

Provable Security of Substitution-Permutation Networks

Yevgeniy Dodis¹, Jonathan Katz², John Steinberger³, Aishwarya
Thiruvengadam², and Zhe Zhang³

¹ Dept. of Computer Science, New York University, USA
dodis@cs.nyu.edu

² Dept. of Computer Science, University of Maryland, USA
{jkatz,aish}@cs.umd.edu

³ Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing
{jpsteinb,leomwzz}@gmail.com

Abstract. Many modern block ciphers are constructed based on the paradigm of substitution-permutation networks (SPNs). But, somewhat surprisingly—especially in comparison with Feistel networks, which have been analyzed by dozens of papers going back to the seminal work of Luby and Rackoff—there are essentially no provable-security results about SPNs. In this work, we initiate a comprehensive study of the security of SPNs as strong pseudorandom permutations when the underlying “*S*-box” is modeled as a public random permutation. We show that 3 rounds of *S*-boxes are necessary and sufficient for secure *linear* SPNs, but that even 1-round SPNs can be secure when non-linearity is allowed.

1 Introduction

Modern block ciphers are generally constructed using two main paradigms [19]: Feistel networks [13] or substitution-permutation networks (SPNs) [29, 13]. These two approaches share the same goal: namely, to extend a “pseudorandom object” on a small domain to a (keyed) pseudorandom permutation on a larger domain by repeating a few, relatively simple operations several times across multiple rounds. Simplifying somewhat, Feistel networks begin with a keyed pseudorandom function on n -bit inputs and extend this to give a keyed pseudorandom permutation on $2n$ -bit inputs; SPNs start with one or more public “random permutations” on n -bit inputs and extend them to give a keyed pseudorandom permutation on wn -bit inputs for some w . Examples of block ciphers based on Feistel networks include DES, FEAL, MISTY and KASUMI; block ciphers based on SPNs include AES, Serpent, and PRESENT.

Although proving security unconditionally for any concrete block cipher is beyond current techniques, we can still hope to prove that particular approaches to constructing block ciphers are sound in an appropriate theoretical framework. Starting with the seminal paper by Luby and Rackoff [20] in the 1980s, there are by now dozens of papers that use this approach to prove security of Feistel

networks (of sufficiently many rounds), i.e., showing that if the underlying building block is an n -bit pseudorandom function then the resulting construction is a $2n$ -bit pseudorandom permutation. In contrast, it is somewhat surprising that there are almost no results about provable security of SPNs. (We discuss relevant prior work below.) Here, we address this gap and explore conditions under which SPNs can be proven secure.

1.1 Our Model and Results

An SPN on wn -bit inputs is computed via repeated invocation of two basic steps: a *substitution step* in which a public (unkeyed) “cryptographic” permutation $S : \{0, 1\}^n \rightarrow \{0, 1\}^n$, called an *S-box*, is computed in a blockwise fashion over the wn -bit intermediate state, and a *permutation step* in which a keyed but “non-cryptographic” permutation on $\{0, 1\}^{wn}$ is applied. An r -round SPN uses r rounds of *S*-boxes (plus an additional permutation step at the beginning). We consider both linear and non-linear SPNs; in a linear SPN, the keyed permutation in each round is linear (or, more generally, affine) in both the key and the intermediate state.

The only “cryptographic hardness” comes from the *S*-box, and we capture this by modeling S as a public, random permutation available to all parties as an oracle. This is a key difference between our work and most prior work analyzing security of SPNs (see Section 1.2), which treated the *S*-box as a key-dependent, random permutation inaccessible to the adversary. In practical constructions of block ciphers, however, the *S*-box is typically unkeyed.

We analyze SPNs in the standard sense of security against adaptive chosen-plaintext and chosen-ciphertext attacks; that is, we analyze the SPN as a strong pseudorandom permutation [20]. We first characterize the security of *linear* SPNs. Based on an attack given by Halevi and Rogaway [16] (credited there to [18]), we show that no 2-round linear SPN with $w \geq 2$ can be secure. (Even a 1-round linear SPN can be secure when $w = 1$; see below for the significance of this result.) Complementing this, and giving a tight characterization, we show that 3-round linear SPNs *are* secure, for any w , if the keyed permutations satisfy some mild technical requirements.

In an effort to reduce the number of rounds, we then turn our attention to non-linear SPNs. Here we show that even a 1-round SPN can be secure if appropriate keyed permutations are used. We identify a combinatorial property on the permutations that suffices for security in this case, and then study the efficiency of constructing permutations satisfying this property. Specifically, we show a construction of a satisfactory permutation with n -bit keys (but having high degree), and another construction with longer keys but having degree 3.

Implications. We view our results as providing support for the SPN approach to constructing block ciphers, but we caution that they say little about any concrete SPN-based block cipher. This is especially true since our positive results (inherently) achieve security only for $q < 2^n$ queries, yet practical constructions tend to use *S*-boxes with a very small domain (e.g., $n \leq 32$).

Although an SPN with $w = 1$ (i.e., no domain extension) may seem uninteresting, it captures the well-known Even-Mansour construction [12] of a keyed pseudorandom permutation from a public random permutation. Our positive results imply security of the Even-Mansour construction (with similar concrete security bounds) as a special case, even in the setting where the pre- and post-whitening keys are identical [11].

An SPN structure can also be used for domain extension of a block cipher, i.e., for building a block cipher F' with wn -bit block length from a block cipher F having n -bit block length. Our results imply security in that setting as well. Although several prior papers have considered this problem (see below), we appear to be the first to analyze it in the case where the attacker is given access to the internal function F , which would correspond in practice to publicly fixing the key to F (thus potentially improving the efficiency of F').

1.2 Related Work

There are only a few prior papers looking at provable security of SPNs. The vast majority of such work analyzes the case of secret, key-dependent S -boxes (rather than public S -boxes as we consider here), and so we survey that work first.

SPNs with secret S -boxes. Naor and Reingold [24] prove security for what can be viewed as a non-linear, 1-round SPN. Their ideas were further developed, in the context of domain extension for block ciphers (see further discussion below), by Chakraborty and Sarkar [5] and Halevi [14].

Iwata and Kurosawa [17] analyze SPNs in which the linear permutation step is based on the specific permutations used in the block cipher Serpent. They show an attack against 2-round SPNs of this form, and prove security for 3-round SPNs against non-adaptive adversaries. In addition to the fact that we consider public S -boxes, our linear SPN model considers generic linear permutations and we prove security against adaptive attackers.

Miles and Viola [23] study SPNs from a complexity-theoretic viewpoint. Two of their results are relevant here. First, they analyze the security of linear SPNs using S -boxes that are not necessarily injective (so the resulting keyed functions are not, in general, invertible). They show that r -round SPNs of this type (for $r \geq 2$) are secure against chosen-plaintext attacks. (In contrast, our results show that 2-round, linear SPNs are not secure against a combination of chosen-plaintext and chosen-ciphertext attacks when $w \geq 2$.) They also analyze SPNs based on a concrete set of S -boxes, but in this case they only show security against linear/differential attacks (a form of chosen-plaintext attack), rather than all possible attacks, and only when the number of rounds is $r = \Theta(\log n)$.

SPNs with public S -boxes. A difference between our work and all the work discussed above is that we treat the S -boxes as public. We are aware of only one prior work analyzing the provable security of SPNs in this setting. Dodis et al. [10] recently studied the *indifferentiability* [21] of confusion-diffusion networks, which can be viewed as *unkeyed* SPNs. One could translate their results to the keyed setting, but that would require using multiple, key-dependent S -boxes

(rather than a fixed, public S -box) and so would not imply our results. We remark further that they show positive results only for 5 rounds and above.

As observed earlier, the Even-Mansour construction [12] of a (keyed) pseudorandom permutation from a public random permutation can be viewed as a 1-round, linear SPN in the degenerate case where $w = 1$ (i.e., no domain extension) and all round permutations are instantiated using simple key mixing. Security of the 1-round Even-Mansour construction against adaptive chosen-plaintext/ciphertext attacks, using independent keys for the initial and final key mixing, was shown in the original paper [12]. Dunkelman, Keller, and Shamir [11] showed that security holds even if the keys used are the same. Our positive results imply security of the 1-round Even-Mansour construction (with similar concrete security bounds) as a special case.

Cryptanalysis of SPNs. Researchers have also explored cryptanalytic attacks on generic SPNs [3, 1, 9, 2]. These works generally consider a model of SPNs in which round permutations are secret, random (invertible) linear transformations, and S -boxes may be secret as well; this makes the attacks stronger but positive results weaker. In many cases the complexities of the attacks are exponential in n (though still faster than a brute-force search for the key), and hence do not rule out asymptotic security results. On the positive side, Biryukov et al. [1] show that 2-round SPNs (of the stronger form just mentioned) are secure against some specific types of attacks, but other attacks on such schemes have recently been identified [9].

Domain extension of block ciphers. It is worth noting that our results also address the problem of *domain extension* for block ciphers. That is, we may view a block cipher F having an n -bit block length as an n -bit S -box (either viewing F as an ideal cipher, fixing its key, and thus viewing it as a public S -box, or viewing F as a pseudorandom permutation, keeping the key secret, and so viewing it as a secret S -box), and then use it in a SPN construction to obtain a block cipher on wn -bit inputs for $w > 1$. As mentioned earlier, non-linear, 1-round SPNs with secret S -boxes have been used for domain extension of block ciphers before [5, 14]. Other approaches for domain extension, not relying on (pure) SPNs, have also been considered [4, 15, 16, 22, 7]. Our main motivation, however, is not to beat prior approaches to domain extension, but rather to study the security of SPNs as used in practice to construct block ciphers.

