Modeling Linear Characteristics of Substitution-Permutation Networks

Liam Keliher[1], Henk Meijer[1], and Stafford Tavares[2]

[1] Department of Computing and Information Science
Queen's University, Kingston, Ontario, Canada
{keliher,henk}@cs.queensu.ca
[2] Department of Electrical and Computer Engineering
Queen's University, Kingston, Ontario, Canada
stafford@eleceng.ee.queensu.ca

Abstract. In this paper we present a model for the bias values associated with linear characteristics of substitution-permutation networks (SPN's). The first iteration of the model is based on our observation that for sufficiently large s-boxes, the best linear characteristic usually involves one active s-box per round. We obtain a result which allows us to compute an upper bound on the probability that linear cryptanalysis using such a characteristic is feasible, as a function of the number of rounds. We then generalize this result, upper bounding the probability that linear cryptanalysis is feasible when any linear characteristic may be used (no restriction on the number of active s-boxes). The work of this paper indicates that the basic SPN structure provides good security against linear cryptanalysis based on linear characteristics after a reasonably small number of rounds.

1 Introduction

A substitution-permutation network (SPN) is a basic cryptosystem architecture which implements Shannon's principles of "confusion" and "diffusion" [15], and which was first proposed by Feistel [4]. An SPN is in some sense the simplest implementation of Shannon's principles. Its basic structural elements of substitution and linear transformation are the foundation of many modern block ciphers, as can be seen from the current AES candidates (for example, Serpent uses a straight SPN structure [1]). Viewing the basic SPN architecture as a "canonical" cryptosystem has provided a useful model for study, yielding a range of analytical and experimental results [6,7,17].

In this paper we consider the linear cryptanalysis of SPN's, developing a model which allows us to bound the probability that a linear attack based on linear characteristics will succeed. The result is of interest because, in practice, linear cryptanalysis often relies on carefully chosen linear characteristics. It should be noted, however, that to achieve "provable security" against linear cryptanalysis, resistance to linear hulls, the counterpart of differentials in differential cryptanalysis, must be demonstrated (see Nyberg [13]).

Howard Heys and Carlisle Adams (Eds.): SAC'99, LNCS 1758, pp. 78–91, 2000.

2 Substitution-Permutation Networks

A substitution-permutation network processes an N-bit plaintext through a series of R rounds, each round consisting of a *substitution stage* followed by a *permutation stage*. In the substitution stage, the current block is viewed as M n-bit subblocks, each of which is fed into a bijective $n \times n$ substitution box (s-box), i.e., a bijective function mapping $\{0,1\}^n \to \{0,1\}^n$. This is followed by a permutation stage, originally a bit-wise permutation, but more generally an invertible linear transformation [5,7]. The permutation stage is usually omitted from the last round. An example of an SPN with $N = 16$, $M = n = 4$, and $R = 3$ is shown in Figure 1. Incorporation of key bits typically involves the derivation

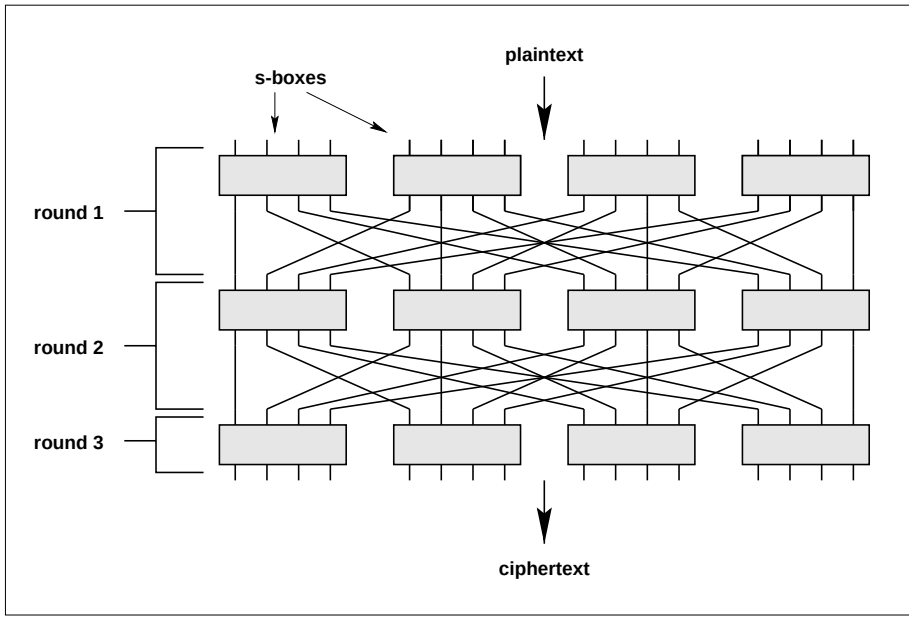

Fig. 1. Example SPN with $N = 16$, $M = n = 4$, $R = 3$

of $(R+1)$ N-bit *subkeys*, denoted $\mathbf{K}^1, \mathbf{K}^2, \ldots, \mathbf{K}^R, \mathbf{K}^{R+1}$, from the original key, $\mathbf{K}$, via a *key scheduling algorithm.* Subkey $\mathbf{K}^r$ is XOR'd with the current block before round r, and subkey $\mathbf{K}^{R+1}$ is XOR'd with the output of the last round to form the ciphertext. For the purpose of what follows, we will assume that $\mathbf{K}$ is an *independent key* [2], a concatenation of $(R+1)$ N-bit subkeys which are not necessarily derivable from some master key via a key-scheduling algorithm (therefore $\mathbf{K} \in \{0,1\}^{N(R+1)}$).

