The Design of Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis

H. M. Heys† and S. E. Tavares‡

†Electrical Engineering
Memorial University of Newfoundland
St. John's, Newfoundland, Canada

‡Department of Electrical and Computer Engineering
Queen's University
Kingston, Ontario, Canada

Abstract — In this paper we examine a class of product ciphers referred to as substitution-permutation networks. We investigate the resistance of these cryptographic networks to two important attacks: differential cryptanalysis and linear cryptanalysis. In particular, we develop upper bounds on the differential characteristic probability and on the probability of a linear approximation as a function of the number of rounds of substitutions. Further, it is shown that using large S-boxes with good diffusion characteristics and replacing the permutation between rounds by an appropriate linear transformation is effective in improving the cipher security in relation to these two attacks.

I. Introduction

A substitution-permutation network (SPN) is a practical product cipher [1][2] implemented as a number of rounds of small substitutions (referred to as S-boxes) connected by bit position permutations. Such ciphers map closely to Shannon's fundamental principles of "confusion" and "diffusion" [3].

Recent cryptanalysis techniques have had a notable effect on the perceived security of many product ciphers. For example, DES [4] has been found to be theoretically cryptanalyzable by differential cryptanalysis using a chosen plaintext approach [5] and by linear cryptanalysis using a known plaintext approach [6]. In this paper, we examine the security of SPNs with respect to these two powerful cryptanalysis techniques and suggest structures that aid in resisting the attacks. In particular, we develop upper bounds on the probability of a differential characteristic and on the deviation of the probability of a linear approximation from the ideal value of 1/2. The objective of the analysis is to determine a flexible architecture that can be efficiently implemented in as few rounds as possible to provide suitably small probabilities for differential characteristics and linear approximations.

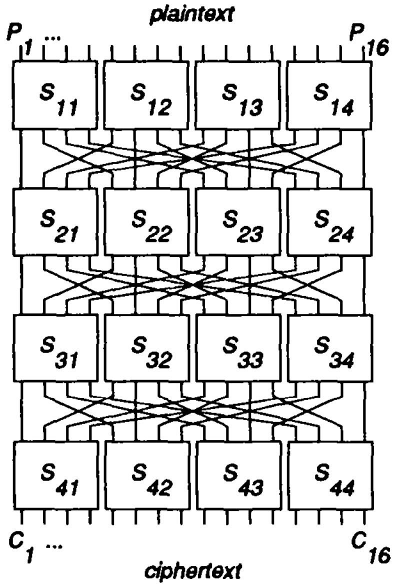

Figure 1. SPN with $N = 16$, $R = 4$, and $n = 4$.

We shall consider a general N-bit SPN as consisting of R rounds of $n \times n$ S-boxes. The number of S-boxes used in each round is represented by M where $M = N/n$. The plaintext and ciphertext are N-bit vectors denoted as $\mathbf{P} = [P_1\ P_2\ ...\ P_N]$ and $\mathbf{C} = [C_1\ C_2\ ...\ C_N]$, respectively. An S-box in the network is defined as an n-bit bijective mapping $S\ :\ \mathbf{X} \rightarrow \mathbf{Y}$ where $\mathbf{X} = [X_1\ X_2\ ...\ X_n]$ and $\mathbf{Y} = [Y_1\ Y_2\ ...\ Y_n]$. A simple example of an SPN is illustrated in Figure 1 with $N = 16$, $R = 4$, and $n = 4$.

We shall assume in our discussion that the network is keyed by XORing N bits of key (as determined by the key scheduling algorithm) before the first substitution, after the last substitution, and between all substitutions. Decryption is performed by applying the key scheduling algorithm in reverse and using the inverse S-boxes.

Rather than strictly confining ourselves to the basic form of substitutions connected by permutations, in this paper

CCS '94- 11/94 Fairfax Va., USA
© 1994 ACM 0-89791-732-4/94/0011..$3.50

we consider the more general model of substitutions connected by invertible linear transformations. However, for consistency, we still refer to the more general architecture as an SPN.

