn)$ and $\mathcal{S} \in \mathrm{Perm}(n)^w$ that outputs τ at the end of the interaction with $\mathcal{D}$, then for an attainable transcript $\tau = (\mathcal{Q}_C, \mathcal{Q}_S)$, let

$$\begin{aligned}\mathrm{p}_1(\mathcal{Q}_C|\mathcal{Q}_S) &= \Pr\left[\widetilde{\mathcal{P}}\xleftarrow{s}\widetilde{\mathrm{Perm}}(\mathcal{T},wn)^\ell, \mathcal{S}\xleftarrow{s}\mathrm{Perm}(n)^r : \widetilde{\mathcal{P}}\vdash\mathcal{Q}_C|\mathcal{S}\vdash\mathcal{Q}_S\right],\\ \mathrm{p}_2(\mathcal{Q}_C|\mathcal{Q}_S) &= \Pr\left[k_1,\ldots,k_\ell\xleftarrow{s}\mathcal{K}^{r+1},\mathcal{S}\xleftarrow{s}\mathrm{Perm}(n)^r : \left(\mathrm{SP}^T_{k_j}[\mathcal{S}]\right)_j\vdash\mathcal{Q}_C|\mathcal{S}\vdash\mathcal{Q}_S\right].\end{aligned}$$

With these definitions, we can get the following lemma, the core of the H-coefficients technique (without defining "bad" transcripts).

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

$$\mathrm{p}_2(\mathcal{Q}_C|\mathcal{Q}_S) \geq (1-\epsilon)\mathrm{p}_1(\mathcal{Q}_C|\mathcal{Q}_S),$$

Then one has

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

The lower bound 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 $j = 1, \cdots, \ell$ in the single user setting. The following lemma is a restatement of Lemma 3 in [?].

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

1. *$\epsilon(x,y) + \epsilon(x,z) \leq \epsilon(x, y+z)$ for every $x, y, z \in \mathbb{N}$,*

2. $\epsilon(\cdot, z)$ *and* $\epsilon(z, \cdot)$ *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*

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

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*

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

So

Lemma 3 *Let* $\delta, \delta' \geq 0$ *and let* n *and* w *be positive integers such that* $w \geq 2$*. Let* T *be a* (δ, δ') *-super blockwise universal tweakable permutation. Then for any integers* p *and* q *such that* $wp + 3w^2p \leq \frac{2^n}{2}$*, one has*

$$\begin{aligned}
\mathrm{Adv}^{su}_{\mathrm{SP}^T}(p,q) &\leq w^2q\left(\delta'p + \delta wq\right)\left(3\delta'p + 3\delta wq + 2\delta' wq\right) + \frac{q^2}{2wn} + \frac{q\left(2wp + 6w^2q\right)^2}{2^{2n}}.\\
\mathrm{Adv}^{mu}_{\mathrm{SP}^T}(p,q) &\leq w^2q\left(\delta'p + (\delta + \delta')\, wq\right)\left(3\delta'p + 3\delta wq + 5\delta' wq\right)\\
&\quad + \frac{q^2}{2^{wn}} + \frac{q\left(2wp + 8w^2q\right)^2}{2^{2n}}.
\end{aligned}$$

Remark 2. For the sake of simplicity, we assume that the three keyed layers are actually the same, which is why we require T to be (δ, δ') -super blockwise universal. However, if one looks closely at the proof, only the middle layer has to be super-blockwise-universal. The first and the last layer only need to be (δ, δ') -super blockwise universal.

Remark 3. When the S-boxes are modeled as block ciphers using secret keys, the security bound (in the standard model) is obtained by setting $p = 0$

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

$$\mathrm{p}\left(\tau'\right) = \Pr\left[\mathcal{S} \xleftarrow{\mathrm{s}} \mathrm{Perm}(n)^2 : \mathrm{SP}^T_k[\mathcal{S}] \vdash \mathcal{Q}_C | \left(S_1 \vdash \mathcal{Q}^{(1)}_{S_1}\right) \wedge \left(S_2 \vdash \mathcal{Q}^{(1)}_{S_2}\right)\right].$$

Then we will get the following lemma:

Lemma 4 *For any good extended transcript* τ'*, one has*

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

if T is a super blockwise tweakable universal permutation, then the security of SP^T converges to 2^n (in terms of the threshold number of queries) as the number of rounds r increases. For detailed certification was show in [**?**].

Lemma 5 *For an even integer* r*, let* SP^T *be an* r *-round substitution-permutation network based on a* (δ, δ') *-super blockwise tweakable universal permutation* T*, Then one has*

$$\mathrm{Adv}^{\mathrm{mu}}_{\mathrm{SP}^T}(p,q) \leq 4\sqrt{q}\left(2wp\delta' + 2w^2q\left(\delta' + \delta\right) + w^2\delta\right)^{\frac{r}{4}}.$$

Hence, assuming $\delta, \delta' \backsimeq 2^{-n}$, and $p = q$, an r -round SP^T is secure up to $2^{\frac{rn}{r+2}}$ queries.

4 security of 4-round SPNs

We now explore conditions under which 4-round, linear SPNs are secure. Recall from subsection 2.1 that a 4-round SPN has five round permutations $\{\pi_i\}_{i=0}^4$, and without loss of generality we may assume

$$\pi_i\left(k_i, x\right) = \begin{cases} x \oplus k_i & i \in \{0,4\} \\ T_i \cdot (x \oplus k_i) & i \in \{1,2,3\} \end{cases}$$

where $T_1, T_2, T_3 \in \mathbb{F}^{w\times w}$ are invertible linear transformations. We prove that a 4-round, linear SPN is secure so long as (i) T_1, T_2 and T_2^{-1}, T_3^{-1} contain no zero entries(Miles and Viola [**?**] show that matrices with maximal branch number [**?**] satisfy this property), and (ii) round keys $\{k_i\}(i = 0, 1, 2, 3, 4)$ are (individually) uniform.

In this section, we will prove the following theorem.

Theorem 1. Assume $w > 1$, Let $\mathcal{C}$ be a 4-round, linear SPN with round permutations as in subsection 2.1 showed and with distribution $\mathcal{K}$ over keys k_0, k_1, k_2, k_3, k_4. If round keys $\{k_i\}(i = 0, 1, 2, 3, 4)$ are (individually) uniform and T_1 and T_3^{-1} contain no zero entries, then for any integers p and q such that $p + wq \leq \frac{2^n}{2}$, one has

$$\begin{aligned}\mathrm{Adv}_{\mathcal{C}}\left(p, q\right) \leq \frac{q^2}{2^{nw}} + \frac{8w^2q(p+wq)^2 + w^2q}{2^n} \\ + \frac{16w^2q(p+wq)(p+wq+3q) + 4w^2q(p+3wq)^2 + w^2q(p+wq)(3p+wq)}{2^{2n}}.\end{aligned} \tag{3}$$

Outline of Proof of Theorem 1. Throughout the proof, we will write a 4-round SP construction as $\mathrm{SP}_k[\mathcal{S}](x)$, where $\mathcal{S} = (S_1, S_2, S_3, S_4)$ is a pair of four public random permutations of $\{0,1\}^n$, and $k = (k_0, k_1, k_2, k_3, k_4) \in \mathcal{K}^5$ is the key, $x \in \{0,1\}^{wn}$ is the plaintext, and, for i = 1, 2, 3, 4,

$$\begin{gathered} S_i^{\|} : \{0,1\}^{wn} \to \{0,1\}^{wn} \\ x = x_1 \|x_2\| \ldots \|x_w \longmapsto S_i\left(x_1\right) \| S_i\left(x_2\right) \| \ldots \| S_i\left(x_w\right). \end{gathered}$$

We also 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.