2 Preliminaries

For $i \in \mathbb{N}$, we let $[i]$ denote the set $\{1, \dots, i\}$. We write $\text{Perm}(m)$ for the set of permutations of $\{0, 1\}^m$. We view n as a cryptographic security parameter and let $\mathbb{F} \stackrel{\text{def}}{=} \text{GF}(2^n)$, which is identified with $\{0, 1\}^n$. If $x \in \mathbb{F}^w = \{0, 1\}^{wn}$, then we denote the j th entry of x (for $j \in [w]$) by $x[j]$.

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 is defined by $r + 1$ keyed permutations $\{\pi_i : K_i \times \{0, 1\}^{wn} \rightarrow \{0, 1\}^{wn}\}_{i=0}^r$, a distribution \mathcal{K} over⁴ $K_0 \times \dots \times K_r$, and a permutation $S : \{0, 1\}^n \rightarrow \{0, 1\}^n$. Given round keys k_0, \dots, k_r and input $x \in \{0, 1\}^{wn}$, the output of the SPN is computed as follows (cf. Figure 1):

- Let⁵ $x_1 := \pi_0(k_0, x)$.
- For $i = 1$ to r do:
 1. $y_i := \tilde{S}(x_i)$, where $\tilde{S}(x[1] \parallel \dots \parallel x[w]) \stackrel{\text{def}}{=} S(x[1]) \parallel \dots \parallel S(x[w])$.
 2. $x_{i+1} := \pi_i(k_i, y_i)$.
- The output is x_{r+1} .

If 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, \dots, k_r .

In our definition of an SPN, we apply a fixed permutation S to all w blocks of the intermediate state in each round. More generally, one could consider using w different functions S_1, \dots, S_w in each round, or even different S -boxes in different rounds. Our positive results hold even when a single permutation S is used, and our negative result holds even if multiple permutations are used.

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. *Keyed permutation $\pi : \mathbb{F}^w \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ is linear⁶ if*

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

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

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

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

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

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

⁴ In practice, the *round keys* are derived from a single, master key using a prescribed *key schedule*, but for our purposes we leave this process implicit in the distribution \mathcal{K} .

⁵ Initial application of a keyed permutation is necessary, since otherwise the attacker could compute \tilde{S} in round 1 on its own, making that round ineffective.

⁶ We could also call it *affine*, but we show shortly that $\Delta = 0$ without loss of generality.

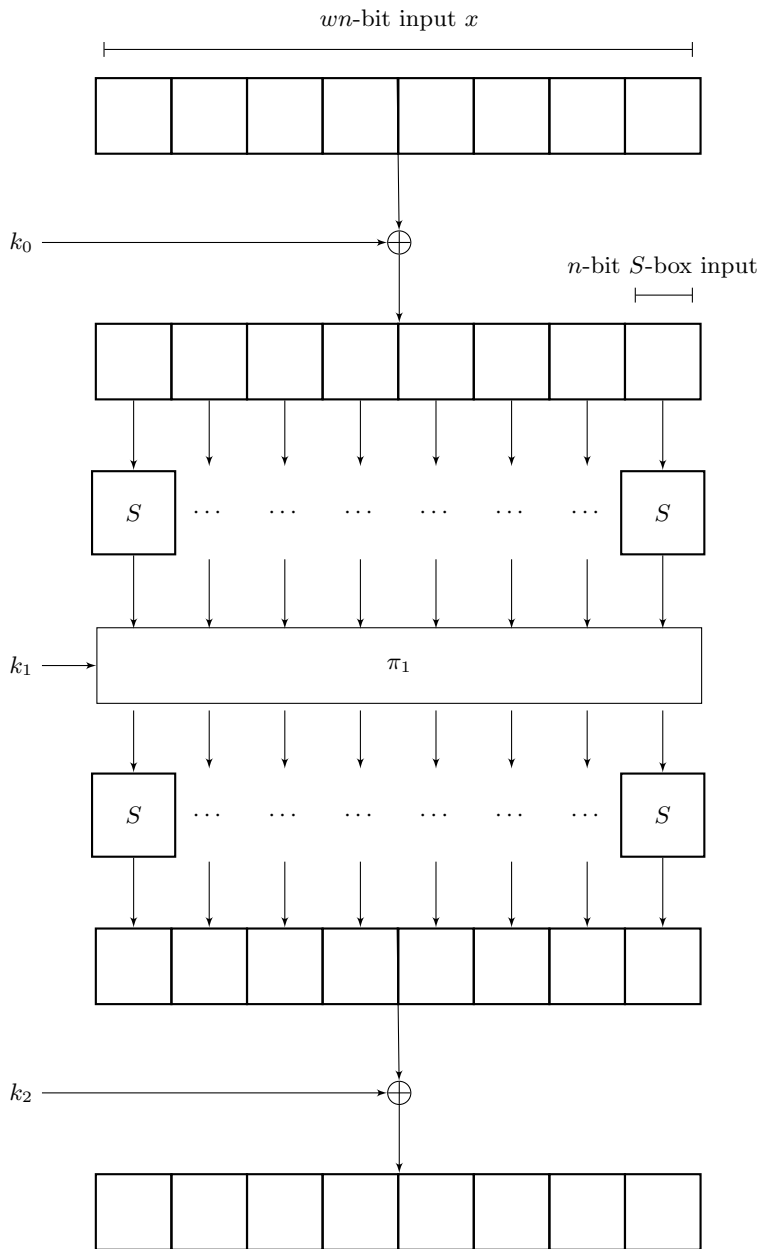


Fig. 1. A 2-round, linear SPN.

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 [19]. 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 $\pi_i(k_i, x) = k_i \oplus x$ for $i \in \{0, r\}$.

Security of an SPN. Our goal is to prove that certain SPNs are strong pseudorandom permutations. We cannot hope to prove such a result unconditionally; instead, we look at SPN *constructions* that are defined by permutations $\{\pi_i : K_i \times \{0, 1\}^{wn} \rightarrow \{0, 1\}^{wn}\}_{i=0}^r$ and a distribution \mathcal{K} , and that take *oracle access* to a public, random function $S : \{0, 1\}^n \rightarrow \{0, 1\}^n$; we write this as \mathcal{C}^S . We then analyze security of the construction against unbounded-time attackers making a bounded number of queries to the construction and to S . Formally, we consider the ability of an adversary D to distinguish two worlds: the “real world,” in which it is given oracle access to S and $\mathcal{C}_{k_0, \dots, k_r}^S$ (for unknown keys k_0, \dots, k_r sampled according to \mathcal{K}), and an “ideal world” in which it has access to S and an independent, random permutation $P : \{0, 1\}^{wn} \rightarrow \{0, 1\}^{wn}$. By default, we always allow D to make forward and inverse queries to both its oracles (though we do not write this explicitly). We have:

Definition 2. *The strong-PRP advantage of a distinguisher D against SPN construction \mathcal{C} is:*

$$\text{Adv}_{\mathcal{C}}(D) \stackrel{\text{def}}{=} \left| \Pr \left[(k_0, \dots, k_r) \leftarrow \mathcal{K} : D^{\mathcal{C}_{k_0, \dots, k_r}^S, S} = 1 \right] - \Pr \left[D^{P, S} = 1 \right] \right|,$$

where P and S are independent, uniform permutations on $\{0, 1\}^{wn}$ and $\{0, 1\}^n$, respectively. The strong-PRP security of \mathcal{C} is

$$\text{Adv}_{\mathcal{C}}(q_C, q_S) \stackrel{\text{def}}{=} \max_D \{ \text{Adv}_{\mathcal{C}}(D) \},$$

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

2.2 The H-coefficient Technique

We use the H-coefficient technique [25–27] to prove various indistinguishability results. We provide a quick overview of its main ingredients here. Our presentation borrows heavily from that of Chen and Steinberger [6]; for further details, refer there or to the tutorial by Patarin [28].

Fix a distinguisher D that makes at most q queries to its oracles. As in the security definition presented above, D ’s aim is to distinguish between two worlds: a “real world” and an “ideal world”. Assume without loss of generality that D is deterministic. The execution of D defines a *transcript* that includes the sequence of queries and answers received from its oracles; D ’s output is a deterministic function of its transcript. Thus if X, Y denote the probability

distributions on transcripts induced by the real and ideal worlds, respectively, then D 's distinguishing advantage is upper bounded by the statistical distance

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

where the sum is taken over all possible transcripts τ .

Let \mathcal{T} denote the set of all transcripts that can be generated by 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

$$\tau \in \mathcal{T}_1 \implies \Pr[X = \tau] / \Pr[Y = \tau] \geq 1 - \epsilon_1. \quad (2)$$

It is then possible to show (see [6] for details) that

$$\Delta(X, Y) \leq \epsilon_1 + \Pr[Y \in \mathcal{T}_2] \quad (3)$$

is an upper bound on the distinguisher's advantage. One should think of ϵ_1 and $\Pr[Y \in \mathcal{T}_2]$ as “small,” so “good” transcripts have nearly the same probability of appearing in the real world and the ideal world, whereas “bad” transcripts have low probability of occurring in the ideal world.

An appeal of the H-coefficient technique is that it handles arbitrary adaptive distinguishers even though the technical calculations involve *a posteriori* probabilities computed with respect to finalized transcripts.

3 Linear SPNs

We begin by exploring the security of linear SPNs. We first show that 2-round linear SPNs cannot be secure against adaptive chosen-plaintext/ciphertext attacks when $w \geq 2$. Complementing this result, and giving a tight characterization, we then prove that 3-round linear SPNs can be secure when the round permutations and keys are chosen appropriately.

3.1 Insecurity of 2-Round, Linear SPNs

We present an attack showing that 2-round, linear SPNs (cf. Figure 1) cannot be secure for $w \geq 2$. The attack is based on one shown by Halevi and Rogaway [16] in a different context; our contribution here is to observe that the attack is applicable to any 2-round, linear SPN.