Of particular importance to our discussion is the notion of nonlinearity and we shall use the following nonlinearity measures when referring to a boolean function or an S-box. The nonlinearity of an n-input boolean function, $f : \{0,1\}^n \rightarrow \{0,1\}$, is defined as the Hamming distance to the nearest affine function:

$$NL(f) = \min_{U_1,\ldots,U_n,V\in\{0,1\}} \#\left\{\mathbf{X} \mid f(\mathbf{X}) \neq \bigoplus_{i=1}^{n} U_i X_i \oplus V\right\}. \tag{1}$$

The nonlinearity of an $n \times n$ bijective mapping or S-box S is defined as the minimum nonlinearity of all non-zero linear combinations of output functions [7]:

$$NL(S) = \min_{W_1,\ldots,W_n\in\{0,1\},\ \text{all}\ W_i\neq 0} NL\left(\bigoplus_{i=1}^{n} W_i f_i\right) \tag{2}$$

where f_i represents the n-input function of the i-th output of the S-box. Letting S^{-1} represent the inverse S-box of S-box S, it can be shown that $NL(S^{-1}) = NL(S)$ [7].

II. Two Important Classes of Cryptanalysis

In this section we discuss two important classes of cryptanalysis which have had significant success against product ciphers.

(a) Differential Cryptanalysis

In a series of papers [5][8][9][10], Biham and Shamir successfully demonstrate the susceptibility of several product ciphers to differential cryptanalysis. Notably, differential cryptanalysis has been successful in breaking weakened versions of DES and can theoretically compromise the security of the full 16–round DES algorithm using 2^{47} chosen plaintexts.

Differential cryptanalysis is an attack which examines changes in the output of the cipher in response to controlled changes in the input. In general, we are interested in bit changes or XOR differences within the network when two plaintexts, $\mathbf{P}'$ and $\mathbf{P}''$ are selected as inputs. We represent the XOR difference of the two plaintexts by $\Delta\mathbf{P} = \mathbf{P}' \oplus \mathbf{P}''$. Let the input and output difference to a particular round i be represented by $\Delta\mathbf{U}_i$ and $\Delta\mathbf{V}_i$, respectively. Differential cryptanalysis relies on the existence of highly probable "characteristics" where an r-round characteristic, Ω_r, is defined as a sequence of difference pairs: $\Omega_r = \{(\Delta\mathbf{U}_1, \Delta\mathbf{V}_1), ..., (\Delta\mathbf{U}_r, \Delta\mathbf{V}_r)\}$. The algorithm tries an appropriate number of chosen plaintexts with $\Delta\mathbf{P} = \Delta\mathbf{U}_1$ and counts the number of times that a sub-key consisting of a subset of the key bits is consistent with the ciphertext difference, $\Delta\mathbf{C}$, assuming that the characteristic has occurred. If the characteristic occurs with probability p_{Ω_r}, the correct sub-key bits are consistent with a probability of at least p_{Ω_r}. After an appropriate number of trials (typically several times more than $1/p_{\Omega_r}$ chosen plaintext pairs) the correct sub-key will be counted significantly more times than incorrect sub-keys.

In this paper, we shall assume that a characteristic probability is determined by the product of the probabilities of the occurrence of a one round difference pair. Letting $P(\Delta\mathbf{U}_i, \Delta\mathbf{V}_i)$ represent the probability of occurrence of the i-th round difference pair, then

$$p_{\Omega_r} = \prod_{i=1}^{r} P(\Delta\mathbf{U}_i, \Delta\mathbf{V}_i). \tag{3}$$

Equation (3) gives exactly the characteristic probability taken over the independent distributions of plaintext and key. Hence, it strictly applies only when the plaintext and the keys applied at each round are independent and uniformly randomly selected for the encryption of each plaintext pair. In practice, equation (3) has been found to provide a reasonable estimate of the characteristic probability in ciphers with mutually dependent round keys.

Differential cryptanalysis of a basic SPN can be applied similarly to the attack on DES-like ciphers. For a DES-like cipher, differential cryptanalysis determines key bits associated with the input to the last round function by using knowledge (directly available from the right half of the ciphertext) of the two input values (and their difference) to the last round function combined with probabilistic knowledge of the output difference of the last round function. Similarly, differential cryptanalysis of a basic SPN can be used to determine the key bits XORed to the output of the last round of S-boxes by using knowledge of the two ciphertext values (and their difference) and the probabilistic knowledge of the input difference to the last round of S-boxes.