We will first define what we mean by an extension of the transcript τ. Then we will extension the outer two rounds and the inner two rounds transcripts respectively. Next, we will define bad transcripts and bad(S_1, S_4), which is the most important step in our proof. Finally, we will peel off he outer two rounds and analyzing the inner two rounds. 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 TWO ROUNDS). We will extend the transcript τ of the attack via a certain randomized process. We begin with choosing a pair of keys $(k_0, k_4) \in \mathcal{K}^2$ 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 $(x, y) \in \mathcal{Q}_C$ 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 $(x \oplus k_0)[i] = u$.
2. there exist an S-box query $(4, u, v) \in \mathcal{Q}_S$ and an integer $i \in \{1, \ldots, w\}$ such that $(y \oplus k_4)[i] = v$.
3. there exist a construction query $(x', y') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(x, y, i) \neq (x', y', j)$ and $(x \oplus k_0)[i] = (x' \oplus k_0)[j]$.
4. there exist a construction query $(x', y') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(x, y, i) \neq (x', y', j)$ and $i \in \{1, \ldots, w\}$ such that $(y \oplus k_4)[i] = (y' \oplus k_4)[j]$.

We are now going to build a new set $\mathcal{Q}'_{S_{outer}}$ of S-box evaluations that will play the role of an extension of $\mathcal{Q}_S$. For each colliding query $(x, y) \in \mathcal{Q}_C$, we will add tuples $(1, (x \oplus k_0)[i], v')_{1 \leq i \leq w}$ (if $(x,\ y)$ collides at the input of S_1) or $(4, u', (y \oplus k_4)[i])_{1 \leq i \leq w}$ (if $(x,\ y)$ collides at the output of S_4) by lazy sampling $v' = S_1((x \oplus k_0)[i])$ or $u' = S_4^{-1}((y \oplus k_4)[i])$, 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 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 $\mathbf{k} = (k_0, k_1, k_2, k_3, k_4)$. 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

$$\mathcal{Q}^{(1)}_{S_1} = \left\{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (1, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_{S_{outer}}\right\}$$
$$\mathcal{Q}^{(1)}_{S_4} = \left\{(u, v) \in \{0,1\}^n \times \{0,1\}^n : (4, u, v) \in \mathcal{Q}_S \cup \mathcal{Q}'_{S_{outer}}\right\}$$

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

$$U_1 = \left\{u_1 \in \{0,1\}^n : (1, u_1, v_1) \in \mathcal{Q}^{(1)}_{S_1}\right\}, \quad V_1 = \left\{v_1 \in \{0,1\}^n : (1, u_1, v_1) \in \mathcal{Q}^{(1)}_{S_1}\right\},$$
$$U_4 = \left\{u_4 \in \{0,1\}^n : (4, u_4, v_4) \in \mathcal{Q}^{(1)}_{S_4}\right\}, \quad V_4 = \left\{v_4 \in \{0,1\}^n : (4, u_4, v_4) \in \mathcal{Q}^{(1)}_{S_4}\right\}$$

be the domains and ranges of $\mathcal{Q}^{(1)}_{S_1}$ and $\mathcal{Q}^{(1)}_{S_4}$, respectively. We define two quantities characterizing an extended transcript τ', namely

$$\alpha_1 \stackrel{\text{def}}{=} \left|\left\{(x, y) \in \mathcal{Q}_C : (x \oplus k_0)[i] \in U_1 \text{ for some } i \in \{1, \ldots, w\}\right\}\right|$$
$$\alpha_4 \stackrel{\text{def}}{=} \left|\left\{(x, y) \in \mathcal{Q}_C : (y \oplus k_4)[i] \in V_4 \text{ for some } i \in \{1, \ldots, w\}\right\}\right|$$

In words, α_1 (resp. α_4) is the number of queries $(x,y) \in \mathcal{Q}_C$ which collide with a query $(u_1,v_1) \in \mathcal{Q}_{S_1}^{(1)}$ (resp. which collide with a query $(u_4,v_4) \in \mathcal{Q}_{S_4}^{(1)}$) in the extended transcript. This corresponds to the number of queries $(x,y) \in \mathcal{Q}_C$ which collide with either an original query $(u_1,v_1) \in \mathcal{Q}_{S_1}^{(0)}$ (resp. which collide with a query $(u_4,v_4) \in \mathcal{Q}_{S_4}^{(0)}$) or with a query $(x',y') \in \mathcal{Q}_C$ at an input of S_1 (resp. at the output of S_4), once the choice of (k_0,k_4) 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 $i = 1, 4$ the number of additional queries included in the extended transcript.

4.1 Bad Transcript for 4-rounds SPN and Probability

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

- (B-1) there exists $(x,y) \in \mathcal{Q}_C, (u_1,v_1) \in \mathcal{Q}_{S_1}^{(1)}, (u_4,v_4) \in \mathcal{Q}_{S_4}^{(1)}$, 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 $(x,y) \in \mathcal{Q}_C, (u_1,v_1) \in \mathcal{Q}_{S_1}^{(1)}, (u_2,v_2) \in \mathcal{Q}_{S_2}$, and index $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0)[i] = u_1$ and $(T_1(S_1(x \oplus k_0) \oplus k_1))[j] = u_2$.
- (B-3) there exists $(x,y) \in \mathcal{Q}_C, (u_3,v_3) \in \mathcal{Q}_{S_3}, (u_4,v_4) \in \mathcal{Q}_{S_4}^{(1)}$, and index $i,j \in \{1,\ldots,w\}$ such that $(y \oplus k_4)[j] = v_4$ and $\left(\left(T_3^{-1}\left(S_4^{-1}(y \oplus k_4)\right)\right) \oplus k_3\right)[i] = v_3$.
- (B-4) there exists $(x,y) \in \mathcal{Q}_C$ and distinct indices $i,j \in \{1,\ldots,w\}$ such that $(x \oplus k_0)[i] = (x \oplus k_0)[j]$, or $(y \oplus k_4)[i] = (y \oplus k_4)[j]$.

Lemma 6 *One has*

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

Proof: We fix any extended transcript, denoted $\left(\mathcal{Q}_C, \mathcal{Q}_S, \mathcal{Q}'_{S_{outer}}\right)$. For any fixed construction query $(x,y) \in \mathcal{Q}_C$, now we upper bound the probabilities of the bad extended transcript.

Consider (B-1) first: Since we have at most $w^2q\left(p+wq\right)^2$ choices for $(x,y) \in \mathcal{Q}_C, (u_1,v_1) \in \mathcal{Q}_{S_1}^{(1)}, (u_4,v_4) \in \mathcal{Q}_{S_4}^{(1)}$ and index $i,j \in \{1,\ldots,w\}$ and since the random choice of k_0 and k_4 are independent, one has

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

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

Then consider (B-4). We assume that $w \neq 2$, because of $w = 1$ does not belong to the primary problem of the SP-networks. Since the random choice of k_0 and k_4 are independent, then we have

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

Then sum of yields (4).