Decryption is accomplished by running the SPN "backwards," reversing the order of the rounds, and in each round performing the inverse linear transformation followed by application of the inverse s-boxes (subkey $\mathbf{K}^{R+1}$ is first XOR'd

with the ciphertext, and each subkey $\mathbf{K}^r$ is XOR'd with the current block *after* decryption round r).

For the purpose of this paper, we adopt an SPN structure with $M = n$ s-boxes of size $n \times n$ ($n \geq 2$) in each round (therefore $N = n^2$), and an inter-round permutation $\pi : \{0,1\}^N \rightarrow \{0,1\}^N$ which connects output bit j of s-box i in round r to input bit i of s-box j in round $r+1$ [8], as in Figure 1. (We use the convention that all numbering proceeds from left to right, beginning at 1.)

In our model, each s-box in the SPN is chosen uniformly and independently from the set of all bijective $n \times n$ s-boxes. In addition, we make the assumption that the input to each encryption round is uniformly and independently distributed over $\{0,1\}^N$. This allows the use of Matsui's Piling-up Lemma [9] in Sections 4 and 5. This assumption does in fact hold if we observe the inputs to the various rounds while varying over all plaintexts *and all keys* $\mathbf{K} \in \{0,1\}^{N(R+1)}$. However, in practice, $\mathbf{K}$ is fixed and only the plaintexts vary. Nyberg [13] provides a rigorous analysis of this issue.

3 Nonlinearity Measures

The linear approximation table (LAT) [9] of an s-box $S : \{0,1\}^n \rightarrow \{0,1\}^n$ is defined as follows: for $\alpha, \beta \in \{0,1\}^n$,

$$\mathrm{LAT}[\alpha,\beta] = \#\left\{\mathbf{X} \in \{0,1\}^n : \alpha \bullet \mathbf{X} = \beta \bullet S(\mathbf{X})\right\} - 2^{n-1} \ ,$$

where $\bullet$ is the inner product summed over $GF(2)$. It follows that $\mathrm{LAT}[0,0] = 2^{n-1}$, and if S is bijective, as is the case in an SPN, then $\mathrm{LAT}[\alpha,\beta] = 0$ if exactly one of α, β is 0. These entries are of no cryptographic significance; in the discussion below we consider only $\mathrm{LAT}[\alpha,\beta]$ for $\alpha, \beta \neq 0$.

If $\mathrm{LAT}[\alpha,\beta] = 0$, then the function $f_\beta(\mathbf{X}) = \beta \bullet S(\mathbf{X})$ is at equal Hamming distance (2^{n-1}) from the affine functions $g_\alpha(\mathbf{X}) = \alpha \bullet \mathbf{X}$ and $g'_\alpha(\mathbf{X}) = (\alpha \bullet \mathbf{X}) \oplus 1$ (here we view functions mapping $\{0,1\}^n \rightarrow \{0,1\}$ as 2^n-bit vectors for the purpose of measuring Hamming distance). A positive value of $\mathrm{LAT}[\alpha,\beta]$ indicates that f_β is closer to g_α, and a negative value indicates that f_β is closer to g'_α. In fact f_β can be approximated by g_α with probability

$$p_{\alpha,\beta} = \frac{\#\left\{\mathbf{X} \in \{0,1\}^n : g_\alpha(\mathbf{X}) = f_\beta(\mathbf{X})\right\}}{2^n} = \frac{\mathrm{LAT}[\alpha,\beta] + 2^{n-1}}{2^n} \ , \tag{1}$$

and by g'_α with probability $(1 - p_{\alpha,\beta})$, computed over the uniform distribution of $\mathbf{X} \in \{0,1\}^n$. It is also useful to define the *bias* associated with $\mathrm{LAT}[\alpha,\beta]$:

$$b_{\alpha,\beta} = p_{\alpha,\beta} - \frac{1}{2} = \frac{\mathrm{LAT}[\alpha,\beta]}{2^n} \ . \tag{2}$$

Obviously $b_{\alpha,\beta} \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. A value of $b_{\alpha,\beta}$ which is (relatively) large in absolute value indicates a (relatively) high probability of success in approximating f_β by an affine function. It is such approximations that are exploited by linear cryptanalysis (Section 4). (Conversely, a bias value of 0 yields no information to

the cryptanalyst.) One measure of the resistance of an s-box S to approximation by affine functions is the *nonlinearity* of S, $\mathrm{NL}(S)$:

$$\mathrm{NL}(S) = 2^{n-1} - \max\left\{|\mathrm{LAT}[\alpha,\beta]| : \alpha,\beta \in \{0,1\}^n,\ \alpha,\beta \neq 0\right\}.$$

Another useful value is the minimum nonlinearity over the s-boxes of the SPN, $\mathrm{NL}_{\min}$:

$$\mathrm{NL}_{\min} = \min\left\{\mathrm{NL}(S) : S \in \mathrm{SPN}\right\}.$$

4 Linear Cryptanalysis of SPN's

Linear cryptanalysis is a known-plaintext attack (ciphertext-only under certain conditions) which was introduced by Matsui in 1993 [9]. Matsui demonstrated that linear cryptanalysis could break DES using 2^{43} known plaintexts [11]. Here we present linear cryptanalysis in the context of SPN's where (absent the complexities of DES) the basic concepts are more easily stated. Linear cryptanalysis of SPN's has been considered to some extent by, among others, Heys and Tavares [7] and Youssef [17].