Hence, a differential attack may be successful if the cryptanalyst is aware of a highly probable characteristic for the first $R-1$ rounds, Ω_{R-1}. The attack targets the round R S-boxes that are affected by the output changes of the characteristic, $\Delta\mathbf{V}_{R-1}$. The targeted sub-key contains the key bits which are XORed with the output of the targeted S-boxes. Consequently, trying all sub-key values, the cryptanalyst can use the known ciphertext values to decrypt the portion of round R associated with the target S-boxes. (Ciphertext pairs which have bit changes in the output of non-targeted S-boxes may be discarded since they can not be generated by characteristic Ω_{R-1}.) If the XOR difference of the target S-box inputs determined by the partial decryption corresponds to $\Delta\mathbf{V}_{R-1}$, then the corresponding sub-key count is incremented. The actual sub-key may be deduced as the key which is consistent most frequently over a number of trials.

In this paper we shall assume that the characteristic probability provides a reasonable estimate of the probability that round r will have a particular output difference, $\Delta\mathbf{V}_r$, given $\Delta\mathbf{P}$. Differential cryptanalysis requires only the likely occurrence of a particular $\Delta\mathbf{V}_r$ and it is conceivable that this $\Delta\mathbf{V}_r$ could occur as the result of several highly probable characteristics. Although the characteristic probability p_{Ω_r} is actually a lower bound on the probability that a particular $\Delta\mathbf{V}_r$ occurs, in cases where a highly probable characteristic may be found, we assume that it dominates the probability of $\Delta\mathbf{V}_r$ and the actual probability of $\Delta\mathbf{V}_r$ is very close to p_{Ω_r}.

Using this assumption, we may approximate the number of chosen plaintexts required to determine the sub-key by N_D where

$$N_D = 1/p_{\Omega_{R-1}}. \tag{4}$$

In practice, the number of chosen plaintexts required will be greater than N_D since we have neglected the factor of 2 (which arises from the fact that the chosen plaintexts are encrypted in pairs) and since many incorrect sub-keys, as well as the correct sub-key, are counted at least once.

Let $\Delta\mathbf{X}$ and $\Delta\mathbf{Y}$ represent the input and output XOR differences, respectively, to an S-box when a plaintext difference $\Delta\mathbf{P}$ is applied to the cipher. The existence of highly probable characteristics depends on two factors: the distribution of S-box XOR difference pairs, $(\Delta\mathbf{X}, \Delta\mathbf{Y})$, and the diffusion of bit changes within the network. We define the probability of an S-box XOR pair $(\Delta\mathbf{X}, \Delta\mathbf{Y})$ to be the probability that $\Delta\mathbf{Y}$ occurs given that one of the input values for $\mathbf{X}$ is randomly selected and the other is related by the difference $\Delta\mathbf{X}$. Let the probability of the most likely S-box XOR pair (other than $(\Delta\mathbf{X} = 0, \Delta\mathbf{Y} = 0)$) be p_δ.

In [11], O'Connor shows that, for large n, the S-box XOR pair probability is expected to be at most $n/2^{n-1}$. Hence, the expected maximum XOR pair probability decreases as the size of the S-box is increased. For 8 × 8 S-boxes, the expected maximum XOR pair probability satisfies $p_\delta \leq 2^{-4}$.

(b) Linear Cryptanalysis

In [6], Matsui presents an effective linear cryptanalysis method for DES. The attack uses a known plaintext technique to extract key information by finding a linear equation consisting of plaintext, ciphertext, and key terms which is statistically likely to be satisfied. The full 16–round DES algorithm is susceptible to the attack with 2^{47} known plaintexts and it is shown that the attack can even be modified to be successful on an 8–round version of DES with 2^{29} encrypted ASCII-coded English blocks using a ciphertext only attack.

In order to attack an SPN using the linear cryptanalysis technique, the cryptanalyst is interested in the best R-round linear approximation of the form:

$$P_{i_1} \oplus ... \oplus P_{i_\gamma} \oplus C_{j_1} \oplus ... \oplus C_{j_\zeta} = K_{k_1} \oplus ... \oplus K_{k_\theta}. \tag{5}$$

If we let p_L represent the probability that equation (5) is satisfied, in order for the linear approximation to be valid $p_L \neq 1/2$ and the best expression is the equation for which $|p_L - 1/2|$ is maximized. If the magnitude $|p_L - 1/2|$ is large enough and sufficient plaintext-ciphertext pairs are available, the equivalent of one key bit, expressed by the XOR sum of the key bits on the right side of equation (5) may be guessed as the value that most often satisfies the linear approximation.