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 $\Pr\left[\mathcal{S} \xleftarrow{\mathbf{s}} (\mathcal{S}(n))^4 : \mathrm{SP}_k[\mathcal{S}] \vdash \mathcal{Q}_C | \mathcal{S} \vdash \mathcal{Q}_S\right]$. It consists of two steps. In the first step, we will lower bound the probability that a pair of functions (S_1, S_4) satisfies certain "bad" conditions that will be defined. With the values given by a "good" pair of functions (S_1, S_4), a transcript of the distinguisher on 4 rounds can be transformed into a special transcript on 2 rounds; in this sense, we "peel off" the outer two rounds. Then in the second step, assuming (S_1, S_4) is good, we analyze the induced 2-round transcript to yield the final bounds. In the following, each step would take a subsection. As mentioned in the Introduction, this two-step approach is motivated by Cogliati et al. [**?**] and [**?**].

PEELING OFF THE OUTER TWO ROUNDS. Pick a pair of S-box (S_1, S_4) such that $S_1 \vdash \mathcal{Q}_{S_1}^{(0)}$ and $S_4 \vdash \mathcal{Q}_{S_4}^{(0)}$, and for each $(x, y) \in \mathcal{Q}_C$ we set $a = S_1(x \oplus k_0)$, $b = S_4^{-1}(y \oplus k_4)$. In this way we obtain q tuples of the form (a, b); for convenience we denote the set of such induced tuples by $\mathcal{Q}_C^*(S_1, S_4)$. Similarly, we also extended the inner two rounds:

We begin with choosing a pair of keys $(k_1, k_3) \in \mathcal{K}^2$ 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 $(a, b) \in \mathcal{Q}_C^*(S_1, S_4)$ is similar to a colliding query is defined as a construction query $(x, y) \in \mathcal{Q}_C$, there we will not describe it in detail.

Then we build a new set $\mathcal{Q}'_{S_{inner}}$ of S-box evaluations that will play the role of an extension of $\mathcal{Q}_C^*(S_1, S_4)$. For each colliding query $(a, b) \in \mathcal{Q}_C^*(S_1, S_4)$, we will add tuples $(2, T_1(a \oplus k_1)[i], v')_{1 \le i \le w}$(if (a, b) collides at the input of S_2) or $\left(3, u', T_3^{-1}(b) \oplus k_3[i]\right)_{1 \le i \le w}$ (if (a, b) collides at the output of S_3) by lazy sampling, as long as it has not been determined by any existing query in $\mathcal{Q}_C^*(S_1, S_4)$, $v' = S_2((T_1(a \oplus k_1)))[i])$ or $u' = S_3^{-1}\left(\left(T_3^{-1}(b) \oplus k_3\right)[i]\right)$. Then we choose the key k_2 uniformly at random. An extended transcript of τ_{inner} will be defined as a tuple $\tau'_{inner} = \left(\mathcal{Q}_C^*(S_1, S_4), \mathcal{Q}_{S_{inner}}, \mathcal{Q}'_{S_{inner}}, \mathbf{k}\right)$ where $\mathbf{k} = (k_1, k_2, k_3)$. 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_{inner} in the real world.

Then for $Y \in \mathcal{T}_1$, define

$$\begin{aligned}
\mathrm{p}(\tau, S_1, S_4) &= \Pr\left[\S^* \xleftarrow{\mathrm{s}} (\mathcal{S}(n))^2 : \mathrm{SP}_k^{S^*} \vdash \mathcal{Q}_C^*(S_1, S_4) \,|S_i \vdash \mathcal{Q}_{S_i}, i = 1, 2, 3, 4\right] \\
&= \Pr\left[S^* \xleftarrow{\mathrm{s}} (\mathcal{S}(n))^2 : \mathrm{SP}_k^{S^*} \vdash \mathcal{Q}_C^*(S_1, S_4) \,|S_2 \vdash \mathcal{Q}_{S_2}, S_3 \vdash \mathcal{Q}_{S_3}\right] \\
&\quad \cdot \Pr\left[S_2 \vdash \mathcal{Q}_{S_2}, S_3 \vdash \mathcal{Q}_{S_3} | S_i \vdash \mathcal{Q}_{S_i}, i = 1, 2, 3, 4\right] \\
&= \Pr\left[S^* \xleftarrow{\mathrm{s}} (\mathcal{S}(n))^2 : \mathrm{SP}_k^{S^*} \vdash \mathcal{Q}_C^*(S_1, S_4) \,|S_2 \vdash \mathcal{Q}_{S_2}, S_3 \vdash \mathcal{Q}_{S_3}\right].
\end{aligned} \tag{5}$$

We define $\mathrm{p}(S_1, S_4) = \Pr\left[(S_1^*, S_4^*) \xleftarrow{\mathrm{S}} (\mathcal{S}(n))^2 : (S_1^*, S_4^*) = (S_1, S_4)\right]$ for convenience. Next we need to consider $\frac{\Pr_{re}(\tau,k)}{\Pr_{id}(\tau,k)}$. Clearly, once S_1 and S_4 are fixed such that $S_1 \vdash \mathcal{Q}_{S_1}$ and $S_4 \vdash \mathcal{Q}_{S_4}$, the event $\mathrm{SP}_k[\mathcal{S}] \vdash \mathcal{Q}_C$ is equivalent to $\mathrm{SP}_k^{S^*} \vdash \mathcal{Q}_C^*(S_1, S_4)$. Hence,

$$\Pr_{re}(\tau, k) \ge \sum_{S_1 \vdash \mathcal{Q}_{S_1}, S_4 \vdash \mathcal{Q}_{S_4} : (S_1, S_4) good} \mathrm{p}(S_1, S_4) \cdot \mathrm{p}(\tau, S_1, S_4) \cdot \mathrm{p}(S_2 \vdash \mathcal{Q}_{S_2}, S_3 \vdash \mathcal{Q}_{S_3}).$$

Because of $\Pr(\mathcal{P} \vdash \mathcal{Q}_C) \leq \frac{1}{(2^{wn})_q}$. Therefore,

Lemma 7 *Once S_1 and S_4 are fixed such that $S_1 \vdash \mathcal{Q}_{S_1}$ and $S_4 \vdash \mathcal{Q}_{S_4}$, we have*

$$\begin{aligned}\frac{\Pr_{re}(\tau,k)}{\Pr_{id}(\tau,k)} &\geq \frac{\sum_{S_1\vdash\mathcal{Q}_{S_1},S_4\vdash\mathcal{Q}_{S_4}:(S_1,S_4)good} \mathrm{p}\left(S_1,S_4\right)\cdot \mathrm{p}\left(\tau,S_1,S_4\right)}{\Pr(S_1\vdash\mathcal{Q}_{S_1},S_4\vdash\mathcal{Q}_{S_4})\cdot\frac{1}{(2^{wn})_q}} \\ &\geq \left(1-\Pr\left[\mathrm{Bad}\left(S_1,S_4\right)|S_1\vdash\mathcal{Q}_{S_1},S_4\vdash\mathcal{Q}_{S_4}\right]\right)\cdot\frac{\mathrm{p}\left(\tau,S_1,S_4\right)}{\frac{1}{(2^{wn})_q}}.\end{aligned} \tag{6}$$