The basic linear attack attempts to extract the equivalent of one key bit, expressed as the XOR sum of a subset of key bits, using a linear equation which relates subsets of the plaintext ($\mathbf{P}$), ciphertext($\mathbf{C}$) and key ($\mathbf{K}$) bits:

$$\mathbf{P}_{i_1} \oplus \mathbf{P}_{i_2} \oplus \cdots \oplus \mathbf{P}_{i_a} \oplus \mathbf{C}_{j_1} \oplus \mathbf{C}_{j_2} \oplus \cdots \oplus \mathbf{C}_{j_b} = \mathbf{K}_{k_1} \oplus \mathbf{K}_{k_2} \oplus \cdots \oplus \mathbf{K}_{k_c} \quad (3)$$

(here $\mathbf{P}_{i_1}$, for example, denotes the i_1^{th} bit of $\mathbf{P}$, numbering from left to right). Such an equation holds with some probability p (and associated bias $b = p - \frac{1}{2}$), computed over the uniform distribution of plaintexts. Matsui's Algorithm 1 [9] extracts the key bit represented by the right-hand side of (3) (with success rate 97.7%) by encrypting $\mathcal{N}_L$ random plaintexts, where

$$\mathcal{N}_L = \frac{1}{b^2} \quad (4)$$

(increasing (reducing) the number of random plaintexts encrypted increases (reduces) the probability that the key bit will be determined correctly).

One-Round Linear Characteristics

A system linear approximation such as (3) can be constructed from one-round linear approximations, also known as *linear characteristics* [2]. Specifically, a one-round characteristic for round r is a tuple

$$\Omega_r = \langle \Gamma_{\mathrm{P}}^r,\ \Gamma_{\mathrm{C}}^r,\ \Gamma_{\mathrm{K}}^r,\ b_r \rangle, \quad (5)$$

where $\Gamma_{\mathrm{P}}^r, \Gamma_{\mathrm{C}}^r \in \{0,1\}^N$ and $\Gamma_{\mathrm{K}}^r \in \{0,1\}^{N(R+1)}$; Γ_{K}^r contains Γ_{P}^r in its r^{th} N-bit subblock, and is zero elsewhere; and bias $b_r \in \left[-\frac{1}{2}, \frac{1}{2}\right]$. Let $S^r(\cdot)$ denote application of the round r s-boxes, which are indexed left to right as $S_1^r, S_2^r, \ldots, S_n^r$.

We can view Γ_{P}^r (Γ_{C}^r) as an input (output) mask for round r, and specifically as the concatenation of n n-bit input (output) masks for the S_i^r, denoted $\Gamma_{\mathrm{P},1}^r$, $\Gamma_{\mathrm{P},2}^r, \ldots, \Gamma_{\mathrm{P},n}^r$ ($\Gamma_{\mathrm{C},1}^r, \Gamma_{\mathrm{C},2}^r, \ldots, \Gamma_{\mathrm{C},n}^r$). For $1 \leq i \leq n$, if both $\Gamma_{\mathrm{P},i}^r$ and $\Gamma_{\mathrm{C},i}^r$ are nonzero, then S_i^r is called an *active* s-box [2]. If the active s-boxes in round r are $S_{i_1}^r, S_{i_2}^r, \ldots, S_{i_A}^r$, and $b_{i_a}^r$ is the bias associated with LAT $\left[\Gamma_{\mathrm{P},i_a}^r, \Gamma_{\mathrm{C},i_a}^r\right]$ for $S_{i_a}^r$ $(1 \leq a \leq A)$, then

$$b_r = 2^{A-1} \prod_{a=1}^{A} b_{i_a}^r \tag{6}$$

by Matsui's Piling-up Lemma [9]. Note that $|b_r| \leq \left|b_{i_a}^r\right|$ for $1 \leq a \leq A$.

It follows from the above, and from equations (1) and (2), that for any independent key $\mathbf{K} \in \{0,1\}^{N(R+1)}$, and uniformly chosen $\mathbf{X} \in \{0,1\}^N$,

$$\mathrm{Prob}\left\{(\Gamma_{\mathrm{P}}^r \bullet \mathbf{X}) \oplus (\Gamma_{\mathrm{C}}^r \bullet S^r(\mathbf{X} \oplus \mathbf{K}^r)) = (\Gamma_{\mathrm{K}}^r \bullet \mathbf{K})\right\} = b_r + \frac{1}{2}\,.$$

Multi-round Linear Characteristics

Given T one-round characteristics $\Omega_1, \Omega_2, \ldots, \Omega_T$ satisfying $\pi(\Gamma_{\mathrm{C}}^t) = \Gamma_{\mathrm{P}}^{t+1}$ for $1 \leq t \leq (T-1)$ (recall that $\pi(\cdot)$ is the inter-round permutation), a single T-round characteristic may be formed from their concatenation:

$$\Omega = \left\langle \Gamma_{\mathrm{P}}^1,\ \Gamma_{\mathrm{C}}^T,\ \Gamma_{\mathrm{K}},\ b \right\rangle,$$

where $\Gamma_{\mathrm{K}} = \Gamma_{\mathrm{K}}^1 \oplus \Gamma_{\mathrm{K}}^2 \oplus \cdots \oplus \Gamma_{\mathrm{K}}^T$, and

$$b = 2^{T-1} \prod_{t=1}^{T} b_t \tag{7}$$

(again from the Piling-up Lemma). If $T = R$, and if Γ_{K}' is derived from Γ_{K} by setting the $(R+1)^{\mathrm{st}}$ (i.e., last) N-bit subblock of Γ_{K} to Γ_{C}^R, then the linear equation represented by $\Omega' = \left\langle \Gamma_{\mathrm{P}}^1,\ \Gamma_{\mathrm{C}}^T,\ \Gamma_{\mathrm{K}}',\ b \right\rangle$, namely

$$\Gamma_{\mathrm{P}}^1 \bullet \mathbf{P} \oplus \Gamma_{\mathrm{C}}^R \bullet \mathbf{C} = \Gamma_{\mathrm{K}}' \bullet \mathbf{K}\,, \tag{8}$$

has the form of (3) (holding with probability $p = b + \frac{1}{2}$, over the uniform distribution of plaintexts, $\mathbf{P}$).