An appropriate linear expression is derived by combining a number of linear expressions for different rounds such that any intermediate terms (i.e., terms that are not plaintext, ciphertext, or key terms) are cancelled. Let the best linear approximation of an S-box, in the form $a_1X_1 \oplus ... \oplus a_nX_n = b_1Y_1 \oplus ... \oplus b_nY_n$, be satisfied with probability p_ϵ assuming input $\mathbf{X}$ is randomly selected. In this paper, we consider the probability that a system linear expression is satisfied to be taken over the independent distributions of plaintext and key. Hence, since the key bits XORed to the network bits prior to entering the S-boxes are independent and uniformly random, the inputs to the S-boxes involved in the linear approximation are independent and uniformly random. Under this assumption, it then follows from Lemma 3 in [6] that

$$|p_L - 1/2| \leq 2^{\alpha-1}|p_\epsilon - 1/2|^\alpha \tag{6}$$

where α is the number of S-box linear approximations combined to give the overall linear approximation.

It can be shown [6] that the number of known plaintexts required to give a 97.7% confidence in the correct key bit may be approximated by N_L where

$$N_L = |p_L - 1/2|^{-2}. \tag{7}$$

It is obvious that N_L can be increased by decreasing $|p_L - 1/2|$. Hence, selecting S-boxes for which $p_\epsilon \rightarrow 1/2$ will clearly aid in thwarting the attack. As well, the larger the number of S-boxes, α, involved in the system equation, the smaller $|p_L - 1/2|$ and the more known plaintexts required for the cryptanalysis.

III. S-box Design Criteria

In this section, we consider S-box design criteria that are relevant to the two attacks and examine the procedures that may be followed to generate S-boxes that satisfy such design constraints.

(a) Diffusion

S-boxes that effectively diffuse bit changes increase resistance to differential cryptanalysis. The diffusion properties of an S-box can be considered by examining the relationship between input and output XORs. Let $wt(\cdot)$ represent the Hamming weight of the specified argument and consider the following definition.

Definition 1: An S-box satisfies a *diffusion order of* λ, $\lambda \geq 0$, if, for $wt(\Delta \mathbf{X}) > 0$,

$$wt(\Delta \mathbf{Y}) > \begin{cases} \lambda + 1 - wt(\Delta \mathbf{X}) & , wt(\Delta \mathbf{X}) < \lambda + 1 \\ 0 & , otherwise. \end{cases} \tag{8}$$

Note that all bijective S-boxes satisfy $\lambda = 0$ and that DES S-boxes satisfy $\lambda = 1$ [12]. As well, the diffusion order is bidirectional, i.e., the inverse S-box S^{-1} satisfies the same diffusion order as S-box S.

Let Π represent the set of permutations for which no two outputs of an S-box are connected to one S-box in the next round. Note that the set Π will only be non-empty if $M \geq n$.

Lemma 1: Let ψ_{r-1} and ψ_{r+1} represent the number of S-boxes included in a characteristic from round $r-1$ and round $r+1$, respectively. For an SPN with $M \geq n$ S-boxes in each round, using a permutation $\pi \in \Pi$ and S-boxes with a diffusion order of λ,

$$\psi_{r-1} + \psi_{r+1} \geq \lambda + 2. \tag{9}$$

Proof: Let w_X and w_Y represent the number of input and output bit changes for a particular S-box in round r selected such that $w_X \neq 0$. From the constraint placed on the permutations of Π and considering that $M \geq n$ and $w_X, w_Y \leq n$, we see that $\psi_{r-1} \geq w_X$ and $\psi_{r+1} \geq w_Y$. Hence,

$$\psi_{r-1} + \psi_{r+1} \geq w_X + w_Y. \tag{10}$$

From the definition of diffusion order, $w_X + w_Y \geq \lambda + 2$ and the inequality of (9) follows. □

Theorem 1: Consider an SPN of R rounds of M S-boxes such that R is a multiple of 4 and $M \geq n$. Using a permutation $\pi \in \Pi$, the probability of an $(R-1)$-round characteristic satisfies

$$p_{\Omega_{R-1}} \leq (p_\delta)^{\frac{\lambda+2}{2}R-(\lambda+1)} \tag{11}$$

where all S-boxes satisfy diffusion order λ and p_δ represents the maximum S-box XOR pair probability.