Proof: For any attainable transcript $\tau_{inner} = \left(\mathcal{Q}_C^*\left(S_1,S_4\right),\mathcal{Q}_{S_{inner}},\mathcal{Q}'_{S_{inner}},\mathbf{k}\right)$, let

$$\begin{aligned}\mathrm{p}_1\left(\mathcal{Q}_C|\mathcal{Q}_S\right) &= \Pr\left[\widetilde{\mathcal{P}} \xleftarrow{s} \widetilde{\mathrm{Perm}}(\mathcal{T},wn)^\ell, \mathcal{S}\xleftarrow{s}\mathrm{Perm}(n)^r : \tilde{\mathcal{P}}\vdash\mathcal{Q}_C|\mathcal{S}\vdash\mathcal{Q}_S\right], \\ \mathrm{p}_2\left(\mathcal{Q}_C|\mathcal{Q}_S\right) &= \Pr\left[k_1,\ldots,k_\ell\leftarrow\mathcal{K}^{r+1}, \mathcal{S}\xleftarrow{s}\mathrm{Perm}(n)^r : \left(\mathrm{SP}_{k_j}[\mathcal{S}]\right)_j\vdash\mathcal{Q}_C|\mathcal{S}\vdash\mathcal{Q}_S\right].\end{aligned}$$

$$\begin{aligned}\mathcal{Q}_{S_2}^{(1)} &= \left\{(u,v)\in\{0,1\}^n\times\{0,1\}^n : (2,u,v)\in\mathcal{Q}_S\cup\mathcal{Q}'_{S_{inner}}\right\}, \\ \mathcal{Q}_{S_3}^{(1)} &= \left\{(u,v)\in\{0,1\}^n\times\{0,1\}^n : (3,u,v)\in\mathcal{Q}_S\cup\mathcal{Q}'_{S_{inner}}\right\}.\end{aligned}$$

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

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 $i = 2, 3$ the number of additional queries included in the extended transcript.

Next, we will prove the below lemma firstly.

Lemma 8 *For any extended $S_1 \vdash \mathcal{Q}_{S_1}, S_4 \vdash \mathcal{Q}_{S_4}$, we have*

$$\begin{aligned}1-\Pr\left[\mathrm{Bad}\left(S_1,S_4\right)|S_1\vdash\mathcal{Q}_{S_1},S_4\vdash\mathcal{Q}_{S_4}\right] &\geq 1-\frac{2w^2q(p+wq)^2}{(N-p)} \\ -\frac{2w^2q(p+wq)(p+wq+2q)}{N\cdot(N-p)} &- \frac{w^2q(p+wq)(p+wq+2q)}{(N-p)^2} - \frac{2w^2q^2(p+wq)}{(N-p-wq)\cdot(N-p)}.\end{aligned} \tag{7}$$

Proof: Then we define a predicate $\mathrm{Bad}\left(S_1,S_4\right)$ on the pair (S_1,S_4), which holds if the corresponding induced set $\mathcal{Q}_C^*\left(S_1,S_4\right)$ fulfills at least one of the following nine "collision" conditions:

(C-1) there exist $(a,b)\in\mathcal{Q}_C^*\left(S_1,S_4\right)$, $i,j\in\{1,\ldots,w\}$, $u_2\in U_2$ and $v_3\in V_3$ such that $\left(T_1\left(a\oplus k_1\right)\right)[i] = u_2$ and $\left(T_3^{-1}\left(b\right)\oplus k_3\right)[i] = v_3$.

(C-2) there exist $(a,b)\in\mathcal{Q}_C^*\left(S_1,S_4\right)$, $i,j\in\{1,\ldots,w\}$, $u_2\in U_2$ and $u_3\in U_3$ such that $\left(T_1\left(a\oplus k_1\right)\right)[i] = u_2$ and $\left(T_2\left(S_2\left(T_1\left(a\oplus k_1\right)\right)\oplus k_2\right)\right)[j] = u_3$.

(C-3) there exist $(a,b)\in\mathcal{Q}_C^*\left(S_1,S_4\right)$, $i,j\in\{1,\ldots,w\}$, $v_2\in V_2$ and $v_3\in V_3$ such that $\left(T_3^{-1}\left(b\right)\oplus k_3\right)[i] = v_3$ and $\left(T_2^{-1}\left(S_3^{-1}\left(T_3^{-1}\left(b\right)\oplus k_3\right)\right)\oplus k_2\right)[j] = v_2$.

(C-4) there exist $(a,b) \in \mathcal{Q}_C^* (S_1, S_4)$, distinct $i, i' \in \{1, \ldots, w\}$, $u_2, u_2' \in U_2$ such that

$$(T_1 (a \oplus k_1))[i] = u_2, \text{ and } (T_1 (a \oplus k_1))[i'] = u_2'.$$

(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

$$(T_1 (a \oplus k_1))[i] = u_2, \text{ and } (T_1 (a \oplus k_1))[i'] = (T_1 (a' \oplus k_1))[i'].$$

(C-6) there exist $(a,b), (a',b') \in \mathcal{Q}_C^* (S_1, S_4)$, $i, i', j, j' \in \{1, \ldots, w\}$, with$(a,j) \neq (a',j')$, $u_2, u_2' \in U_2$ such that $(T_1 (a \oplus k_1))[i] = u_2, (T_1 (a' \oplus k_1))[i'] = u_2'$ and

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

(C-7) there exist $(a,b) \in \mathcal{Q}_C^* (S_1, S_4)$, distinct $i, i' \in \{1, \ldots, w\}$, $v_3, v_3' \in V_3$ such that

$$\left(T_3^{-1} (b) \oplus k_3\right)[i] = v_3, \text{ and } \left(T_3^{-1} (b) \oplus k_3\right)[i'] = v_3'.$$

(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

$$\left(T_3^{-1} (b) \oplus k_3\right)[i] = v_3, \text{ and } \left(T_3^{-1} (b) \oplus k_3\right)[i] = \left(T_3^{-1} (b') \oplus k_3\right)[i'].$$

(C-9) there exist $(a,b), (a',b') \in \mathcal{Q}_C^* (S_1, S_4)$, $i, i', j, j' \in \{1, \ldots, w\}$, with$(b,j) \neq (b',j')$, $v_3, v_3' \in V_3$ such that $\left(T_3^{-1} (b) \oplus k_3\right)[i] = v_3, \left(T_3^{-1} (b') \oplus k_3\right)[i'] = v_3'$ and

$$\left(T_2^{-1} \left(S_3^{-1} \left(T_3^{-1} (b) \oplus k_3\right)\right) \oplus k_2\right)[j] = \left(T_2^{-1} \left(S_3^{-1} \left(T_3^{-1} (b') \oplus k_3\right)\right) \oplus k_2\right)[j'].$$

Because of $\Pr[\text{Bad}(S_1, S_4) | S_1 \vdash \mathcal{Q}_{S_1}, S_4 \vdash \mathcal{Q}_{S_4}]$ is conditioned on $S_1 \vdash \mathcal{Q}_{S_1}, S_4 \vdash \mathcal{Q}_{S_4}$, we now upper bound the probabilities of the seven conditions in turn. The sets of attainable transcripts fulfilling condition (C-1), (C-2), (C-3), (C-4), (C-5), (C-6), (C-7) will be denoted $\Theta_1, \Theta_2, \Theta_3, \Theta_4, \Theta_5, \Theta_6, \Theta_7, \Theta_8, \Theta_9$, respectively.