Recall from the previous section that any 2-round, linear SPN can be expressed in the following form. On input $x_0 \in \mathbb{F}^w$ and keys $k_0, k_1, k_2 \in \mathbb{F}^w$ do:

1. Compute $x_1 := x_0 \oplus k_0$ followed by $y_1 := \tilde{S}(x_1)$.
2. Compute $x_2 := \pi_1(k_1, y_1) = T \cdot (y_1 \oplus k_1)$ for some invertible linear transformation T .
3. Compute $y_2 := \tilde{S}(x_2)$ followed by $x_3 := y_2 \oplus k_2$, and return x_3 .

We show an attacker D , given access to an oracle $\mathcal{O} : \{0, 1\}^{wn} \rightarrow \{0, 1\}^{wn}$ (with $w \geq 2$), that distinguishes whether \mathcal{O} is an instance of the above construction (using uniform keys k_0, k_1, k_2) or a random permutation on $\{0, 1\}^{wn}$. The attacker D proceeds as follows:

1. Choose inputs x_0, x'_0 that are equal on all blocks except the first.
2. Query $\mathcal{O}(x_0)$ and $\mathcal{O}(x'_0)$ to obtain x_3 and x'_3 respectively.
3. Set $\hat{x}_3 := x'_3[1] \parallel x_3[2] \parallel \dots \parallel x_3[w]$ and $\hat{x}'_3 := x_3[1] \parallel x'_3[2] \parallel \dots \parallel x'_3[w]$. Then query $\mathcal{O}^{-1}(\hat{x}_3)$ and $\mathcal{O}^{-1}(\hat{x}'_3)$ to obtain \hat{x}_0 and \hat{x}'_0 respectively.
4. If $\hat{x}_0[2] \parallel \dots \parallel \hat{x}_0[w] = \hat{x}'_0[2] \parallel \dots \parallel \hat{x}'_0[w]$, then output 1; otherwise, output 0.

It is not hard to see that if \mathcal{O} is a random permutation on $\{0, 1\}^{wn}$ then D outputs 1 with negligible probability. On the other hand, we claim that when \mathcal{O} is an instance of the above construction then D always outputs 1. To see this, let y_1, x_2 be the intermediate values during evaluation of $\mathcal{O}(x_0)$; let y'_1, x'_2 be the intermediate values during evaluation of $\mathcal{O}(x'_0)$; let \hat{y}_1, \hat{x}_2 be the intermediate values during evaluation of $\mathcal{O}^{-1}(\hat{x}_3)$; and let \hat{y}'_1, \hat{x}'_2 be the intermediate values during evaluation of $\mathcal{O}^{-1}(\hat{x}'_3)$. Observe first that $\hat{x}_2 \oplus \hat{x}'_2 = x_2 \oplus x'_2$. From this it follows that

$$\begin{aligned}
\hat{y}_1 \oplus \hat{y}'_1 &= (T^{-1}\hat{x}_2 \oplus k_1) \oplus (T^{-1}\hat{x}'_2 \oplus k_1) \\
&= T^{-1} \cdot (\hat{x}_2 \oplus \hat{x}'_2) \\
&= T^{-1} \cdot (x_2 \oplus x'_2) \\
&= T^{-1} \cdot (Ty_1 \oplus Ty'_1) \\
&= T^{-1} \cdot (T \cdot (y_1 \oplus y'_1)) \\
&= y_1 \oplus y'_1.
\end{aligned}$$

Since y_1 and y'_1 are equal on all but their first blocks (by construction of x_0, x'_0), we conclude that \hat{y}_1 and \hat{y}'_1 also agree everywhere but in their first blocks. But this implies that \hat{x}_0 and \hat{x}'_0 are equal everywhere except in their first blocks, and so D outputs 1.

We remark that D makes only four queries to the construction—two in the forward direction, and two in the inverse direction—and no queries to S . We also note that the attack does not require linearity of T ; it suffices for the permutation T to be *additive*, i.e., for T to satisfy

$$\forall x, y \in \{0, 1\}^{wn} : T(x + y) = T(x) + T(y).$$

(Note that additivity of T implies additivity of T^{-1} .) Since \mathbb{F} has characteristic 2, the “blockwise squaring” transformation $T : \mathbb{F}^w \rightarrow \mathbb{F}^w$ where $T(x)[j] = x[j]^2$ for all $j \in [w]$ is an example of a transformation that is additive but nonlinear.

3.2 Security of 3-Round, Linear SPNs

We now explore conditions under which 3-round, linear SPNs are secure. Recall from Section 2.1 that a 3-round SPN has four round permutations $\{\pi_i\}_{i=0}^3$, and

without loss of generality we may assume

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

where $T_1, T_2 \in \mathbb{F}^{w \times w}$ are invertible linear transformations. We prove that a 3-round, linear SPN is secure so long as (i) T_1 and T_2^{-1} contain no zero entries (Miles and Viola [23] show that matrices with maximal branch number [8] satisfy this property), and (ii) round keys k_0 and k_3 are (individually) uniform.

Theorem 1. *Assume $w > 1$. Let \mathcal{C} be a 3-round, linear SPN with round permutations as in (4) and with distribution \mathcal{K} over keys k_0, k_1, k_2, k_3 . If k_0 and k_3 are uniformly distributed and the matrices T_1, T_2^{-1} contain no zero entries, then*

$$\text{Adv}_{\mathcal{C}}(q_C, q_S) \leq \frac{5w^2q_C^2 + 4wq_Cq_S}{2^n - q_S - 2w} + \frac{q_C^2}{2^{wn}}.$$

Proof. Fix a deterministic distinguisher D . Without loss of generality, we assume D makes exactly q_C (non-redundant) forward/inverse queries to its left oracle that is either \mathcal{C}_k^S or P , and exactly q_S (non-redundant) forward/inverse queries to its right oracle that is the S -box. We call a query from D to its left oracle a *construction query* (even though in the ideal world the oracle is P), and a query from D to its right oracle an *S -box query*.

The interaction between D and its oracles can be recorded in the form of two sets of pairs $Q_C \subseteq \{0, 1\}^{wn} \times \{0, 1\}^{wn}$ and $Q_S \subseteq \{0, 1\}^n \times \{0, 1\}^n$, where Q_C contains every pair (x, y) for which D made a construction query x that was answered by y or an inverse query y that was answered by x , and Q_S is defined similarly with respect to S -box queries. Note that D 's interaction with its oracles can be unambiguously reconstructed from these sets since D is deterministic.

Following [6], we augment the transcript (Q_C, Q_S) with a *key value* $k = (k_0, k_1, k_2, k_3)$. In the real world, k is the actual key used by the construction. In the ideal world, k is a dummy key sampled independently from all other values according to the prescribed key distribution \mathcal{K} . Thus, a transcript τ has the final form $\tau = (Q_C, Q_S, k_0, k_1, k_2, k_3)$.

Let \mathcal{T} be set of all transcripts that can be generated with nonzero probability in the ideal world. (This includes all transcripts that can be generated with nonzero probability in the real world.) As in Section 2.2, let X, Y be the distributions over transcripts in the real and ideal worlds, respectively.

We define a set $\mathcal{T}_2 \subseteq \mathcal{T}$ of *bad transcripts* as follows: a transcript $\tau = (Q_C, Q_S, k_0, k_1, k_2, k_3)$ is bad if and only if one of these events occurs:

1. There exist a pair $(x, y) \in Q_C$, a pair $(a, b) \in Q_S$, and an index $j \in [w]$ such that $(x \oplus k_0)[j] = a$ or $(y \oplus k_3)[j] = b$.
2. There exist a pair $(x, y) \in Q_C$ and distinct indices $j, j' \in [w]$ such that $(x \oplus k_0)[j] = (x \oplus k_0)[j']$ or $(y \oplus k_3)[j] = (y \oplus k_3)[j']$.
3. There exist distinct pairs $(x, y), (x', y') \in Q_C$ and distinct indices $j, j' \in [w]$ such that $(x \oplus k_0)[j] = (x' \oplus k_0)[j']$ or $(y \oplus k_3)[j] = (y' \oplus k_3)[j']$.

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

Since, in the ideal world, the values k_0, k_3 are independent of Q_C, Q_S and (individually) uniform in $\{0, 1\}^{wn}$, a simple union bound shows that

$$\Pr[Y \in \mathcal{T}_2] < 2wq_Cq_S/2^n + w(w-1)q_C/2^n + w(w-1)q_C(q_C-1)/2^n$$

where the three terms account for the three events above, in that order. Thus

$$\Pr[Y \in \mathcal{T}_2] \leq 2wq_Cq_S/2^n + w(w-1)q_C^2/2^n. \quad (5)$$

This gives us “one half” of (3).

In order to finish applying the H-coefficient technique, it remains to lower bound the ratio

$$\frac{\Pr[X = \tau]}{\Pr[Y = \tau]}$$

for $\tau \in \mathcal{T}_1$. Let $\Omega_X = \text{Perm}(n) \times K$ be the probability space underlying the real world, whose measure is the product of the uniform measure on $\text{Perm}(n)$ and the measure induced by the distribution \mathcal{K} on keys. (Thus, each element of Ω_X is a pair (S, k) with $S \in \text{Perm}(n)$ and $k = (k_0, k_1, k_2, k_3) \in K$.) Also let

$$\Omega_Y = \text{Perm}(wn) \times \text{Perm}(n) \times K$$

be the probability space underlying the ideal world, whose measure is the product of the uniform measure on $\text{Perm}(wn)$ with the measure on Ω_X .