In order to break DES, Matsui used auxiliary techniques which allowed a single linear characteristic to be used for the extraction of more than one key bit [9,11]. Since such techniques are not relevant to the discussion which follows, we do not present them here.

5 Model for Distribution of Biases

For the purpose of linear cryptanalysis, clearly the attacker is interested in the R-round linear characteristic whose accompanying bias is maximum in absolute

value, termed the *best* linear characteristic (such a characteristic is not necessarily unique), since it minimizes $\mathcal{N}_L$ (see (4)). (For the auxiliary techniques mentioned in Section 4 and applied to SPN's, $(R-q)$-round characteristics are used, for certain integers $q \geq 1$). We limit our consideration to linear characteristics which activate one or more s-boxes in each round, since this is a necessary condition for the accompanying bias (computed using the Piling-up Lemma) to be nonzero. Note that this condition need not be enforced for linear characteristics of ciphers based on the Feistel network architecture, such as DES.

Let $\mathcal{L}_R$ be the set of all R-round linear characteristics. For a fixed SPN, i.e., for a fixed set of s-boxes, and for a given $\Omega \in \mathcal{L}_R$, let $b(\Omega)$ be the bias associated with Ω. Define

$$B_R = \max\left\{|b(\Omega)| : \Omega \in \mathcal{L}_R\right\}.$$

Clearly $B_R \in \left[0, \frac{1}{2}\right]$. In addition, let $\mathcal{L}_R^A$ be the set of all R-round linear characteristics which activate a total of A s-boxes ($A \geq R$), and define

$$B_R^A = \max\left\{|b(\Omega)| : \Omega \in \mathcal{L}_R^A\right\}.$$

5.1 Modeling Biases of Characteristics in $\mathcal{L}_R^R$

We began our research by creating a computer program to search for the best R-round linear characteristic of a given SPN, for varying values of n and R. The program, tailored to the SPN structure, is based on Matsui's algorithm which finds the best linear characteristic of DES [10]. We quickly observed that the best characteristic almost always involved one active s-box in each round (i.e., it belonged to $\mathcal{L}_R^R$), especially as the s-box dimension was increased. In fact, when 500 16-round SPN's with 8×8 s-boxes were generated at random, the best linear characteristic for the first r rounds, $1 \leq r \leq 16$, was always found to be in $\mathcal{L}_R^R$.

This is not fully intuitive—increasing the number of active boxes in a given round allows the search algorithm more choices for the input mask to the next round, potentially increasing the absolute value of the bias associated with that round; but it also decreases the absolute value of the bias for the round having multiple active s-boxes, by increasing the number of terms in the product of the Piling-up Lemma (see (6)).

In this section, in keeping with the above observation, we derive information about the distribution of values of B_R^R. We begin with the following result [14,16]:

Lemma 1. *Let S be a bijective $n \times n$ s-box, $n \geq 2$, and let $\alpha, \beta \in \{0,1\}^n$, with $\alpha, \beta \neq 0$. Then the set of possible values for the bias associated with* $\mathrm{LAT}[\alpha, \beta]$ *is*

$$\left\{\frac{\pm 2\ell}{2^n} : \ell \text{ an integer, } 0 \leq \ell \leq 2^{n-2}\right\},$$

where the biases $\frac{\pm 2\ell}{2^n}$ each occur with probability

$$\frac{\binom{2^{n-1}}{2^{n-2}+\ell}^2}{\binom{2^n}{2^{n-1}}},$$

computed over the uniform distribution of bijective $n \times n$ s-boxes.

The probability distribution given by Lemma 1 for $n = 8$ is plotted in Figure 2 (using a $\log_{10}$ scale on the vertical axis).

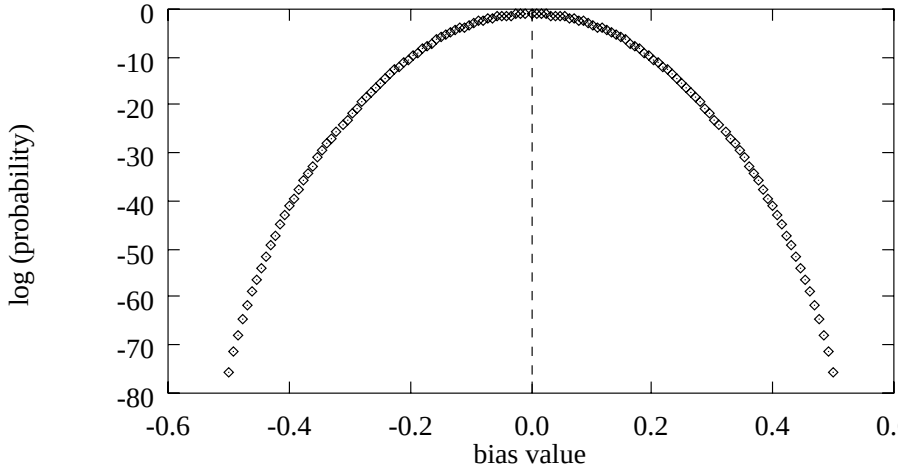

Fig. 2. Probability distribution for bias value of single LAT entry (8×8 bijective s-box)