Condition (C-1). If there exist $(a,b) \in \mathcal{Q}_C^* (S_1, S_4)$, $(u_2, v_2) \in \mathcal{Q}_{S_2}^{(1)}, (u_3, v_3) \in \mathcal{Q}_{S_3}^{(1)}$ such that $(T_1 (a \oplus k_1))[i] = u_2$ and $\left(T_3^{-1} (b) \oplus k_3\right)[i] = v_3$, $i, j \in \{1, \ldots, w\}$ then for $(x,y) \in \mathcal{Q}_C$, satisfy that $(T_1 (S_1 (x \oplus k_0) \oplus k_1))[i] = u_2$ and $\left(T_3^{-1} \left(S_4^{-1} (y \oplus k_4)\right) \oplus k_3\right)[j] = v_3$, it can not be $(x \oplus k_0)[i] \in \mathcal{Q}_{S_1}^{(1)}$, otherwise would satisfy (B-2). Similarly, $(y \oplus k_4)[j] \in \mathcal{Q}_{S_4}^{(1)}$. Thus conditioned on $S_1 \vdash \mathcal{Q}_{S_1}$ and $S_4 \vdash \mathcal{Q}_{S_4}$, the two values $(S_1 (x \oplus k_0))[i]$ and $\left(S_4^{-1} (y \oplus k_4)\right)[j]$ remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_4})$. Because every entry in the i_0th column of T_1 and T_4 is nonzero, thus for each $(a,b) \in \mathcal{Q}_C^* (S_1, S_4)$, $(u_2, v_2) \in \mathcal{Q}_{S_2}^{(1)}$, $(u_3, v_3) \in \mathcal{Q}_{S_3}^{(1)}$, the probability that both $(T_1 (S_1 (x \oplus k_0) \oplus k_1))[i] = u_2$ and $\left(T_3^{-1} \left(S_4^{-1} (y \oplus k_4)\right) \oplus k_3\right)[j] = v_3$ hold is at most $\frac{1}{(N-p)^2}$. Since we have at most $w^2 q (p + wq)^2$ such tuples, so

$$\Pr[\tau_{inner} \in \Theta_1] \leq \frac{w^2 q (p + wq)^2}{(N-p)^2}.$$

Condition (C-2) and Condition (C-3). If there exist $(a,b) \in \mathcal{Q}_C^* (S_1, S_4)$, $(u_2, v_2) \in \mathcal{Q}_{S_2}^{(1)}, (u_3, v_3) \in \mathcal{Q}_{S_3}^{(1)}$, $i, j \in \{1, \ldots, w\}$ such that

$$(T_1 (a \oplus k_1))[i] = u_2, \quad (T_2 (S_2 (T_1 (a \oplus k_1)) \oplus k_2))[j] = u_3$$

then $(T_1 (S_1 (x \oplus k_0) \oplus k_1))[i] = u_2$ and $(T_2 (S_2 (T_1 (S_1 (x \oplus k_0) \oplus k_1)) \oplus k_2))[j] = u_3$ for $(x,y) \in \mathcal{Q}_C$, it can not be $(x \oplus k_0)[i] \in \mathcal{Q}_{S_1}^{(1)}$, otherwise would satisfy (B-2). Thus

conditioned on $S_1 \vdash \mathcal{Q}_{S_1}$ and $S_4 \vdash \mathcal{Q}_{S_4}$, the value $(S_1(x \oplus k_0))[i]$ remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_4})$. Because every entry in the i_0th column of T_1 is nonzero, the probability that there exist $(x,y) \in \mathcal{Q}_C$, $(u_2,v_2) \in \mathcal{Q}_{S_2}^{(1)}$, $i \in \{1,\ldots,w\}$ such that $(T_1(S_1(x \oplus k_0) \oplus k_1))[i] = u_2$ is upper bounded by $\frac{wq(p+wq)}{N-p}$. And Since the random choice of k_2 is independent from the queries transcript and from the choice of k_0, k_1, thus the probability, over the random choice of k_2 that there exist $(u_3,v_3) \in \mathcal{Q}_{S_3}^{(1)}$, $j \in \{1,\ldots,w\}$ such that $(T_2(S_2(T_1(S_1(x \oplus k_0) \oplus k_1)) \oplus k_2))[j] = u_3$, conditioned on $(T_1(S_1(x \oplus k_0) \oplus k_1))[i] = u_2$ is upper bounded by $\frac{w(p+wq)}{N}$. Thus, by summing over every construction query, one has

$$\Pr[\tau_{inner} \in \Theta_2] \leq \frac{w^2 q(p+wq)^2}{N \cdot (N-p)}.$$

Similarly, one has

$$\Pr[\tau_{inner} \in \Theta_3] \leq \frac{w^2 q(p+wq)^2}{N \cdot (N-p)}.$$

Conditions (C-4). Similar to the previous has mentioned, it can not be $(x \oplus k_0)[i] \in \mathcal{Q}_{S_1}^{(1)}$, otherwise would satisfy (B-2). Thus conditioned on $S_1 \vdash \mathcal{Q}_{S_1}$ and $S_4 \vdash \mathcal{Q}_{S_4}$, the value $(S_1(x \oplus k_0))[i]$ remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_4})$. Then take advantage of (B-4), it can not be $(x \oplus k_0)[i] = (x \oplus k_0)[j]$, or $(y \oplus k_4)[i] = (y \oplus k_4)[j]$. That is $(a \oplus k_1)[i] \neq (a \oplus k_1)[i']$ must be established. So, one has

$$\Pr[\tau_{inner} \in \Theta_4] \leq \frac{w^2 q(p+wq)^2}{N-p}.$$

Conditions (C-5). We have the value $(S_1(x \oplus k_0))[i]$ remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_4})$. Because of the fact that there exists i with $x[i] \neq x'[i]$, that is there exist i with $(a \oplus k_1)[i'] \neq (a' \oplus k_1)[i']$. So,

$$\Pr[\tau_{inner} \in \Theta_5] \leq \frac{w^2 q^2(p+wq)}{(N-p)^2}.$$

The proof of (C-7) and (C-8) is similar to the above-mentioned.

Conditions (C-6) and (C-9). Because of the value $(S_1(x \oplus k_0))[i]$ remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_4})$. We divide (C-6) into two subevents: the first concerning with $j \neq j'$, while the second concerning with $j = j'$.