Let $\nu = (Q_C^\nu, Q_S^\nu, k^\nu)$ be a transcript. An element $\omega = (S^*, k^*) \in \Omega_X$ is *compatible with ν* if $k^* = k^\nu$, if $S^*(a) = b$ for all $(a, b) \in Q_S^\nu$, and if $\mathcal{C}_{k^*}^{S^*}(x) = y$ for all $(x, y) \in Q_C^\nu$. An element $\omega = (P^*, S^*, k^*) \in \Omega_Y$ is *compatible with ν* if $k^* = k^\nu$, if $S^*(a) = b$ for all $(a, b) \in Q_S^\nu$, and if $P^*(x) = y$ for all $(x, y) \in Q_C^\nu$. We write

$$\omega \downarrow \nu$$

to indicate that an element $\omega \in \Omega_X \cup \Omega_Y$ is compatible with ν .

For the rest of the proof we fix a transcript $\tau = (Q_C, Q_S, k) \in \mathcal{T}_1$ so, in particular, Q_C, Q_S , and k will be fixed for the rest of the proof. Since $\tau \in \mathcal{T}$, it is easy to see (cf. [6]) that

$$\Pr[X = \tau] = \Pr_{\omega \leftarrow \Omega_X}[\omega \downarrow \tau] \quad (6)$$

$$\Pr[Y = \tau] = \Pr_{\omega \leftarrow \Omega_Y}[\omega \downarrow \tau], \quad (7)$$

where the notation indicates that ω is sampled from the relevant probability space according to that space’s probability measure. (In other words, the probability of obtaining τ in each world is just the probability that the random coins of that world are “compatible” with τ in the sense outlined above.) We bound $\Pr[X = \tau]/\Pr[Y = \tau]$ by reasoning about the latter probabilities.

As additional notation/terminology:

- Say that $S^* \in \text{Perm}(n)$ is *compatible* with a transcript $\nu = (Q_C^\nu, Q_S^\nu, k^\nu)$, and write $S^* \downarrow \nu$, if $(S^*, k) \in \Omega_X$ is compatible with ν , where k is the key value of the fixed transcript τ .

- Likewise, say that $(P^*, S^*) \in \text{Perm}(wn) \times \text{Perm}(n)$ is *compatible* with a transcript $\nu = (Q_C^\nu, Q_S^\nu, k^\nu)$, and write $(P^*, S^*) \downarrow \nu$, if $(P^*, S^*, k^\nu) \downarrow \nu$.

Incorporating these notations, the product structure of Ω_X, Ω_Y implies

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

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

$$\frac{\Pr[X = \tau]}{\Pr[Y = \tau]} = \frac{\Pr_{S^*}[S^* \downarrow \tau]}{\Pr_{P^*, S^*}[(P^*, S^*) \downarrow \tau]}.$$
 (8)

It is immediate that

$$\Pr_{P^*, S^*}[(P^*, S^*) \downarrow \tau] = \frac{(2^{wn} - q_C)!}{2^{wn}!} \cdot \frac{(2^n - q_S)!}{2^n!}$$
 (9)

since Q_C, Q_S have size exactly q_C, q_S , respectively.

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

$$\begin{aligned}\Pr_{S^*}[S^* \downarrow \tau] &= \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k)] \\ &= \Pr_{S^*}[S^* \downarrow (\emptyset, Q_S, k)] \cdot \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid S^* \downarrow (\emptyset, Q_S, k)] \\ &= \frac{(2^n - q_S)!}{2^n!} \cdot \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid S^* \downarrow (\emptyset, Q_S, k)].\end{aligned}$$
 (10)

Define

$$\begin{aligned}\text{Dom}(\tau) &\stackrel{\text{def}}{=} \{a \in \{0, 1\}^n : (a, b) \in Q_S \text{ for some } b \in \{0, 1\}^n\} \\ \text{Range}(\tau) &\stackrel{\text{def}}{=} \{b \in \{0, 1\}^n : (a, b) \in Q_S \text{ for some } a \in \{0, 1\}^n\} \\ \text{ExtDom}(\tau) &\stackrel{\text{def}}{=} \{(x \oplus k_0)[j] : (x, y) \in Q_C, j \in [w]\} \\ \text{ExtRange}(\tau) &\stackrel{\text{def}}{=} \{(y \oplus k_3)[j] : (x, y) \in Q_C, j \in [w]\}.\end{aligned}$$

Note that $\text{ExtDom}(\tau)$ (resp., $\text{ExtRange}(\tau)$) contains all the first-round S -box inputs (resp., third-round S -box outputs) corresponding to the construction queries in Q_C . We let $\text{Good}(S^*)$ be a predicate of S^* that holds if and only if all the following conditions are met (as usual, \tilde{S}^* denotes blockwise evaluation of S^* on a wn -bit string):

1. $S^* \downarrow (\emptyset, Q_S, k)$.
2. $T_1(\tilde{S}^*(x \oplus k_0) \oplus k_1)[j] \notin \text{Dom}(\tau) \cup \text{ExtDom}(\tau)$ for all $(x, y) \in Q_C$ and all $j \in [w]$.
3. $(T_2^{-1}\tilde{S}^{*-1}(y \oplus k_3) \oplus k_2)[j] \notin \text{Range}(\tau) \cup \text{ExtRange}(\tau)$ for all $(x, y) \in Q_C$ and all $j \in [w]$.

4. $T_1(\tilde{S}^*(x \oplus k_0) \oplus k_1)[j] \neq T_1(\tilde{S}^*(x' \oplus k_0) \oplus k_1)[j']$ for all distinct tuples $(x, y, j), (x', y', j') \in Q_C \times [w]$.
5. $(T_2^{-1}\tilde{S}^{*-1}(y \oplus k_3) \oplus k_2)[j] \neq (T_2^{-1}\tilde{S}^{*-1}(y' \oplus k_3) \oplus k_2)[j']$ for all distinct tuples $(x, y, j), (x', y', j') \in Q_C \times [w]$.

The second condition requires that no second-round S -box inputs are in $\text{Dom}(\tau) \cup \text{ExtDom}(\tau)$, and the fourth condition requires that all second-round S -box inputs are distinct; the third and fifth conditions parallel these, but for second-round S -box *outputs*.

We have

$$\begin{aligned}
& \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid S^* \downarrow (\emptyset, Q_S, k)] \\
& \geq \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \wedge \text{Good}(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)] \\
& = \Pr_{S^*}[\text{Good}(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)] \cdot \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid \text{Good}(S^*)], \quad (11)
\end{aligned}$$

using the fact that $\text{Good}(S^*) \implies S^* \downarrow (\emptyset, Q_S, k)$ for the final equality. Thus, all that remains is to lower bound the two terms in the product of (11).

Let $\text{Bad}_i(S^*)$ be the predicate that is true if and only if condition i in the definition of $\text{Good}(S^*)$ is violated. Note that

$$\Pr_{S^*}[\overline{\text{Good}(S^*)} \mid S^* \downarrow (\emptyset, Q_S, k)] \leq \sum_{i=2}^5 \Pr_{S^*}[\text{Bad}_i(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)],$$

since the first condition in the definition of $\text{Good}(S^*)$ cannot be violated here. We now upper bound $\Pr_{S^*}[\text{Bad}_i(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)]$ for $i = 2, 3, 4, 5$.

Lemma 1. $\Pr_{S^*}[\text{Bad}_2(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)] \leq wq_C(q_S + wq_C)/(2^n - q_S - w)$.

Proof. Fix some $(x, y) \in Q_C$ and an index $j \in [w]$. Since τ is a good transcript, $(x \oplus k_0)[i] \notin \text{Dom}(\tau)$ for all $i \in [w]$, and $(x \oplus k_0)[i] \neq (x \oplus k_0)[i']$ for $i' \neq i$. So after conditioning on $S^* \downarrow (\emptyset, Q_S, k)$ and the values of $S^*((x \oplus k_0)[i])$ for $i \neq 1$, the value $S^*((x \oplus k_0)[1])$ is uniform in a set of size $2^n - q_S - w + 1$. Because every entry in the first column of T_1 is nonzero, we have

$$\begin{aligned}
& \Pr_{S^*}[T_1(\tilde{S}^*(x \oplus k_0) \oplus k_1)[j] \in \text{Dom}(\tau) \cup \text{ExtDom}(\tau) \mid S^* \downarrow (\emptyset, Q_S, k)] \\
& \leq \frac{|\text{Dom}(\tau)| + |\text{ExtDom}(\tau)|}{2^n - q_S - w + 1} \\
& \leq \frac{q_S + wq_C}{2^n - q_S - w}.
\end{aligned}$$

The statement follows by a union bound over all $(x, y) \in Q_C, j \in [w]$. \square

Lemma 2. $\Pr_{S^*}[\text{Bad}_3(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)] \leq wq_C(q_S + wq_C)/(2^n - q_S - w)$.

Proof. (Symmetric to Lemma 1.) \square

Lemma 3. $\Pr_{S^*}[\text{Bad}_4(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)] \leq w^2 q_C^2 / (2^n - q_S - 2w)$.

Proof. Fix distinct $(x, y, j), (x', y', j') \in Q_C \times [w]$. Then either $(x, y) \neq (x', y')$ (which implies $x \neq x'$) or $x = x'$ but $j \neq j'$.