Before proceeding to the next lemma, it is useful to define the following two sets, for $R \geq 1$ and $n \geq 2$:

$$\mathcal{H}_n = \left\{1, \ldots, 2^{n-2}\right\}$$
$$\mathcal{H}_n^R = \left\{\ell_1 \ell_2 \cdots \ell_R : \ \ell_r \in \mathcal{H}_n \text{ for } 1 \leq r \leq R\right\}.$$

Lemma 2. *Let $\Omega \in \mathcal{L}_R^R$. Then the set of possible nonzero values for $b(\Omega)$ is*

$$\left\{ \pm \frac{h}{2^{(n-2)R+1}} : \ h \in \mathcal{H}_n^R \right\}, \tag{9}$$

where the biases $\pm \frac{h}{2^{(n-2)R+1}}$ each occur with probability

$$2^{R-1} \sum_{\substack{\ell_1, \ell_2, \ldots, \ell_R \in \mathcal{H}_n \\ \ell_1 \ell_2 \cdots \ell_R = h}} \prod_{r=1}^{R} \frac{\binom{2^{n-1}}{2^{n-2}+\ell_r}^2}{\binom{2^n}{2^{n-1}}}, \tag{10}$$

computed over all R-round SPN's with s-boxes chosen uniformly and independently from the set of bijective $n \times n$ s-boxes. The probability that $b(\Omega) = 0$ is

given by

$$\left(\frac{\binom{2^{n-1}}{2^{n-2}}^2}{\binom{2^n}{2^{n-1}}}\right)^R + \sum_{T=1}^{R-1}\left[\binom{R}{T}2^{T-1}\left(\sum_{\ell_1,\ldots,\ell_T\in\mathcal{H}_n}\prod_{t=1}^{T}\frac{\binom{2^{n-1}}{2^{n-2}+\ell_t}^2}{\binom{2^n}{2^{n-1}}}\right)\left(\frac{\binom{2^{n-1}}{2^{n-2}}^2}{\binom{2^n}{2^{n-1}}}\right)^{R-T}\right].$$

Proof. Each $\Omega \in \mathcal{L}_R^R$ represents a "chain" of active s-boxes through the SPN. Since Ω uniquely determines the n-bit input/output masks for each active s-box, the bias associated with each s-box is determined by a single LAT entry. Let b_r be the bias associated with the active s-box in round r, for $1 \le r \le R$. It follows that b_r takes on the values (with the corresponding probabilities) of Lemma 1.

Now suppose that $b(\Omega) \neq 0$ (therefore each $b_r \neq 0$). Let $s = s(\Omega)$ be the number of active s-boxes whose bias is *negative*. Then from (7), $b(\Omega)$ is of the form

$$\begin{aligned}
2^{R-1}\prod_{r=1}^{R} b_r &= (-1)^s\ 2^{R-1}\left(\frac{2\ell_1}{2^n}\right)\left(\frac{2\ell_2}{2^n}\right)\cdots\left(\frac{2\ell_R}{2^n}\right), \text{ for some } \ell_1,\ldots,\ell_R \in \mathcal{H}_n \\
&= (-1)^s\ \frac{\ell_1\ell_2\cdots\ell_R}{2^{(n-2)R+1}} \\
&= (-1)^s\ \frac{h}{2^{(n-2)R+1}}, \quad h = \ell_1\ell_2\cdots\ell_R \in \mathcal{H}_n^R\ ,
\end{aligned}$$

which gives (9).

Consider the case that $b(\Omega)$ is positive, i.e., $b(\Omega) = \frac{h}{2^{(n-2)R+1}}$ for some $h \in \mathcal{H}_n^R$ (so $s(\Omega)$ is even). We have $|b_r| = \frac{2\ell_r}{2^n}$, for some $\ell_r \in \mathcal{H}_n$ $(1 \le r \le R)$, with $\ell_1\ell_2\cdots\ell_R = h$. Keeping the ℓ_r fixed, there are 2^{R-1} ways of assigning $+/-$ signs to the b_r such that $s(\Omega)$ is even. For any such assignment, it follows from Lemma 1 that the probability that the active s-boxes will yield the sequence of biases $b_1, b_2, \ldots, b_R$ is

$$\prod_{r=1}^{R}\frac{\binom{2^{n-1}}{2^{n-2}+\ell_r}^2}{\binom{2^n}{2^{n-1}}}\ .$$

Summing over all $\ell_1, \ell_2, \ldots, \ell_R$ such that $\ell_1\ell_2\cdots\ell_R = h$, we get (10). It is easy to see that the case $b(\Omega) = \frac{-h}{2^{(n-2)R+1}}$ occurs with the same probability.

The proof in the case $b(\Omega) = 0$ is based on the observation that a sequence of bias values $b_1, b_2, \ldots, b_R$ whose product is 0 must consist of T nonzero values (and $(R-T)$ zero values), for some T, with $0 \le T \le (R-1)$. The details are omitted here.

Lemma 3. $\#\mathcal{L}_R^R = n^R\,(2^n-1)^2$.

Proof. The number of ways to choose one active s-box per round is n^R. For a given choice of active s-boxes, the n-bit output mask for the active s-box in round r, $1 \le r \le (R-1)$, is determined: it consists of all zeros with a 1 in

position j, where j is the index of the active s-box in round $r+1$. Similarly, the n-bit input masks for the active s-boxes in rounds $2 \ldots R$ are determined. All that remains is the choice of input mask for the active s-box in round 1, and the output mask for the active s-box in round R. Since each such n-bit mask must be nonzero, we have $(2^n - 1)^2$ choices, and the result follows.