Proof: An upper bound on the most probable $(R-1)$-round characteristic can be derived by considering the concatenation of the most probable $(R-4)$-round characteristic and the most probable 3–round characteristic. Further, a bound on the most likely $(R-4)$-round characteristic can be determined as $(R-4)/4$ iterations of the most probable 4–round characteristic, and, hence, the $(R-1)$-round characteristic probability satisfies

$$p_{\Omega_{R-1}} \leq (p_{\Omega_4}^{max})^{\frac{R-4}{4}}(p_{\Omega_3}^{max}) \tag{12}$$

where $p_{\Omega_3}^{max}$ and $p_{\Omega_4}^{max}$ are upper bounds on the probability of 3 and 4–round characteristics, respectively.

In general, an upper bound on a characteristic probability can be derived by determining the characteristic which involves the fewest number of S-boxes and utilizing the maximum S-box XOR pair probability p_δ. From Lemma 1, the minimum number of S-boxes used by a characteristic in any 4 consecutive rounds is $2(\lambda+2)$ and therefore

$$p_{\Omega_4}^{max} = (p_\delta)^{2(\lambda+2)}. \tag{13}$$

As well, by considering that the constraint of Lemma 1 applies to the first and third rounds of a 3–round characteristic and that the second round has only one S-box, the minimum number of S-boxes used by a characteristic in any 3 consecutive rounds is $\lambda + 3$. Therefore,

$$p_{\Omega_3}^{max} = (p_\delta)^{\lambda+3}. \tag{14}$$

Combining (12), (13), and (14) results in (11) and the theorem is proven. □

From Theorem 1 we see that S-boxes satisfying a high diffusion order can be used to decrease the upper bound on characteristic probabilities and thereby strengthen a network against differential cryptanalysis. One obvious approach to generate such S-boxes would be to randomly select an $n \times n$ bijective mapping and discard those which do not satisfy the appropriate property. Unfortunately, we have found experimentally that S-boxes which satisfy diffusion orders of $\lambda \geq 1$ are extremely rare and cannot generally be found by random search.

In Figure 2, we present an algorithm to select the S-box output values using a depth-first-search approach as an efficient method of generating S-boxes that satisfy a particular diffusion order. In the algorithm of Figure 2, we use the variables i and $S(i)$ to represent, in decimal form, the S-box input and corresponding output, respectively. As well, $rand(\cdot)$ represents the random selection of an element from the specified set.

There are limitations to the applicability of the depth-first-search algorithm. For example, while the algorithm successfully found many 8×8 S-boxes which satisfied diffusion orders of $\lambda = 1$ and $\lambda = 2$, it could not successfully find S-boxes with $\lambda \geq 3$. In the next section, we show that, although the algorithm is designed to find S-boxes that satisfy a particular diffusion order, it is also valuable in generating S-boxes which are cryptographically strong in other respects.

```
$\Gamma = \{0, 1, 2, ..., 2^n - 1\}$
$\Lambda_0 = \Gamma$
$i = 0$
$do$
    $if\ (\Lambda_i \neq \{\emptyset\})\ then$
        $S(i) = rand(\Lambda_i)$
        $\Lambda_i = \Lambda_i - \{S(i)\}$
        $if\ ((i, S(i))\ satisfy\ \lambda)\ then$
            $\Gamma = \Gamma - \{S(i)\}$
            $i = i + 1$
            $\Lambda_i = \Gamma$
        $endif$
    $else$
        $i = i - 1$
        $\Gamma = \Gamma + \{S(i)\}$
    $endif$
$while\ (i \leq 2^n - 1)$
$output:\ \ (i, S(i))\ for\ 0 \leq i \leq 2^n - 1$
$end$
```

Figure 2. Algorithm to Find S-boxes Satisfying Diffusion Order λ.

(b) Nonlinearity

An important cryptographic property for product ciphers is nonlinearity. Since the S-boxes are the only nonlinear components of an SPN, it is crucial to consider the amount of nonlinearity required in S-boxes to provide adequate overall SPN security. The linear cryptanalysis method of Matsui [6] is one basis for determining the amount of nonlinearity required in an S-box.