Assume first that $x \neq x'$. Then $x[i_0] \neq x'[i_0]$ for some $i_0 \in [w]$. By the definition of a good transcript, $(x \oplus k_0)[i_0] \neq (x \oplus k_0)[i]$ for all $i \neq i_0$ and $(x \oplus k_0)[i_0] \neq (x' \oplus k_0)[i]$ for all i . So after conditioning on $S^* \downarrow (\emptyset, Q_S, k)$ and the values of $S^*((x \oplus k_0)[i])$ for $i \neq i_0$ and $S^*((x' \oplus k_0)[i])$ for $i \in [w]$, the value of $S^*((x \oplus k_0)[i_0])$ is uniform in a set of size at least $2^n - q_S - 2w + 1$. Because every entry in the i_0 th column of T_1 is nonzero, we have

$$\begin{aligned} \Pr_{S^*}[T_1(\tilde{S}^*(x \oplus k_0) \oplus k_1)[j] = T_1(\tilde{S}^*(x' \oplus k_0) \oplus k_1)[j'] \mid S^* \downarrow (\emptyset, Q_S, k)] \\ \leq \frac{1}{2^n - q_S - 2w}. \end{aligned}$$

Assume next that $x = x'$ and so $j \neq j'$. Since T_1 is invertible, the j th and j' th rows of T_1 are linearly independent and, in particular, there exists an index $i_0 \in [w]$ such that the (j, i_0) th and (j', i_0) th entries of T_1 are not equal. After conditioning on $S^* \downarrow (\emptyset, Q_S, k)$ and the values of $S^*((x \oplus k_0)[i])$ for $i \neq i_0$, the value of $S^*((x \oplus k_0)[i_0])$ is uniform in a set of size $2^n - q_S - w + 1$. It follows that

$$\begin{aligned} \Pr_{S^*}[T_1(\tilde{S}^*(x \oplus k_0) \oplus k_1)[j] = T_1(\tilde{S}^*(x \oplus k_0) \oplus k_1)[j'] \mid S^* \downarrow (\emptyset, Q_S, k)] \\ \leq \frac{1}{2^n - q_S - w}. \end{aligned}$$

The statement now follows by taking a union bound over all possible pairs of distinct elements $(x, y, j), (x', y', j') \in Q_C \times [w]$. \square

Lemma 4. $\Pr_{S^*}[\text{Bad}_5(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)] \leq w^2 q_C^2 / (2^n - q_S - 2w)$.

Proof. (Symmetric to Lemma 3.) \square

Combining the bounds of Lemmas 1–4, we find

$$\begin{aligned} \Pr_{S^*}[\text{Good}(S^*) \mid S^* \downarrow (\emptyset, Q_S, k)] &\geq 1 - \frac{2w^2 q_C^2}{2^n - q_S - 2w} - \frac{2w q_C (q_S + w q_C)}{2^n - q_S - w} \\ &\geq 1 - \frac{4w^2 q_C^2 + 2w q_C q_S}{2^n - q_S - 2w}. \end{aligned} \quad (12)$$

Our next step is to lower bound the term $\Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid \text{Good}(S^*)]$ from (11). For any $S_\perp \in \text{Perm}(n)$ such that $\text{Good}(S_\perp)$ is true, define

$$Q^{\text{Ext}}(S_\perp) = \{(a, S_\perp(a))\}_{a \in \text{ExtDom}(\tau)} \cup \{(S_\perp^{-1}(b), b)\}_{b \in \text{ExtRange}(\tau)}.$$

Let $\text{Perm}_\perp(n) \subset \text{Perm}(n)$ be maximal such that the predicate $\text{Good}(S_\perp)$ holds for every $S_\perp \in \text{Perm}_\perp(n)$ and such that $Q^{\text{Ext}}(S_\perp) \neq Q^{\text{Ext}}(S'_\perp)$ for distinct

$S_\perp, S'_\perp \in \text{Perm}_\perp(n)$. (I.e., $\text{Perm}_\perp(n)$ is a system of representatives, with one representative per distinct value of $Q^{\text{Ext}}(S_\perp)$.) Then the event

$$\text{Good}(S^*) \wedge (S^* \downarrow (Q_C, Q_S, k))$$

is the disjoint union of the events

$$\{\text{Good}(S^*) \wedge (S^* \downarrow (Q_C, Q_S \cup Q^{\text{Ext}}(S_\perp), k))\}_{S_\perp \in \text{Perm}_\perp(n)},$$

and so

$$\begin{aligned} & \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid \text{Good}(S^*)] \\ &= \sum_{S_\perp \in \text{Perm}_\perp(n)} \Pr_{S^*}[S^* \downarrow (Q_C, Q_S \cup Q^{\text{Ext}}(S_\perp), k) \mid \text{Good}(S^*)] \\ &= \sum_{S_\perp \in \text{Perm}_\perp(n)} \left(\Pr_{S^*}[S^* \downarrow (\emptyset, Q_S \cup Q^{\text{Ext}}(S_\perp), k) \mid \text{Good}(S^*)] \times \right. \\ & \quad \left. \Pr_{S^*}[S^* \downarrow (Q_C, Q_S \cup Q^{\text{Ext}}(S_\perp), k) \mid S^* \downarrow (\emptyset, Q_S \cup Q^{\text{Ext}}(S_\perp), k)] \right). \quad (13) \end{aligned}$$

Fixing an arbitrary $S_\perp \in \text{Perm}_\perp(n)$, parts 4 and 5 of the definition of $\text{Good}(S_\perp)$ imply that the sets

$$\begin{aligned} A &= \left\{ T_1(\tilde{S}_\perp(x \oplus k_0) \oplus k_1)[j] : (x, y) \in Q_C, j \in [w] \right\} \\ B &= \left\{ (T_2^{-1}\tilde{S}_\perp^{-1}(y \oplus k_3) \oplus k_2)[j] : (x, y) \in Q_C, j \in [w] \right\} \end{aligned}$$

each consist of wq_C *distinct* elements, whereas parts 2 and 3 of the same definition imply that

$$\begin{aligned} A \cap (\text{Dom}(\tau) \cup \text{ExtDom}(\tau)) &= \emptyset, \\ B \cap (\text{Range}(\tau) \cup \text{ExtRange}(\tau)) &= \emptyset. \end{aligned}$$

It follows that $S^* \downarrow (Q_C, Q_S \cup Q^{\text{Ext}}(S_\perp), k)$ iff $S^* \downarrow (\emptyset, Q_S \cup Q^{\text{Ext}}(S_\perp), k)$ and $S^*(a) = b$ for all wq_C “matching” pairs (a, b) in $A \times B$ (that is, we match the element $a \in A$ associated with $(x, y) \in Q_C$ and $j \in [w]$ with the element $b \in B$ associated to the same (x, y) and j). Thus,

$$\begin{aligned} & \Pr_{S^*}[S^* \downarrow (Q_C, Q_S \cup Q^{\text{Ext}}(S_\perp), k) \mid S^* \downarrow (\emptyset, Q_S \cup Q^{\text{Ext}}(S_\perp), k)] \\ &= \frac{(2^n - q_S - |Q^{\text{Ext}}(S_\perp)| - wq_C)!}{(2^n - q_S - |Q^{\text{Ext}}(S_\perp)|)!} \\ &\geq \frac{(2^n - q_S - wq_C)!}{(2^n - q_S)!}. \end{aligned}$$

Then since

$$\sum_{S_\perp \in \text{Perm}_\perp(n)} \Pr_{S^*}[S^* \downarrow (\emptyset, Q_S \cup Q^{\text{Ext}}(S_\perp), k) \mid \text{Good}(S^*)] = 1,$$

(13) implies that

$$\Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid \text{Good}(S^*)] \geq \frac{(2^n - q_S - wq_C)!}{(2^n - q_S)!}. \quad (14)$$

Combining (11), (12), and (14), we thus obtain

$$\begin{aligned} \Pr_{S^*}[S^* \downarrow (Q_C, Q_S, k) \mid S^* \downarrow (\emptyset, Q_S, k)] \\ \geq \left(1 - \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w}\right) \frac{(2^n - q_S - wq_C)!}{(2^n - q_S)!}. \end{aligned}$$

By (10) we therefore have

$$\Pr_{S^*}[S^* \downarrow \tau] \geq \frac{(2^n - q_S)!}{2^n!} \left(1 - \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w}\right) \frac{(2^n - q_S - wq_C)!}{(2^n - q_S)!},$$

and so (using (8) and (9))

$$\begin{aligned} \frac{\Pr[X = \tau]}{\Pr[Y = \tau]} &= \frac{\Pr_{S^*}[S^* \downarrow \tau]}{\Pr_{P^*, S^*}[(P^*, S^*) \downarrow \tau]} \\ &\geq \left(1 - \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w}\right) \frac{(2^n - q_S - wq_C)!}{(2^n - q_S)!} \bigg/ \frac{(2^{wn} - q_C)!}{2^{wn}!} \\ &\geq \left(1 - \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w}\right) \left(\frac{1}{2^n - q_S}\right)^{wq_C} \bigg/ \left(\frac{1}{2^{wn} - q_C}\right)^{q_C} \\ &\geq \left(1 - \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w}\right) \left(\frac{1}{2^n}\right)^{wq_C} \bigg/ \left(\frac{1}{2^{wn} - q_C}\right)^{q_C} \\ &= \left(1 - \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w}\right) \left(1 - \frac{q_C}{2^{wn}}\right)^{q_C} \\ &= 1 - \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w} - \frac{q_C^2}{2^{wn}}. \end{aligned}$$

Combining with (5), which gave an upper bound on the probability of obtaining a bad transcript in the ideal world, yields a final upper bound of

$$\begin{aligned} \frac{2wq_Cq_S}{2^n} + \frac{w(w-1)q_C^2}{2^n} + \frac{4w^2q_C^2 + 2wq_Cq_S}{2^n - q_S - 2w} + \frac{q_C^2}{2^{wn}} \\ \leq \frac{5w^2q_C^2 + 4wq_Cq_S}{2^n - q_S - 2w} + \frac{q_C^2}{2^{wn}} \end{aligned}$$

on the distinguisher's advantage, as per (3). This completes the proof. \square

A minimal secure (linear) SPN. We proved that a 3-round, linear SPN is secure if the keys k_0 and k_3 are individually uniform and T_1, T_2^{-1} contain no 0-entries. No assumptions were made about independence of k_0, k_3 , nor were any assumptions made about the distributions of k_1, k_2 . So the theorem implies

security for the following “minimal” 3-round, linear SPN: Let $k_0 = k_3 = k$, where k is uniform, set $k_1 = k_2 = 0^{wn}$, and let $T_1 = T_2^{-1} = T$ be invertible with no 0-entries. Define keyed permutations

$$\pi_i(k, x) = \begin{cases} x \oplus k & i \in \{0, 3\} \\ Tx & i = 1 \\ T^{-1}x & i = 2. \end{cases} \quad (15)$$

We have:

Corollary 1. *Assume $w > 1$. Let \mathcal{C} be a 3-round, linear SPN with round permutations as in (15) and \mathcal{K} choosing uniform $k_0 = k_3$ and $k_1 = k_2 = 0^{wn}$. Then*

$$\text{Adv}_{\mathcal{C}}(q_{\mathcal{C}}, q_{\mathcal{S}}) \leq \frac{5w^2q_{\mathcal{C}}^2 + 4wq_{\mathcal{C}}q_{\mathcal{S}}}{2^n - q_{\mathcal{S}} - 2w} + \frac{q_{\mathcal{C}}^2}{2^{wn}}.$$

4 Non-Linear SPNs

In the previous section we considered linear SPNs and showed that 3 rounds are necessary for security to hold. In this section, we show that by allowing non-linear permutations, the number of rounds (i.e., the number of applications of the S -boxes) needed for constructing a secure SPN can be reduced.