The main result of this section is given in Theorem 1. First, however, it is useful to have the following intermediate result. For $\Omega \in \mathcal{L}_R^A$ and $\lambda \in \left(0, \frac{1}{2}\right]$, define

$$p_R^A(\lambda) = \text{Prob}\left\{|b(\Omega)| \geq \lambda\right\},$$

computed over all R-round SPN's with s-boxes chosen uniformly and independently from the set of bijective $n \times n$ s-boxes. Arguing as in the proof of Lemma 2, it can be shown that $p_R^A(\lambda)$ is independent of the choice of $\Omega \in \mathcal{L}_R^A$.

Lemma 4. *Let $\lambda \in \left(0, \frac{1}{2}\right]$, and define $\Lambda = \lambda \cdot 2^{(n-2)R+1}$. Then*

$$p_R^R(\lambda) = 2^R \sum_{\substack{h \in \mathcal{H}_n^R \\ h \geq \Lambda}} \left[\sum_{\substack{\ell_1, \ldots, \ell_R \in \mathcal{H}_n \\ \ell_1 \cdots \ell_R = h}} \prod_{r=1}^{R} \frac{\binom{2^{n-1}}{2^{n-2}+\ell_r}^2}{\binom{2^n}{2^{n-1}}} \right].$$

Proof. Let $\Omega \in \mathcal{L}_R^R$. Then $p_R^R(\lambda) = \text{Prob}\left\{|b(\Omega)| \geq \lambda\right\} = 2 \cdot \text{Prob}\left\{b(\Omega) \geq \lambda\right\}$, since the distribution of probabilities corresponding to the possible values of $b(\Omega)$ is symmetric about 0, by Lemma 2. Therefore, we can assume that $b(\Omega)$ is positive, and write $b(\Omega) = \frac{h}{2^{(n-2)R+1}}$, for some $h \in \mathcal{H}_n^R$. It follows that

$$\begin{aligned} p_R^R(\lambda) &= 2 \cdot \text{Prob}\left\{b(\Omega) \geq \lambda\right\} \\ &= 2 \cdot \text{Prob}\left\{h \geq \lambda \cdot 2^{(n-2)R+1}\right\} \\ &= 2 \cdot \text{Prob}\left\{h \geq \Lambda\right\} \\ &= 2^R \sum_{\substack{h \in \mathcal{H}_n^R \\ h \geq \Lambda}} \left[\sum_{\substack{\ell_1, \ldots, \ell_R \in \mathcal{H}_n \\ \ell_1 \cdots \ell_R = h}} \prod_{r=1}^{R} \frac{\binom{2^{n-1}}{2^{n-2}+\ell_r}^2}{\binom{2^n}{2^{n-1}}} \right], \qquad (11) \end{aligned}$$

where (11) follows from (10) in Lemma 2.

Theorem 1. *Consider an R-round SPN with $n \times n$ s-boxes, n per round, and assume that each s-box is chosen uniformly and independently from the set of all bijective $n \times n$ s-boxes. Let the inter-round permutation, $\pi(\cdot)$, be as above. If $\lambda \in \left(0, \frac{1}{2}\right]$, and $\Lambda = \lambda \cdot 2^{(n-2)R+1}$ then*

$$\text{Prob}\left\{B_R^R \geq \lambda\right\} \leq (2n)^R (2^n - 1)^2 \sum_{\substack{h \in \mathcal{H}_n^R \\ h \geq \Lambda}} \left[\sum_{\substack{\ell_1, \ldots, \ell_R \in \mathcal{H}_n \\ \ell_1 \cdots \ell_R = h}} \prod_{r=1}^{R} \frac{\binom{2^{n-1}}{2^{n-2}+\ell_r}^2}{\binom{2^n}{2^{n-1}}} \right]. \qquad (12)$$

Proof. We have

$$\begin{aligned} \text{Prob}\left\{B_R^R \geq \lambda\right\} &= \text{Prob}\left\{\exists\ \Omega \in \mathcal{L}_R^R \text{ such that } |b(\Omega)| \geq \lambda\right\} \\ &\leq \sum_{\Omega \in \mathcal{L}_R^R} \text{Prob}\left\{|b(\Omega)| \geq \lambda\right\} \qquad (13) \\ &= \#\mathcal{L}_R^R \cdot p_R^R(\lambda)\ , \qquad (14) \end{aligned}$$

where (14) follows from (13) because the distribution of $b(\Omega)$ is independent of the choice of Ω. Substituting the results from Lemma 3 and Lemma 4 into (14) and combining constant terms gives (12), finishing the proof.

5.2 An Improved Result

Since the initial submission of this paper, we have been able to generalize the main result (Theorem 1). The improved result, given in Theorem 2 below, upper bounds the probability that linear cryptanalysis of an SPN using linear characteristics is feasible, with no restriction on the number of active s-boxes (of course, we still require a *minimum* of one active s-box per round).

Theorem 2. *Consider an R-round SPN with $n \times n$ s-boxes, n per round, and assume that each s-box is chosen uniformly and independently from the set of all bijective $n \times n$ s-boxes. Let the inter-round permutation, $\pi(\cdot)$, be as above. If $\lambda \in \left(0, \frac{1}{2}\right]$, and $\Lambda = \lambda \cdot 2^{(n-2)R+1}$ then*

$$\text{Prob}\left\{B_R \geq \lambda\right\} \ \leq \ \sum_{A=R}^{nR} \#\mathcal{L}_R^A \cdot p_R^A(\lambda)\ . \qquad (15)$$

Comment on Proof and Computation

Arguing as in the proof of Theorem 1, it follows that each term in the sum of (15) of the form $\#\mathcal{L}_R^A \cdot p_R^A(\lambda)$ is an upper bound on the probability that linear cryptanalysis is feasible using characteristics from $\mathcal{L}_R^A$. Therefore the sum of all such terms is an upper bound on the probability that linear cryptanalysis using any $\Omega \in \mathcal{L}_R$ is feasible.