Consider an SPN in which the lowest nonlinearity of an S-box is NL_{min}, i.e., $NL(S) \geq NL_{min}$ for all S-boxes. Then the best linear approximation of an S-box occurs with probability p_ϵ where

$$|p_\epsilon - 1/2| = \frac{2^{n-1} - NL_{min}}{2^n}. \qquad (15)$$

Since there must be at least one S-box approximation included in the linear expression of equation (5) for each round, the best possible linear approximation has $\alpha = R$ and satisfies:

$$\begin{aligned} |p_L - 1/2| &\leq 2^{R-1}|p_\epsilon - 1/2|^R \\ &\leq 2^{R-1}\left[\frac{2^{n-1} - NL_{min}}{2^n}\right]^R. \end{aligned} \qquad (16)$$

λ	min NL	max NL	%NL=94	%NL=96	%NL=98
0	86	98*	38.5	23.5	5.5
1	86	96	48	26	0
2	36	96	34	2	0

*S-boxes with $NL(S) = 100$ have been found using a more thorough search.

Table 1. Nonlinearities of 8 × 8 S-boxes.

It is known that there are $n \times n$ bijective mappings for which $NL(S) \geq 2^{n-1} - 2^{n/2}$ [13]. Assuming that S-boxes are used that have $NL(S) = 2^{n-1} - 2^{n/2}$, combining (7) and (16) we see that the number of known plaintexts required to determine one bit of key is at least $2^{nR-2(R-1)}$. For example, if an 8–round SPN was constructed using 8 x 8 S-boxes with $NL(S) = 112$, it would take about 2^{50} known plaintexts to determine one key bit.

In [14], O'Connor shows that, as n gets larger, the expected distance of a randomly selected n-bit function (not necessarily balanced) from the nearest affine function increases and p_ϵ approaches the ideal value of 1/2. In view of this, we expect that, as n gets large, S-boxes with high nonlinearities will be plentiful and easy to find by random search.

In order to confirm this intuition, 200 8 × 8 bijective S-boxes (i.e., $\lambda = 0$) were randomly generated and their nonlinearities examined. As well, 50 S-boxes were constructed using the depth-first-search algorithm for the diffusion orders of $\lambda = 1$ and $\lambda = 2$. The results are given in Table 1. We surmise that, as the diffusion characteristics become more constraining, the S-box nonlinearities are adversely affected. However, for $\lambda = 0$, 1, or 2, it is still reasonable to expect to find S-boxes with high nonlinearities of 94 or 96.

IV. Linear Transformations Between Rounds

The permutations of an SPN belong to a specialized class of the set of linear transformations that may be used to achieve Shannon's diffusion effect. In this section, we consider another class of invertible linear transformations that may be used between rounds of S-boxes to increase the resistance to differential and linear cryptanalysis.

Let N be even and consider the class of invertible linear transformations defined by

$$\mathbf{V} = \pi(\mathcal{L}(\mathbf{U})) \qquad (17)$$

where $\mathbf{V} = [V_1\ V_2\ ...\ V_N]$ is the vector of input bits to a round of S-boxes, $\mathbf{U} = [U_1\ U_2\ ...\ U_N]$ is the vector of bits from the previous round output, $\pi \in \Pi$, and $\mathcal{L}(\mathbf{U}) = [L_1(\mathbf{U})\ ...\ L_N(\mathbf{U})]$. The set Π is defined to be the set of permutations for which no two outputs of an S-box are connected to one S-box in the next round and

$$L_i(\mathbf{U}) = U_1 \oplus \ldots \oplus U_{i-1} \oplus U_{i+1} \oplus \ldots \oplus U_N. \tag{18}$$