This section is organized as follows. We first define what it means for a keyed permutation over $\{0, 1\}^{wn}$ to be *blockwise universal*.⁷ We then show how to use blockwise-universal permutations to construct a 1-round SPN. Finally, we explore various constructions of blockwise-universal permutations.

Interestingly, for $w = 1$ we show that simple key mixing gives a blockwise-universal permutation; as a corollary of our work, we thus obtain a proof of security for the classical Even-Mansour construction [12], even in the case where the pre- and post-whitening keys are the same [11]. For $w \geq 2$ our results from Section 3.1 imply that no linear function can be blockwise universal, but we show that several non-linear constructions are possible.

4.1 Secure 1-Round SPNs via Blockwise-Universal Permutations

We begin by defining the notion of a blockwise-universal (keyed) permutation over \mathbb{F}^w . Let the *blocks* of $y \in \mathbb{F}^w$ be $y[1], \dots, y[w] \in \mathbb{F}$. Informally, a keyed permutation $\pi : K \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ is blockwise universal if, for any distinct $x, x' \in \mathbb{F}^w$ and any $c \in \mathbb{F}$, the probability (taken over uniform $k \in K$) of each of the following events is low: (1) a block of $\pi(k, x)$ is equal to a block of $\pi(k, x')$, (2) two different blocks of $\pi(k, x)$ are equal, (3) a block of $\pi(k, x)$ is equal to c . Formally:

Definition 3. *A keyed permutation $\{\pi : K \times \mathbb{F}^w \rightarrow \mathbb{F}^w\}$ is (ϵ, ϵ') -blockwise universal if the following hold:*

⁷ A similar notion was defined in [24, 15, 14] and even called blockwise universal in [15, 14]. The definition we give here is related, but different.

1. For all distinct $(x, i), (x', i') \in \mathbb{F}^w \times [w]$, we have

$$\Pr_{k \leftarrow K} [\pi(k, x)[i] = \pi(k, x')[i']] \leq \epsilon.$$

2. For all $(x, i, c) \in \mathbb{F}^w \times [w] \times \mathbb{F}$, we have $\Pr_{k \leftarrow K} [\pi(k, x)[i] = c] \leq \epsilon'$.

If $\epsilon = \epsilon'$, we simply call the keyed permutation ϵ -blockwise universal.

We now show that if π is blockwise universal, then a 1-round SPN construction \mathcal{C} using round permutations $\pi_0 = \pi$ and $\pi_1 = \pi^{-1}$ is secure. In fact, \mathcal{C} is secure even when π_0, π_1 share the same (uniform) key. I.e., we may define \mathcal{C} as

$$\mathcal{C}_k^S(x) \stackrel{\text{def}}{=} \pi^{-1}(k, \tilde{S}(\pi(k, x))).$$

Theorem 2. *Let $\pi : K \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ be (ϵ, ϵ') -blockwise universal. Then*

$$\text{Adv}_{\mathcal{C}}(q_C, q_S) \leq w^2 q_C^2 \epsilon + 2w q_C q_S \epsilon',$$

where \mathcal{C} is the 1-round SPN construction in which $\pi_0 = \pi$, $\pi_1 = \pi^{-1}$, and in which \mathcal{K} samples a uniform $k \in K$ and sets $k_0 = k_1 = k$.

Proof. The proof is conceptually similar to the proof of Theorem 1, though the technical details are simpler here. Fix a deterministic distinguisher D . Without loss of generality, assume D makes exactly q_C (non-redundant) forward/inverse queries to its left oracle that is either \mathcal{C}_k or P , and exactly q_S (non-redundant) forward/inverse queries to its right oracle that is the S -box. We call a query from D to its left oracle a *construction query* (even though in the ideal world the oracle is P), and a query from D to its right oracle an *S-box query*.

As previously, the interaction between D and its oracles is recorded in two sets of pairs $Q_C \subseteq \{0, 1\}^{wn} \times \{0, 1\}^{wn}$ and $Q_S \subseteq \{0, 1\}^n \times \{0, 1\}^n$, where Q_C contains every pair (x, y) for which D made a construction query x that was answered by y or an inverse query y that was answered by x , and Q_S is defined similarly with respect to S -box queries. As in the proof of Theorem 1, we also append the key value k to the transcript in the real world and append a (uniform) dummy key value $k \in K$ to the transcript in the ideal world; a transcript τ thus has the form of a triple $\tau = (Q_C, Q_S, k)$.

Let \mathcal{T} be the set of all possible transcripts that can be generated by D in the ideal world. We say that a transcript $\tau = (Q_C, Q_S, k)$ is *bad* if either:

1. There exist a pair $(x, y) \in Q_C$, a pair $(a, b) \in Q_S$, and an index $j \in [w]$ such that $\pi(k, x)[j] = a$ or $\pi(k, y)[j] = b$.
2. There exist distinct tuples $(x, y, j), (x', y', j') \in Q_C \times [w]$ such that $\pi(k, x)[j] = \pi(k, x')[j']$ or $\pi(k, y)[j] = \pi(k, y')[j']$.

We let $\mathcal{T}_2 \subseteq \mathcal{T}$ denote the set of bad transcripts. Transcripts in $\mathcal{T}_1 = \mathcal{T} \setminus \mathcal{T}_2$ are called *good* transcripts.

Let X, Y be the distributions over transcripts in the real and ideal worlds, respectively. Because the key value k is independent of Q_C, Q_S in the ideal

world, the definition of (ϵ, ϵ') -blockwise universality and two applications of a union bound give

$$\Pr[Y \in \mathcal{T}_2] \leq 2wq_Cq_S\epsilon' + w^2q_C^2\epsilon.$$

We next lower bound the ratio

$$\frac{\Pr[X = \tau]}{\Pr[Y = \tau]}$$

for transcripts $\tau \in \mathcal{T}_1$. Let Ω_X, Ω_Y be the probability spaces underlying the real and ideal worlds respectively. That is,

$$\begin{aligned}\Omega_X &= \{(S, k) : S \in \text{Perm}(n), k \in K\} \\ \Omega_Y &= \{(P, S, k) : P \in \text{Perm}(wn), S \in \text{Perm}(n), k \in K\},\end{aligned}$$

each with uniform measure.

For the rest of the proof, fix a transcript $\tau = (Q_C, Q_S, k) \in \mathcal{T}_1$. We say an element $\omega = (S^*, k^*) \in \Omega_X$ is *compatible with* τ if $k^* = k$, if $S^*(a) = b$ for all $(a, b) \in Q_S$, and if $\mathcal{C}_k^{S^*}(x) = y$ for all $(x, y) \in Q_C$. Analogously, an element $\omega = (P^*, S^*, k^*) \in \Omega_Y$ is *compatible with* τ if $k^* = k$, if $S^*(a) = b$ for all $(a, b) \in Q_S$, and if $P^*(x) = y$ for all $(x, y) \in Q_C$. We write $\omega \downarrow \tau$ to denote compatibility between $\omega \in \Omega_X \cup \Omega_Y$ and τ .

Since

$$\begin{aligned}\Pr[X = \tau] &= |\{\omega \in \Omega_X : \omega \downarrow \tau\}| / |\Omega_X| \\ \Pr[Y = \tau] &= |\{\omega \in \Omega_Y : \omega \downarrow \tau\}| / |\Omega_Y|\end{aligned}$$

(compare with (6), (7)), we have

$$\begin{aligned}\frac{\Pr[X = \tau]}{\Pr[Y = \tau]} &= \frac{|\{\omega \in \Omega_X : \omega \downarrow \tau\}|}{|\Omega_X|} \cdot \frac{|\Omega_Y|}{|\{\omega \in \Omega_Y : \omega \downarrow \tau\}|} \\ &= \frac{(2^n - q_S - wq_C)!}{2^n! |K|} \cdot \frac{2^{wn}! 2^n! |K|}{(2^{wn} - q_C)! (2^n - q_S)!} \\ &= \frac{(2^n - q_S - wq_C)! 2^{wn}!}{(2^n - q_S)! (2^{wn} - q_C)!} \geq 1,\end{aligned}$$

where the fact that $\tau \in \mathcal{T}_1$ is used in the second equality. Hence we may apply the H-coefficient technique with $\epsilon_1 = 0$ (cf. Section 2.2), and D 's distinguishing advantage is upper bounded by

$$\epsilon_1 + \Pr[Y \in \mathcal{T}_2] \leq 2wq_Cq_S\epsilon' + w^2q_C^2\epsilon$$

as claimed. □

4.2 Constructing Blockwise-Universal Permutations

We now show several constructions of blockwise-universal permutations.