In order to extract useful values from (15), it is necessary to transform the right-hand side into an expression which can be evaluated. The sub-terms p_R^A can be evaluated using a slightly modified version of Lemma 4. The main work lies in computing the sub-terms $\#\mathcal{L}_R^A$. We solved this in a recursive fashion. The key observation is that if $\Omega \in \mathcal{L}_R^A$ activates α s-boxes in round R, then the sub-characteristic Ω' obtained by removing round R is an element of $\mathcal{L}_{R-1}^{A-\alpha}$. Counting the number of ways that an R^{th} round with α active s-boxes can be added to Ω', and summing over all values of α, completes the computation. The details can be found in the full version of this paper.

6 Computational Results

The second computer program created to carry out this research computes the distribution of biases associated with an R-round characteristic $\Omega \in \mathcal{L}_R^R$, as given by Lemma 2. The program works iteratively, computing the distribution for a given round r before proceeding to round $(r+1)$. For $n = 8$ and $R = 3$, the resulting distribution has 28451 bias values. These are plotted in Figure 3, using a $\log_{10}$ scale for the y-axis.

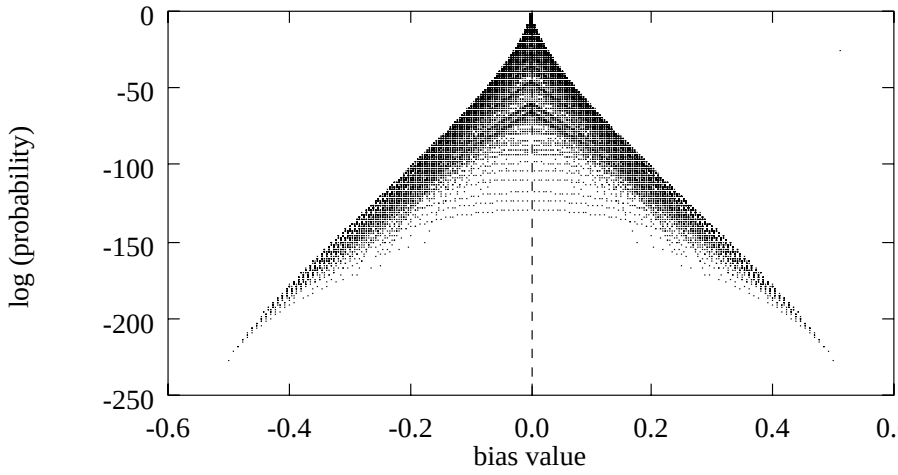

Fig. 3. Distribution of $b(\Omega)$ for $\Omega \in \mathcal{L}_R^R$, with $n = 8$, $R = 3$

Linear cryptanalysis of an N-bit SPN using an R-round linear characteristic $\Omega \in \mathcal{L}_R^R$ is *feasible* if the number of plaintexts required in the best case is at most 2^N, the number of plaintexts available, i.e., if

$$\mathcal{N}_L = \frac{1}{\left(B_R^R\right)^2} \leq 2^N \iff B_R^R \geq 2^{-N/2} \tag{16}$$

(this is for Matsui's Algorithm 1, with a success rate of 97.7% [9]). Setting $\lambda = 2^{-N/2}$, Theorem 1 gives an upper bound on the probability that (16) holds. A modified version of the program used to determine the distribution of $b(\Omega)$ above, for $\Omega \in \mathcal{L}_R^R$, was used to evaluate this upper bound, by computing (14). Results for the case $n = 8$, $N = 64$ (so $\lambda = 2^{-32}$), and $R = 10 \ldots 16$ are presented in the second column of Table 1. The third column of Table 1 gives the upper bound from the improved result of Theorem 2. In addition, the fourth column of Table 1 gives the experimental probability that (16) holds, obtained by generating 500 16-round, 64-bit SPN's with random 8×8 s-boxes, and computing B_R^R for the first r rounds, for $10 \leq r \leq 16$. (In fact we computed B_R, and found that in each case it was identical to B_R^R, as mentioned in Section 5.)

It is quite interesting that the generalized upper bound of Theorem 2 yields values which are very close to the values obtained from Theorem 1 (in fact, for $R \geq 13$ they are identical to four decimal places). This is evidence that the first term of the sum in (15) (which is exactly the upper bound of Theorem 1) is the dominant term, supporting our earlier observation that the best linear characteristic is usually found in $\mathcal{L}_R^R$.

Number of rounds	Restricted upper bound (Theorem 1)	Unrestricted upper bound (Theorem 2)	Experimental (500 trials)	$\mathcal{N}_L$ lower bound (older result)
10	–	–	1.000	2^{30}
11	–	–	0.962	2^{33}
12	4.3823×10^{-3}	4.3824×10^{-3}	0.000	2^{36}
13	4.6480×10^{-10}	4.6480×10^{-10}	0.000	2^{39}
14	8.8615×10^{-19}	8.8615×10^{-19}	0.000	2^{42}
15	2.8796×10^{-29}	2.8796×10^{-29}	0.000	2^{44}
16	1.5177×10^{-41}	1.5177×10^{-41}	0.000	2^{47}

Table 1. Probability that linear cryptanalysis is feasible, for $n = 8$, $R = 10 \ldots 16$ (contrasted with lower bound on $\mathcal{N}_L$)

We have placed the values of Table 1 in the context of an earlier related result. In [7], Heys and Tavares, using the same SPN structure, give an expression which provides a lower bound on $\mathcal{N}_L$ in terms of $\mathrm{NL}_{\min}$, namely

$$\mathcal{N}_L \;\geq\; 2^{2(1-R)} \left(\frac{2^n}{2^{n-1} - \mathrm{NL}_{\min}} \right)^{2R}. \tag{17}$$