For the first case, to make

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

achieved, we just leverage the fact that $k_2[j]$ and $k_2[j']$ are uniform and independent, so the collision holds with probability $\frac{1}{N}$. Because of $a$remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_4})$, let (a',b') be the unique query such that the collision happened. Then the probability that $(T_1(a \oplus k_1))[i] = u_2, (T_1(a' \oplus k_1))[i'] = u_2'$ is at most $\frac{1}{N-p}$, because we have at most $w^2q^2(p+wq)$ such tuples, one has

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

For the case of $j = j'$ with distinct $(a,b),(a',b')$, that is there is only one index has different value of input and output. Because of the value $(S_1(x' \oplus k_0))[i]$ also remain uniform in $\{0,1\}^n \backslash (\mathcal{Q}_{S_1} \cup \mathcal{Q}_{S_4})$ conditioned on the fact that the value $(S_1(x \oplus k_0))[i]$ is uniform. Then we leverage the randomness due to lazy sampling $S_2(T_1(a \oplus k_1))$. Conditioned on

(C-4), for $i'' \neq i$, the value $T_1(a \oplus k_1)[i'']$ "does not collide with" pairs in $\mathcal{Q}_{S_2}^{(1)}$, and will be assigned a random outputs during the lazy sampling process. Simultaneously conditioned on (C-5), for distinct $i'' \neq i$, if $(T_1(a \oplus k_1))[i] = u_2$, it holds $(T_1(a \oplus k_1))[i''] \neq (T_1(a' \oplus k_1))[i'']$. Since T_2 contain no zero entries, so the value $(T_2(S_2(T_1(a \oplus k_1)) \oplus k_2))[i'']$ could not be disturbed by the value of $(T_2(S_2(T_1(a' \oplus k_1)) \oplus k_2))[i'']$ and thus uniform in at least $\frac{1}{N-p-wq}$. One has,

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

So, combine these two subevents, one has

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

Similarly, one has

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

Then we have

$$\begin{aligned}1 - \Pr[\mathrm{Bad}(S_1,S_4) \,|\, S_1 \vdash \mathcal{Q}_{S_1}, S_4 \vdash \mathcal{Q}_{S_4}] \geq 1 &- \frac{2w^2q(p+wq)^2}{(N-p)} \\ - \frac{2w^2q(p+wq)(p+wq+2q)}{N\cdot(N-p)} &- \frac{w^2q(p+wq)(p+wq+2q)}{(N-p)^2} - \frac{2w^2q^2(p+wq)}{(N-p-wq)\cdot(N-p)}.\end{aligned}$$

Lemma 9 *Pick a pair of functions (S_1, S_4), peeling off the outer two round and it holds*

$$\begin{aligned}\frac{\mathrm{p}(\tau, S_1, S_4)}{(2^{wn})_q} \geq 1 &- \frac{4w^2q(p+wq)^2}{N} \\ &- \frac{8w^2q(p+wq)(p+wq+3q) + 4w^2q(p+3wq)^2}{N^2} - \frac{q^2}{N^w}.\end{aligned} \tag{8}$$

Proof: For any extended transcript $\tau'_{inner} = \left(\mathcal{Q}_C^*(S_1,S_4), \mathcal{Q}_{S_{inner}}, \mathcal{Q}'_{S_{inner}}, \mathbf{k}\right)$, let us denote

$$\begin{aligned}\mathrm{p} &= \Pr\left[(\mathbf{k},\mathcal{S}) \xleftarrow{s} \mathcal{K}^3 \times \mathrm{Perm}(n)^2 : \left(\mathcal{S} \vdash \mathcal{Q}_{S_{inner}} \cup \mathcal{Q}'_{S_{inner}}\right) \wedge \left(\mathrm{SP}_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_C^*(S_1,S_4)\right) \wedge \mathbf{k}\right] \\ \mathrm{p}(\tau'_{inner}) &= \Pr\left[\mathcal{S} \xleftarrow{\mathbf{s}} \mathrm{Perm}(n)^2 : \mathrm{SP}_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_C^*(S_1,S_4) \,|\, \left(S_2 \vdash \mathcal{Q}_{S_2}^{(1)}\right) \wedge \left(S_3 \vdash \mathcal{Q}_{S_3}^{(1)}\right)\right].\end{aligned}$$

we will write $(r)_s = \frac{r!}{(r-s)!}$. Note that one has

$$\begin{aligned}&\Pr\left[(\mathcal{P},\mathcal{S}) \xleftarrow{s} \mathrm{Perm}(wn) \times \mathrm{Perm}(n)^2 : (\mathcal{S} \vdash \mathcal{Q}_{S_{inner}}) \wedge (\mathrm{P} \vdash \mathcal{Q}_C^*(S_1,S_4))\right] \\ &\leq \frac{1}{(2^{wn})_q (2^n)_p (2^n)_p}. \\ &\Pr\left[(\mathbf{k}',\mathcal{S}) \xleftarrow{s} \mathcal{K}^3 \times \mathrm{Perm}(n)^2 : (\mathcal{S} \vdash \mathcal{Q}_{S_{inner}}) \wedge (\mathrm{SP}_{\mathbf{k}}[\mathcal{S}] \vdash \mathcal{Q}_C^*(S_1,S_4))\right] \\ &\geq \sum_{\tau'_{inner} \in \Theta_{\mathrm{Good}}(\tau_{inner})} \mathrm{p} \\ &\geq \sum_{\tau'_{inner} \in \Theta_{\mathrm{Good}}(\tau_{inner})} \frac{1}{|\mathcal{K}|^3 (2^n)_{p+\beta_2} (2^n)_{p+\beta_3}} \mathrm{p}(\tau'_{inner}).\end{aligned}$$

Define

$$\mathrm{p}_1 = \Pr\left[\mathrm{P} \xleftarrow{s} \mathrm{Perm}(wn), \mathcal{S} \xleftarrow{s} \mathrm{Perm}(n)^2 : \widetilde{\mathrm{P}} \vdash \mathcal{Q}_C^* \left(S_1, S_4\right) | \mathcal{S}_{inner} \vdash \mathcal{Q}_{S_{inner}}\right],$$
$$\mathrm{p}_2 = \Pr\left[\mathbf{k}' \xleftarrow{s} \mathcal{K}^3, \mathcal{S} \xleftarrow{s} \mathrm{Perm}(n)^r : (\mathrm{SP}_{\mathbf{k}}[\mathcal{S}]) \vdash \mathcal{Q}_C^* \left(S_1, S_4\right) | \mathcal{S}_{inner} \vdash \mathcal{Q}_{S_{inner}}\right].$$

Then

$$\mathrm{p}_1 \leq \left(2^{wn}\right)_p,$$
$$\mathrm{p}_2 \geq \sum_{\tau'_{inner} \in \Theta_{\mathrm{Good}}(\tau_{inner})} \frac{1}{|\mathcal{K}|^3 \left((2^n - p)\right)_{\beta_2} \left((2^n - p)\right)_{\beta_3}} \mathrm{p}\left(\tau'_{inner}\right).$$

Thus one has

$$\begin{aligned}\frac{\mathrm{p}_2}{\mathrm{p}_1} &\geq \frac{\left(2^{wn}\right)_p}{|\mathcal{K}|^3 \left((2^n - p)\right)_{\beta_2} \left((2^n - p)\right)_{\beta_3}} \mathrm{p}\left(\tau'_{inner}\right) \\ &\geq \min_{\tau'_{inner} \in \Theta_{\mathrm{good}}\ (\tau_{inner})} \left(\left(2^{wn}\right)_q \mathrm{p}\left(\tau'_{inner}\right)\right) \sum_{\tau'_{inner} \in \Theta_{\mathrm{good}}\ (\tau_{inner})} \frac{1}{|\mathcal{K}|^3 \left(2^n - p\right)_{\beta_2} \left(2^n - p\right)_{\beta_3}}.\end{aligned}$$

Note that the weighted sum $\sum_{\tau'_{inner} \in \Theta_{\mathrm{good}}\ (\tau_{inner})} \frac{1}{|\mathcal{K}|^3 (2^n - p)_{\beta_2} (2^n - p)_{\beta_3}}$ corresponds exactly to the probability that a random inner extended transcript is good when it is sampled as follows:

1. choose keys $k_1, k_3 \in \mathcal{K}$ uniformly and independently at random;
2. choose the partial extension of the S-box queries based on the new collisions $\mathcal{Q}'_{S_{inner}}$ uniformly at random (meaning that each possible u or v is chosen uniformly at random in the set of its authorized values);
3. finally choose $k_2 \in \mathcal{K}$ uniformly at random, independently from everything else.