Key mixing ($w = 1$). Let $w = 1$ and $k \in \{0, 1\}^n$. Define $\pi(k, x) = x \oplus k$. It is trivial to see that this construction is $(0, 2^{-n})$ -blockwise universal: if $x \neq x'$, then $x \oplus k \neq x' \oplus k$ (meaning $\epsilon = 0$); also, for any c we have $x \oplus k = c$ with probability $\epsilon' = 2^{-n}$ when k is uniform.

Instantiating the construction analyzed in Theorem 2 with this permutation yields the Even-Mansour construction [12] with the same key used for both pre- and post-whitening. Our results thus imply that the Even-Mansour construction in this case has a concrete security bound of $2q_C q_S / 2^n$, matching the security bound given by Dunkelman, Keller, and Shamir [11].

A construction of degree 3. A consequence of our attack in Section 3.1 is that blockwise-universal permutations with $w > 1$ must be non-linear. We now show a construction of degree 3. This construction is inspired by (though distinct from and considerably simpler than) a construction of a *non-keyed* permutation given by Dodis et al. [10] that achieves (in their terminology) good “entry-wise random collision resistance.”

Let $w \geq 2$ and let $T \in \mathbb{F}^{w \times w}$ be an invertible matrix of the form

$$T = \begin{bmatrix} 1 & & & \\ 1 & & & \\ \vdots & & * & \\ 1 & & & \end{bmatrix},$$

i.e., the first column of T is all 1s. We define a polynomial $p : \mathbb{F}^w \rightarrow \mathbb{F}$ by

$$p(x) = \bigoplus_{j=2}^w x[j]^3$$

and then define a transformation $\eta : \mathbb{F}^w \rightarrow \mathbb{F}^w$ by

$$\eta(x)[i] = \begin{cases} x[i] \oplus p(x) & \text{if } i = 1, \\ x[i] & \text{otherwise.} \end{cases}$$

It is easy to see that η is a permutation of \mathbb{F}^w . (In fact, since \mathbb{F} has characteristic 2, the permutation η is an *involution*, i.e., it is its own inverse.) Finally, define the keyed permutation $\pi : \mathbb{F}^w \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ as

$$\pi(k, x) = T \cdot \eta(x \oplus k). \tag{16}$$

Note that π is the composition of three invertible transformations, where the first transformation consists of the map $x \rightarrow x \oplus k$; hence, π is a keyed permutation.

Theorem 3. *The keyed permutation $\pi : \mathbb{F}^w \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ defined in (16) is $(2/2^n, 1/2^n)$ -blockwise universal.*

Proof. We start by noting that

$$\forall i : \pi(k, x)[i] = (Tx)[i] \oplus (Tk)[i] \oplus p(x \oplus k), \tag{17}$$

by the structure of T . The term $(Tk)[i]$ is a linear combination of the variables $k[1], \dots, k[w]$ in which $k[1]$ has coefficient 1, whereas

$$p(x \oplus k) = (x[2] \oplus k[2])^3 \oplus \dots \oplus (x[w] \oplus k[w])^3$$

can be viewed as the sum of $w - 1$ degree-3 polynomials in the variables $k[2], \dots, k[w]$ whose coefficients depend on x . Since $(Tk)[i]$ is the only term in (17) that depends on $k[1]$, it is easy to see that the second condition in the definition of blockwise universality is satisfied with $\epsilon' = 1/2^n$.

To verify the first condition of Definition 3, let $(x, i), (x', i') \in \mathbb{F}^w \times [w]$ be distinct. Then

$$\begin{aligned} & \pi(k, x)[i] \oplus \pi(k, x')[i'] \\ &= (Tx)[i] \oplus (Tx')[i] \oplus (Tk)[i] \oplus (Tk)[i'] \oplus p(x \oplus k) \oplus p(x' \oplus k). \end{aligned}$$

If the last $w - 1$ entries of x, x' are equal, then $p(x \oplus k) = p(x' \oplus k)$ and moreover $(Tx)[i] \oplus (Tx')[i] = x[1] \oplus x'[1]$; thus,

$$\pi(k, x)[i] \oplus \pi(k, x')[i'] = x[1] \oplus x'[1] \oplus (Tk)[i] \oplus (Tk)[i'].$$

If $i = i'$ then $x[1] \oplus x'[1] \neq 0$ (otherwise (x, i) would be equal to (x', i')), so $\pi(k, x)[i] \neq \pi(k, x')[i']$. If $i \neq i'$ then $(Tk)[i] \oplus (Tk)[i']$ is uniform (by linear independence of the rows of T), so $\pi(k, x)[i] = \pi(k, x')[i']$ with probability $1/2^n$. In any case,

$$\Pr_k[\pi(k, x)[i] = \pi(k, x')[i']] \leq 1/2^n.$$

On the other hand, if the last $w - 1$ entries of x, x' are not all equal then there exists a $j \in \{2, \dots, w\}$ such that $x[j] \neq x'[j]$. Then

$$(x[j] \oplus k[j])^3 \oplus (x'[j] \oplus k[j])^3$$

is a (nonzero) polynomial of degree 2 in $k[j]$. By extension, $p(x, k) \oplus p(x', k)$ and hence $\pi(k, x)[i] \oplus \pi(k, x')[i']$ are nonzero polynomials of degree 2 in $k[j]$ as well. Fixing arbitrary values of $k[j']$ for $j' \neq j$, the probability that this polynomial evaluates to zero over uniform choice of $k[j]$ is thus at most $2/2^n$; hence

$$\Pr_k[\pi(k, x)[i] = \pi(k, x')[i']] \leq 2/2^n$$

in this case. This concludes the proof. \square

A construction with short keys. Let $T \in \mathbb{F}^{w \times w}$ be an invertible matrix, with entries $T_{i,j}$, such that (i) $T_{i,j} \neq 0$ for all $i, j \in [w]$, (ii) $\bigoplus_{j=1}^w T_{i,j} \neq 0$ for all $i \in [w]$, and (iii) $\bigoplus_{j=1}^w T_{i,j} \neq \bigoplus_{j=1}^w T_{i',j}$ if $i \neq i'$. (A random matrix has all the required properties with high probability.) Then we define the keyed permutation $\pi : \mathbb{F} \setminus \{0\} \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ by $\pi(k, x) = Tz(k, x)$, where

$$z(k, x)[i] = x[i] \cdot k^{i+1} \oplus k$$

for $i = 1, \dots, w$. It is easy to verify that π is invertible when k is nonzero.

This construction can be viewed as applying a “local” keyed, non-linear transformation to each block $x[i]$, and then applying a linear transformation to the result. Here we use a much shorter key k as compared to the previous construction, but at the expense of the non-linear transformation having degree $w + 1$.

Theorem 4. *The keyed permutation $\pi : \mathbb{F} \setminus \{0\} \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ defined above is $((w + 1)/(2^n - 1))$ -blockwise universal.*

Proof. We first verify property 1 of Definition 3. Let $(x, i), (x', i') \in \mathbb{F}^w \times [w]$ be distinct. By definition of π , we have $\pi(k, x)[i] = \pi(k, x')[i']$ if and only if

$$\bigoplus_{j=1}^w T_{i,j}(x[j] \cdot k^{j+1} \oplus k) = \bigoplus_{j=1}^w T_{i',j}(x'[j] \cdot k^{j+1} \oplus k).$$

Rewriting the equation, this is the same as

$$\left(\bigoplus_{j=1}^w (T_{i,j} \oplus T_{i',j}) \right) k \oplus \bigoplus_{j=1}^w (T_{i,j} x[j] \oplus T_{i',j} x'[j]) k^{j+1} = 0. \quad (18)$$

If $i \neq i'$ then, since $\sum_{j=1}^w T_{i,j} \neq \sum_{j=1}^w T_{i',j}$, (18) is a polynomial equation in k of degree at least 1 and at most $w + 1$. If $i = i'$ then $x \neq x'$ and so there exists $i_0 \in [w]$ such that $x[i_0] \neq x'[i_0]$. Again, this means (18) is a polynomial equation in k of degree at least $i_0 + 1$ and at most $w + 1$. In either case, the probability over uniform choice of k that the equation holds is at most $(w + 1)/(2^n - 1)$.

To see property 2, observe that $\pi(k, x)[i] = c$ for some $c \in \mathbb{F}$ if and only if $\bigoplus_{j=1}^w T_{i,j}(x[j] \cdot k^{j+1} \oplus k) = c$. This is a polynomial equation in k of degree at least 1 (since $\bigoplus_{j=1}^w a_{i,j} \neq 0$) and at most $w + 1$. So the probability this equation holds for uniform k is at most $(w + 1)/(2^n - 1)$. This concludes the proof. \square

A second construction with short keys. We give another instantiation with n -bit keys that achieves the same parameters as above, but is (arguably) more direct and intuitive. Let $k \in \mathbb{F} \setminus \{0\}$. Let $C_1, \dots, C_w \in \mathbb{F}$ be any w distinct nonzero elements. Then, we define

$$\pi(k, x)[i] := \bigoplus_{j=1}^w (k \cdot C_i)^{j+1} x[j] \oplus k \cdot C_i, \quad (19)$$

for $i = 1, \dots, w$. It is easy to verify that π is invertible when k is nonzero.