The linear transformation may be efficiently implemented by noting that each $L_i(\mathbf{U})$ can be simply determined by XORing U_i with the XOR sum of all U_j, $1 \le j \le N$, i.e.,

$$L_i(\mathbf{U}) = U_i \oplus Q \tag{19}$$

where

$$Q = \bigoplus_{j=1}^{N} U_j. \tag{20}$$

Theorem 2: Consider an SPN of R rounds of M S-boxes such that R is a multiple of 4 and $M \ge n$. Let $n \ge 3$ and each S-box satisfy diffusion order λ such that $\lambda \le (n-1)/2$. Using the linear transformation of equation (17), the probability of an $(R-1)$-round characteristic satisfies

$$p_{\Omega_{R-1}} \le (p_\delta)^{\frac{\lambda+2}{2}R-(\lambda+1)} \tag{21}$$

where p_δ represents the maximum S-box XOR pair probability. Further, for $\lambda = 0$, the characteristic probability can be more tightly bounded by

$$p_{\Omega_{R-1}} \le (p_\delta)^{\frac{3}{2}R-2}. \tag{22}$$

Note that for $\lambda = 0$ the linear transformation has decreased the upper bound on the characteristic probability and for $\lambda > 0$ the bound on the characteristic probability has remained unchanged.

Consider now the effects of the linear transformation on the applicability of linear cryptanalysis. Using the linear transformation ensures that there are a large number of S-box approximations included in the system linear approximation, thereby increasing the number of required plaintexts.

Theorem 3: Consider an SPN of R rounds of M S-boxes such that R is even and $M \ge n$. Using the linear transformation of equation (17), the best possible R-round linear approximation requires $\alpha = 3R/2$ S-box approximations and the probability of the linear approximation satisfies

$$|p_L - 1/2| \le 2^{\frac{3}{2}R-1}|p_\epsilon - 1/2|^{\frac{3}{2}R} \tag{23}$$

where p_ϵ represents the probability of the best S-box linear approximation.

Proof: We shall show in the proof that, using the linear transformation of equation (17), it is impossible to involve only one S-box per round in the linear approximation. Let the number of S-boxes from round i involved in the overall system linear approximation be represented by ψ_i. Consider round r to contribute only one S-box to the linear approximation, i.e., $\psi_r = 1$. The linear approximation of this S-box involves a linear combination of the input bits, $a_1X_1 \oplus a_2X_2 \oplus \ldots \oplus a_nX_n$, where $\mathbf{a} = [a_1 \ldots a_n]$, $a_i \in \{0,1\}$, and a linear combination of the output bits, $b_1Y_1 \oplus b_2Y_2 \oplus \ldots \oplus b_nY_n$, where $\mathbf{b} = [b_1 \ldots b_n]$, $b_i \in \{0,1\}$, so that the probability of

$$\bigoplus_{i=1}^{n} a_iX_i = \bigoplus_{i=1}^{n} b_iY_i \tag{24}$$

does not equal 1/2. (Note that the trivial case of $\mathbf{a} = \mathbf{0}$ and $\mathbf{b} = \mathbf{0}$ is of no use in linear cryptanalysis and is ignored.)

Without loss of generality, assume that the S-box included in the system linear approximation from round r is the first S-box so that $\mathbf{X} = [X_1\ X_2 \ldots X_n] = [V_1\ V_2 \ldots V_n]$ where V_i is the i-th input bit to round r. The input to round r is determined by the permutation π so that $V_i = L_{j_i}(\mathbf{U})$ where $\mathbf{U}$ is the vector of output bits from the S-boxes of round $r-1$. Subsequently, we have $X_i = U_{j_i} \oplus Q$ where Q is defined in equation (20) and each U_{j_i}, $1 \le i \le n$, comes from a different S-box (as a result of the definition of the permutation π). We now have

$$\begin{aligned} \bigoplus_{i=1}^{n} a_iX_i &= \bigoplus_{i=1}^{n} a_i \cdot (U_{j_i} \oplus Q) \\ &= \bigoplus_{i=1}^{n} a_iU_{j_i} \oplus \bigoplus_{i=1}^{n} a_iQ \\ &= \begin{cases} \bigoplus_{i=1}^{n} a_iU_{j_i} \oplus Q & , wt(\mathbf{a})\ odd \\ \bigoplus_{i=1}^{n} a_iU_{j_i} & , wt(\mathbf{a})\ even. \end{cases} \end{aligned} \tag{25}$$

Hence, if $wt(\mathbf{a})$ is odd, then the sum used for the input of the round r S-box is determined by $N - wt(\mathbf{a})$ outputs of round $r-1$ since a term is removed from Q when $a_i = 1$. If $wt(\mathbf{a})$ is even, then the sum used for the input of the round r S-box is determined by $wt(\mathbf{a})$ outputs of round $r-1$ since a term is only included in the summation when $a_i = 1$.