Thus, the exact probability of observing the inner extended transcript τ'_{inner} is

$$\frac{1}{|\mathcal{K}|^3 \left(2^n - p\right)_{\beta_2} \left(2^n - p\right)_{\beta_3}}.$$

and we have

$$\sum_{\tau'_{inner} \in \Theta_{\mathrm{good}}\ (\tau_{inner})} \frac{1}{|\mathcal{K}|^3 \left(2^n - p\right)_{\beta_2} \left(2^n - p\right)_{\beta_3}} = \Pr\left[\tau'_{inner} \in \Theta_{\mathrm{good}}\ (\tau_{inner})\right].$$

One finally gets

$$\frac{\mathrm{p}_2}{\mathrm{p}_1} \geq \Pr\left[\tau'_{inner} \in \Theta_{\mathrm{good}}\ (\tau_{inner})\right] \cdot \min_{\tau'_{inner} \in \Theta_{\mathrm{good}}} \left(\left(2^{wn}\right)_q p(\tau'_{inner})\right). \tag{9}$$

The previous proof is conditioned on $S_1 \vdash \mathcal{Q}_{S_1}, S_4 \vdash \mathcal{Q}_{S_4}$, but $\Pr\left[\tau'_{inner} \in \Theta_{\mathrm{good}}\ (\tau_{inner})\right]$, we need to consider $S_1 \vdash \mathcal{Q}^{(1)}_{S_1}, S_4 \vdash \mathcal{Q}^{(1)}_{S_4}$. That is the probability $\left(T_1\left(S_1\left(x \oplus k_0\right) \oplus k_1\right)\right)[i] = u_2$ or $\left(T_3^{-1}\left(S_4^{-1}\left(y \oplus k_4\right)\right) \oplus k_3\right)[j] = v_3$ hold is at most $\frac{1}{(N-p-wq)}$, so

$$\begin{aligned}\Pr\left[\tau'_{inner} \in \Theta_{\text{good}}\left(\tau_{inner}\right)\right] \geq & 1-\frac{2w^2q(p+wq)^2}{(N-p-wq)}-\frac{2w^2q(p+wq)(p+wq+2q)}{N\cdot(N-p-wq)} \\ & -\frac{w^2q(p+wq)(p+wq+2q)}{(N-p-wq)^2}-\frac{2w^2q^2(p+wq)}{(N-p-wq)^2}.\end{aligned} \tag{10}$$

From the Lemma 9 of [**?**], we have

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

then combine all of (9), (10), we can obtain

$$\begin{aligned}\frac{\mathrm{p}\left(\tau, S_1, S_4\right)}{\left(2^{wn}\right)_q} \geq & \left(1-\frac{q^2}{2^{wn}}-\frac{q\left(2wp+6w^2q\right)^2}{2^{2n}}\right) \\ & \cdot\left(1-\frac{2w^2q(p+wq)^2}{(N-p-wq)}-\frac{2w^2q(p+wq)(p+wq+2q)}{N\cdot(N-p-wq)}\right. \\ & \left.-\frac{w^2q(p+wq)(p+wq+2q)}{(N-p-wq)^2}-\frac{2w^2q^2(p+wq)}{(N-p-wq)^2}\right) \\ \geq & 1-\frac{2w^2q(p+wq)^2}{(N-p-wq)}-\frac{2w^2q(p+wq)(p+wq+2q)}{N\cdot(N-p-wq)} \\ & -\frac{w^2q(p+wq)(p+wq+2q)}{(N-p-wq)^2}-\frac{2w^2q^2(p+wq)}{(N-p-wq)^2} \\ & -\frac{q^2}{2^{wn}}-\frac{q\left(2wp+6w^2q\right)^2}{2^{2n}} \\ \geq & 1-\frac{4w^2q(p+wq)^2}{N}-\frac{8w^2q(p+wq)(p+wq+2q)}{N^2} \\ & -\frac{8w^2q^2(p+wq)}{N^2}-\frac{q^2}{2^{wn}}-\frac{q\left(2wp+6w^2q\right)^2}{2^{2n}} \\ = & 1-\frac{4w^2q(p+wq)^2}{N} \\ & -\frac{8w^2q(p+wq)(p+wq+3q)+4w^2q(p+3wq)^2}{N^2}-\frac{q^2}{N^w}.\end{aligned}$$

then combine (7), (8), we can obtain

$$\begin{aligned}\mathrm{Adv}_{\mathcal{C}}\left(p,q\right) \leq & \frac{q^2}{2^{nw}}+\frac{8w^2q(p+wq)^2+w^2q}{2^n} \\ & +\frac{16w^2q(p+wq)(p+wq+3q)+4w^2q(p+3wq)^2+w^2q(p+wq)(3p+wq)}{2^{2n}}.\end{aligned}$$

5 beyond birthday bound for tweakable linear SPNs

We also explore conditions under which 6-round, tweakable linear SPNs are secure. A 6-round SPN has seven round permutations $\{\pi_i\}_{i=0}^{6}$, and without loss of generality we may assume

$$\pi_i\left(k_i,t,x\right)=\begin{cases} x\oplus k_i\oplus t & i\in\{0,6\} \\ T_i\cdot\left(x\oplus k_i\oplus t\right) & i\in\{1,2,3,4,5\}\end{cases}$$

where $T_1, T_2, T_3, T_4, T_5 \in \mathbb{F}^{w\times w}$ are invertible linear transformations. We prove that a 6-round, linear SPN is secure so long as (i) T_1, T_2 T_3 and T_3^{-1}, T_4^{-1},T_5^{-1} contain no zero entries(Miles and Viola [**?**] show that matrices with maximal branch number [**?**] satisfy this property), and (ii) round keys $\{k_i\}(i = 0, 1, 2, 3, 4, 5, 6)$ are (individually) uniform.

We will prove the following theorem firstly.