Theorem 5. *The keyed permutation $\pi : \mathbb{F} \setminus \{0\} \times \mathbb{F}^w \rightarrow \mathbb{F}^w$ as in (19) is $((w + 1)/(2^n - 1))$ -blockwise universal.*

Proof. The proof is quite similar to that of Theorem 4. We first show that π satisfies property 1 of Definition 3. By definition of π , we have $\pi(k, x)[i] = \pi(k, x')[i']$ if and only if

$$\bigoplus_{j=1}^w (k \cdot C_i)^{j+1} x[j] \oplus k \cdot C_i = \bigoplus_{j=1}^w (k \cdot C_{i'})^{j+1} x'[j] \oplus k \cdot C_{i'}.$$

This is equivalent to

$$(C_i - C_{i'})k \oplus \bigoplus_{j=1}^w (C_i^{j+1}x[j] \oplus C_{i'}^{j+1}x'[j])k^{j+1} = 0. \quad (20)$$

Fix distinct $(x, i) \neq (x', i') \in \mathbb{F}^w \times [w]$. If $i \neq i'$ then $C_i \neq C_{i'}$ and so (20) is a polynomial equation in k of degree at least 1 and at most $w + 1$. If $i = i'$ then $x \neq x'$, and so there exists $i_0 \in [w]$ such that $x[i_0] \neq x'[i_0]$. Again, this implies that (20) is a polynomial equation in k of degree at least $t + 1$ and at most $w + 1$. In either case, the probability over uniform choice of k that the equation holds is at most $(w + 1)/(2^n - 1)$.

To see property 2, observe that $\pi(k, x)[i] = c$ for some $c \in \mathbb{F}$ if and only if $\bigoplus_{j=1}^w (k \cdot C_i)^{j+1}x[j] \oplus k \cdot C_i = c$. This is a polynomial equation in k of degree at least 1 (since C_i is nonzero by assumption) and at most $w + 1$. The probability with which this equation holds for uniform k is at most $(w + 1)/(2^n - 1)$. This concludes the proof. \square

Relation to our 3-round, linear SPN construction. We conclude with the following informal observation relating the result of Theorem 2 to our 3-round, linear SPN construction from Section 3.2: The initial round of the “minimal” linear SPN discussed there (i.e., key mixing, followed by evaluation of \tilde{S} , and then finally a linear transformation) can be shown to be a blockwise-universal permutation if the S -box is viewed as part of the key of the permutation. To see this, consider any $(x, i) \neq (x', i')$. If $x = x'$ but $i \neq i'$, then key mixing with a uniform wn -bit key ensures that the output is uniform, so two different blocks collide with probability $1/2^n$. On the other hand, if $x \neq x'$ then $x[j] \neq x'[j]$ for some j . After the key mixing, the S -boxes will be applied to two unequal values $x[j] \oplus k[j]$ and $x'[j] \oplus k[j]$, which means the resulting values $y[j]$ and $y'[j]$ will be uniform and (essentially) independent. Subsequent application of the linear transformation T ensures that any blocks i and i' of the outputs will also be uniform and uncorrelated, hence unlikely to collide.

Thus, the 3-round, linear SPN construction can be viewed almost as a “special case” of our 1-round, non-linear SPN, in which the blockwise-universal permutations are implemented via a linear SPN round. We stress that this is only intuition, and formally we cannot derive Theorem 1 as a corollary of Theorem 2 because (i) the same S -boxes are shared in the permutations and the middle layer, and (ii) the S -boxes are *public*, which is not taken into account in the definition of blockwise universality.

5 Conclusion and Open Problems

We study the security of SPNs as strong pseudorandom permutations when the S -box is modeled as a public random permutation. This model captures the design approach of most block ciphers following the SPN paradigm. Within this model, we give an exact characterization of the properties required to achieve security in both the linear and non-linear settings.

A number of interesting open questions remain. For instance, while generic information-theoretic attacks show that constructions with at most 1 round cannot surpass birthday security (presuming a key of $O(wn)$ bits) we are not aware of matching birthday attacks at 3 rounds. Hence the question of determining the exact security of linear 3-round SPNs (and in particular, whether the security goes beyond birthday or not) remains open. Moreover, proving beyond-birthday security at *any* number of rounds remains open as well.

Another, more technical question concerns SPNs with a limited number of nonlinear rounds. Specifically, if we limit consideration to SPNs using exactly one nonlinear keyed permutation, then we do not know if 2 rounds suffice for security. (Note that a 1-round network with this structure is easily attacked. On the other hand, 3 rounds suffice by the results of this paper.)

Acknowledgments

Work of the second and fourth authors was performed under financial assistance award 70NANB15H328 from the U.S. Department of Commerce, National Institute of Standards and Technology.

References

1. Alex Biryukov, Charles Bouillaguet, and Dmitry Khovratovich. Cryptographic schemes based on the ASASA structure: Black-box, white-box, and public-key (extended abstract). In *Advances in Cryptology—Asiacrypt 2014, Part I*, volume 8873 of *LNCS*, pages 63–84. Springer, 2014.
2. Alex Biryukov and Dmitry Khovratovich. Decomposition attack on SASASASAS. Available at <http://eprint.iacr.org/2015/646>.
3. Alex Biryukov and Adi Shamir. Structural cryptanalysis of SASAS. *Journal of Cryptology*, 23(4):505–518, 2010.
4. D. Bleichenbacher and A. Desai. A construction of a super-pseudorandom cipher, February 1999. Unpublished manuscript.
5. Debrup Chakraborty and Palash Sarkar. A new mode of encryption providing a tweakable strong pseudo-random permutation. In *Fast Software Encryption—FSE 2006*, volume 4047 of *LNCS*, pages 293–309. Springer, 2006.
6. Shan Chen and John P. Steinberger. Tight security bounds for key-alternating ciphers. In *Advances in Cryptology—Eurocrypt 2014*, volume 8441 of *LNCS*, pages 327–350. Springer, 2014.
7. Jean-Sébastien Coron, Yevgeniy Dodis, Avradip Mandal, and Yannick Seurin. A domain extender for the ideal cipher. In *7th Theory of Cryptography Conference—TCC 2010*, volume 5978 of *LNCS*, pages 273–289. Springer, 2010.
8. Joan Daemen. *Cipher and Hash Function Design Strategies Based on Linear and Differential Cryptanalysis*. PhD thesis, Katholieke Universiteit Leuven, 1995.
9. Itai Dinur, Orr Dunkelman, Thorsten Kranz, and Gregor Leander. Decomposing the ASASA block cipher construction. Available at <http://eprint.iacr.org/2015/507>.
10. Yevgeniy Dodis, Martijn Stam, John P. Steinberger, and Tianren Liu. Indifferentiability of confusion-diffusion networks. In *Advances in Cryptology—Eurocrypt 2016, Part II*, volume 9666 of *LNCS*, pages 679–704. Springer, 2016.

11. Orr Dunkelman, Nathan Keller, and Adi Shamir. Minimalism in cryptography: The Even-Mansour scheme revisited. In *Advances in Cryptology—Eurocrypt 2012*, volume 7237 of *LNCS*, pages 336–354. Springer, 2012.
12. Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. In *Advances in Cryptology—Asiacrypt’91*, volume 739 of *LNCS*, pages 210–224. Springer, 1991.
13. H. Feistel. Cryptography and computer privacy. *Scientific American*, 228(5):15–23, 1973.
14. Shai Halevi. Invertible universal hashing and the TET encryption mode. In *Advances in Cryptology—Crypto 2007*, volume 4622 of *LNCS*, pages 412–429. Springer, 2007.
15. Shai Halevi and Phillip Rogaway. A tweakable enciphering mode. In *Advances in Cryptology—Crypto 2003*, volume 2729 of *LNCS*, pages 482–499. Springer, 2003.
16. Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In *Cryptographers’ Track—RSA 2004*, volume 2964 of *LNCS*, pages 292–304. Springer, 2004.
17. Tetsu Iwata and Kaoru Kurosawa. On the pseudorandomness of the AES finalists—RC6 and Serpent. In *Fast Software Encryption—FSE 2000*, volume 1978 of *LNCS*, pages 231–243. Springer, 2000.
18. Antoine Joux. Cryptanalysis of the EMD mode of operation. In *Advances in Cryptology—Eurocrypt 2003*, volume 2656 of *LNCS*, pages 1–16. Springer, 2003.
19. J. Katz and Y. Lindell. *Introduction to Modern Cryptography, 2nd edition*. Chapman & Hall/CRC Press, 2015.
20. Michael Luby and Charles Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17(2):373–386, 1988.
21. Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In *1st Theory of Cryptography Conference—TCC 2004*, volume 2951 of *LNCS*, pages 21–39. Springer, 2004.
22. David A. McGrew and Scott R. Fluhrer. The security of the extended codebook (XCB) mode of operation. In *14th Annual Intl. Workshop on Selected Areas in Cryptography (SAC)*, volume 4876 of *LNCS*, pages 311–327. Springer, 2007.
23. Eric Miles and Emanuele Viola. Substitution-permutation networks, pseudorandom functions, and natural proofs. *J. ACM*, 62(6):46, 2015.
24. Moni Naor and Omer Reingold. On the construction of pseudorandom permutations: Luby-Rackoff revisited. *Journal of Cryptology*, 12(1):29–66, 1999.
25. Jacques Patarin. Pseudorandom permutations based on the D.E.S. scheme. In *1st European Symposium on Research in Computer Security (ESORICS)*, LNCS, pages 185–187, 1990.
26. Jacques Patarin. *Etude de Générateurs de Permutations Basés sur les Schémas du DES*. PhD thesis, INRIA, 1991.
27. Jacques Patarin. Luby-Rackoff: 7 rounds are enough for $2^{n(1-\epsilon)}$ security. In *Advances in Cryptology—Crypto 2003*, volume 2729 of *LNCS*, pages 513–529. Springer, 2003.
28. Jacques Patarin. The “coefficients-H” technique (invited talk). In *SAC 2008: 15th Annual Intl. Workshop on Selected Areas in Cryptography (SAC)*, LNCS, pages 328–345. Springer, 2009.
29. Claude E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal*, 28(4):656–715, 1949.