This is based on the worst-case scenario (from the perspective of the cipher designer): the existence of an R-round linear characteristic in $\mathcal{L}_R^R$, such that the absolute value of the bias associated with each active s-box is the maximum possible, namely $\left| \left(2^{n-1} - \mathrm{NL}_{\min}\right) / 2^n \right|$. Evaluating (17) in the case $n = 8$ ($N = 64$), with $\mathrm{NL}_{\min} = 80$, gives the values in the rightmost column of Table 1. Taken alone, these lower bounds seem to imply that linear cryptanalysis of at least 16 rounds is feasible (in fact, (17) does not tell us that linear cryptanalysis becomes infeasible until $R \geq 22$). However, the result of Theorem 2 shows this to be excessively pessimistic—the probability that linear cryptanalysis of an SPN is feasible, using any characteristic $\Omega \in \mathcal{L}_R$, is small for $R \geq 12$ (computed over all SPN's, as per our model). This evidence of resistance to linear cryptanalysis is especially interesting when compared to a result of Chen [3], who showed that under certain assumptions about the XOR tables of the s-boxes, the same 64-bit SPN is also resistant to differential cryptanalysis for $R \geq 12$.

7 Conclusion

In this paper we have presented a model for the bias values associated with linear characteristics of substitution-permutation networks. We first considered linear characteristics which activate one s-box in each round, since experimentally these usually provide the best bias value. We determined the distribution of bias values which can be associated with such characteristics. This allowed us to evaluate an upper bound on the probability that linear cryptanalysis using such linear characteristics is feasible, as a function of the number of rounds. This probability is computed over all SPN's with s-boxes chosen uniformly and independently from the set of all bijective $n \times n$ s-boxes.

We then gave a generalization of the above result, stating an upper bound on the probability that linear cryptanalysis of an SPN is feasible, with no restriction on the number of s-boxes activated by the linear characteristics used. Experimental data indicates that the restricted and the generalized upper bounds yield nearly identical values, supporting the observation that the best linear characteristics almost always activate one s-box per round.

The work of this paper further supports the idea that the basic SPN structure merits study, both as a source of theoretical results, and as a practical cipher architecture with good security properties after a relatively small number of rounds.

Acknowledgment

This work was funded in part by Communications and Information Technology Ontario (CITO), and by the Natural Sciences and Engineering Research Council (NSERC), Canada.

References

1. R. Anderson, E. Biham and L. Knudsen, *Serpent: A flexible block cipher with maximum assurance,* The First Advanced Encryption Standard Candidate Conference, Proceedings, Ventura, California, August 1998.
2. E. Biham, *On Matsui's linear cryptanalysis,* Advances in Cryptology—EUROCRYPT'94, Springer-Verlag, Berlin, pp. 341–355, 1995.
3. Z.G. Chen and S.E. Tavares, *Towards provable security of substitution-permutation encryption networks,* Fifth Annual International Workshop on Selected Areas in Cryptography—SAC'98, Springer-Verlag, Berlin, LNCS 1556, pp. 43–56, 1999.
4. H. Feistel, *Cryptography and computer privacy,* Scientific American, Vol. 228, No. 5, pp. 15–23, May 1973.
5. H.M. Heys, *The design of substitution-permutation network ciphers resistant to cryptanalysis,* Ph.D. Thesis, Queen's University, Kingston, Canada, 1994.
6. H.M. Heys and S.E. Tavares, *Avalanche characteristics of substitution-permutation encryption networks,* IEEE Transactions on Computers, Vol. 44, No. 9, pp. 1131–1139, September 1995.

7. H.M. Heys and S.E. Tavares, *Substitution-permutation networks resistant to differential and linear cryptanalysis,* Journal of Cryptology, Vol. 9, No. 1, pp. 1–19, 1996.
8. J.B. Kam and G.I. Davida, *Structured design of substitution-permutation encryption networks,* IEEE Transactions on Computers, Vol. C-28, No. 10, pp. 747–753, October 1979.
9. M. Matsui, *Linear cryptanalysis method for DES cipher,* Advances in Cryptology—Proceedings of EUROCRYPT'93, Springer-Verlag, Berlin, pp. 386–397, 1994.
10. M. Matsui, *On correlation between the order of s-boxes and the strength of DES,* Advances in Cryptology—EUROCRYPT'94, Springer-Verlag, Berlin, pp. 366–375, 1995.
11. M. Matsui, *The first experimental cryptanalysis of the Data Encryption Standard,* Advances in Cryptology—CRYPTO'94, Springer-Verlag, Berlin, pp. 1–11, 1994.
12. National Institute of Standards and Technology, Information Technology Laboratory, The First Advanced Encryption Standard Candidate Conference, Proceedings, Ventura, California, August 1998.
13. K. Nyberg, *Linear approximation of block ciphers,* Advances in Cryptology—EUROCRYPT'94, Springer-Verlag, Berlin, pp. 439–444, 1995.
14. L. O'Connor, *Properties of linear approximation tables,* Fast Software Encryption: Second International Workshop, Springer-Verlag, Berlin, pp. 131–136, 1995.
15. C.E. Shannon, *Communication theory of secrecy systems,* Bell System Technical Journal, Vol. 28, no. 4, pp. 656–715, 1949.
16. A.M. Youssef and S.E. Tavares, *Resistance of balanced s-boxes to linear and differential cryptanalysis,* Information Processing Letters, Vol. 56, pp. 249–252, 1995.
17. A.M. Youssef *Analysis and design of block ciphers* Ph.D. Thesis, Queen's University, Kingston, Canada, 1997.