Theorem 2. Assume $w > 1$, Let $\mathcal{C}$ be a 6-round, tweakable linear SPN with round permutations as in subsection 2.1 showed and with distribution $\mathcal{K}$ over keys $k_0, k_1, k_2, k_3, k_4, k_5, k_6$. If round keys $\{k_i\}(i = 0, 1, 2, 3, 4, 5, 6)$ are (individually) uniform and T_1 and T_5^{-1} contain no zero entries, then for any integers p and q such that $p + wq \leq \frac{2^n}{2}$, one has

$$\begin{aligned}\mathrm{Adv}_{\mathcal{C}}(p,q) \leq \frac{q^2}{2^{nw}} + \frac{8w^2q(p+wq)^2 + w^2q}{2^n} \\ + \frac{16w^2q(p+wq)(p+wq+3q) + 4w^2q(p+3wq)^2 + w^2q(p+wq)(3p+wq)}{2^{2n}}.\end{aligned} \tag{11}$$

Outline of Proof of Theorem 2. Throughout the proof, we will write a 6-round SP construction as $\mathrm{SP}_k^T[\mathcal{S}](x)$, where $\mathcal{S} = (S_1, S_2, S_3, S_4, S_5, S_6)$ is a pair of six public random permutations of $\{0,1\}^n$, and $k = (k_0, k_1, k_2, k_3, k_4, k_6, k_7) \in \mathcal{K}^7$ is the key, $x \in \{0,1\}^{wn}$ is the plaintext. and, for i = 1, 2, 3, 4,

$$\begin{gathered}S_i^{\|} : \{0,1\}^{wn} \to \{0,1\}^{wn} \\ x = x_1 \|x_2\| \ldots \|x_w \longmapsto S_i(x_1) \| S_i(x_2) \| \ldots \| S_i(x_w).\end{gathered}$$

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

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

and let

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

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

Similar to the 4-round SPN, we will first define what we mean by an extension of the transcript τ. Then we will extension the outer four rounds and the inner two rounds transcripts respectively. Next, we will define bad transcripts, which is the most important step in our proof. Finally, we will peel off he outer two rounds(for the outer four round, we will peel off the outermost two round first) and analyzing the inner two rounds. 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 $(y \oplus k_6 \oplus t)[i] = v$.

3. there exist a construction query $(t', x', y') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(t, x, y, i) \neq (t', x', y', j)$ and $(x \oplus k_0 \oplus t)[i] = (x' \oplus k_0 \oplus t)[j]$.

4. there exist a construction query $(t', x', y') \in \mathcal{Q}_C$ and an integer $i, j \in \{1, \ldots, w\}$ such that $(t, x, y, i) \neq (t, x', y', j)$ and $i \in \{1, \ldots, w\}$ such that $(y \oplus k_6 \oplus t)[i] = (y' \oplus k_6 \oplus t)[j]$.

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 $(1, (x \oplus k_0 \oplus t)[i], v'_1)_{1 \leq i \leq w}$ (if (t, x, y) collides at the input of S_1), or (if (t, x, y) collides at the output of S_6) $(6, u'_6, (y \oplus k_6 \oplus t)[i])_{1 \leq i \leq w}$, 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

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

In words, $\mathcal{Q}^{(1)}_{S_i}$ summarizes each constraint that is forced on S_i by $\mathcal{Q}_S$ and $\mathcal{Q}'_{S_1}$. Let

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

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

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

In words, α_1 (resp. α_6) is the number of queries $(t, x, y) \in \mathcal{Q}_C$ which collide with a query $(u_1, v_1) \in \mathcal{Q}^{(1)}_{S_1}$ (resp. $(u_6, v_6) \in \mathcal{Q}^{(1)}_{S_6}$) 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 $(u_1, v_1) \in \mathcal{Q}^{(0)}_{S_1}$ (resp. which collide with a query $(u_6, v_6) \in \mathcal{Q}^{(0)}_{S_6}$) 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

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

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

5.1 Bad Transcript for 6-rounds tweakable linear SPN and Probability

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

- (E-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 $(y \oplus k_6 \oplus t)[j] = v_6$.
- (E-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 $(T_1(S_1(x \oplus k_0 \oplus t) \oplus k_1 \oplus t))[j] = u_2$.
- (E-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 $\left(T_5^{-1}\left(S_6^{-1}(y \oplus k_6 \oplus t)\right) \oplus k_5 \oplus t\right)[i] = v_5$.
- (E-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 $(y \oplus k_6 \oplus t)[i] = (y \oplus k_6 \oplus t)[j]$.

Lemma 10 *One has*

$$\Pr[\tau' \in \Theta_{bad}(\tau)] \leq \frac{w^2q(p+wq)(3p+wq)}{N^2} + \frac{w^2q}{N}. \tag{12}$$

Proof: We fix any extended transcript, denoted $\left(\mathcal{Q}_C, \mathcal{Q}_S, \mathcal{Q}'_{S_{outmost}}\right)$. For any fixed construction query $(t,x,y) \in \mathcal{Q}_C$, now we upper bound the probabilities of the bad extended transcript.

Consider (E-1): Since we have at most $w^2q(p+wq)^2$ choices for $(t,x,y) \in \mathcal{Q}_C, (u_1,v_1) \in \mathcal{Q}_{S_1}^{(1)}, (u_6,v_6) \in \mathcal{Q}_{S_6}^{(1)}$ and index $i,j \in \{1,\ldots,w\}$ and since the random choice of k_0 and k_6 are independent, one has

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

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

Then consider (B-4). We assume that $w \neq 2$, because of $w = 1$ does not belong to the primary problem of the SP-networks. Since the random choice of k_0 and k_6 are independent, then we have

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

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 $\mathbf{k} = (k_0,k_1,k_2,k_3,k_4,k_5,k_6)$. After define the extended transcript τ'' is bad,

Lemma 11 *One has*

$$\Pr[\tau'' \in \Theta_{bad}(\tau)] \leq \frac{w^2q(p+wq)(3p+wq)}{N^2} + \frac{w^2q}{N}. \tag{13}$$

The proof is similar to Lemma 10.

Then combine (11), (12), we can get

$$\Pr[\tau \in \Theta_{bad}(\tau)] \leq \frac{2w^2q(p+wq)(3p+wq)}{N^2} + \frac{2w^2q}{N}. \tag{14}$$

5.2 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*

$$1 - \Pr\left[\mathrm{Bad}\left(S_1, S_2, S_5, S_6\right) | S_1 \vdash \mathcal{Q}_{S_1}, S_2 \vdash \mathcal{Q}_{S_2}, S_5 \vdash \mathcal{Q}_{S_5}, S_6 \vdash \mathcal{Q}_{S_6}\right] \geq 1 - \frac{2w^2q(p+wq)^2}{(N-p)}$$
$$- \frac{2w^2q(p+wq)(p+wq+2q)}{N \cdot (N-p)} - \frac{w^2q(p+wq)(p+wq+2q)}{(N-p)^2} - \frac{2w^2q^2(p+wq)}{(N-p-wq) \cdot (N-p)}. \tag{15}$$

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:

(F-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 $(T_2 (c \oplus k_2 \oplus t))[i] = u_3$ and $\left(T_4^{-1} (d) \oplus k_4 \oplus t\right)[i] = v_4$.

(F-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 $(T_2 (c \oplus k_2 \oplus t))[i] = u_3$ and $(T_3 (S_3 (T_2 (c \oplus k_2 \oplus t)) \oplus k_3 \oplus t))[j] = u_4$.

(F-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 $\left(T_3^{-1} \left(S_4^{-1} \left(T_4^{-1} (d) \oplus k_4 \oplus t\right)\right) \oplus k_3 \oplus t\right)[j] = v_3$.

(F-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

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

(F-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

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

(F-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 $(T_2(c\oplus k_2\oplus t))[i] = u_3, (T_2(c'\oplus k_2\oplus t'))[i] = u_3'$ and

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

(F-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

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

(F-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

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

(F-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

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

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

Proof: We just consider (F-6) and (F-9) here (Others are similar to the Lemma 8). 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

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

Acknowledgements

Chun Guo was partly supported by the Program of Qilu Young Scholars (Grant No. 61580089963177) of Shandong University. Weijia Wang was partly supported by the Program of Qilu Young Scholars of Shandong University. Meiqin Wang was supported by ...