If, for example, $wt(\mathbf{a}) = 1$, then the corresponding S-box input bit used in the linear approximation is a function of $N-1$ output bits from round $r-1$ and, hence, $\psi_{r-1} = M$. If, however, $wt(\mathbf{a}) = 2$, then $\psi_{r-1} = 2$. Hence, considering other values for $wt(\mathbf{a})$, $1 \le wt(\mathbf{a}) \le n$, we may now conclude that given $\psi_r = 1$, $\psi_{r-1} \ge 2$.

A similar analysis may be used to determine a lower bound on the number of S-boxes included in the linear approximation from round $r+1$, ψ_{r+1}, given $\psi_r = 1$. This is possible due to the following easily verifiable observations: $\mathcal{L}^{-1} \equiv \mathcal{L}$, $\pi^{-1} \in \Pi$, and $\mathcal{L}(\pi(\cdot)) \equiv \pi(\mathcal{L}(\cdot))$. Hence, we have

$$\mathbf{U}^* = \pi^{-1}(\mathcal{L}(\mathbf{V}^*)) \tag{26}$$

where $\mathbf{U}^*$ is the vector of output bits of the round r substitutions and $\mathbf{V}^*$ is the vector of input bits to the round $r+1$ substitutions. Since (26) is of a similar form to (17), we may determine the bound for ψ_{r+1} analogously to the

TYPE	λ	$R = 8$		$R = 16$	
		N_D^{min}	N_L^{min}	N_D^{min}	N_L^{min}
Permutation $\pi(\cdot)$	0	2^{28}	2^{34}	2^{60}	2^{66}
	1	2^{40}		2^{88}	
	2	2^{52}		2^{116}	
Linear Transform $\pi(\mathcal{L}(\cdot))$	0	2^{40}	2^{50}	2^{88}	2^{98}
	1	2^{40}		2^{88}	
	2	2^{52}		2^{116}	

Table 2. Resistance to Cryptanalysis for Networks Using 8×8 S-boxes with $p_\delta = 2^{-4}$ and $NL_{min} = 96$.

bound for ψ_{r-1}. Hence, it follows that $\psi_{r+1} \geq 2$ given $\psi_r = 1$.

We conclude, therefore, that the number of S-boxes involved in the linear approximation from any 2 consecutive rounds must be at least 3 and for an R-round SPN, assuming R is even, $\alpha \geq 3R/2$. □

Note that results similar to Theorem 2 and Theorem 3 can be derived for $\mathcal{L}(\mathrm{U})$ defined as other invertible linear transformations where each $L_i(\mathrm{U})$ may contain fewer than the $N - 1$ terms of equation (18).

V. Summary of Results

In Table 2, for SPNs of 8 and 16 rounds, we have summarized lower bounds on the values of N_D and N_L (defined in equations (4) and (7), respectively). Both networks are assumed to be composed of 8×8 S-boxes where the maximum S-box XOR pair probability is $p_\delta = 2^{-4}$ and the minimum S-box nonlinearity is $NL_{min} = 96$. Results are presented for networks using permutations from the set Π and for networks using a linear transformation of the form of equation (17). Note that the analysis of Table 2 is equally applicable to the decryption as well as the encryption network. (This is important since the decryption network may also be attacked using either cryptanalysis method.)

VI. Conclusion

In this paper we have developed bounds on the probabilities of a differential characteristic and a linear approximation for substitution-permutation networks. It is important to note that the bounds are of interest, not because they give a provable lower bound on the complexity of the cryptanalysis, but because they suggest the level of difficulty required in implementing the attacks. For example, in a differential attack, the cryptanalyst typically identifies a high probability input difference to the last round by searching for high probability differential characteristics. Similarly, for linear cryptanalysis, a good linear approximation can be practically used by a cryptanalyst to determine which subsets of plaintext and ciphertext bits to examine in the attack.

The analysis presented in this paper suggests the following general design principles for substitution-permutation networks:

- large, randomly selected S-boxes are very likely to have high nonlinearity,
- S-boxes which have good diffusion properties increase the resistance to differential cryptanalysis, and
- the use of an appropriate linear transformation between rounds increases the resistance to linear cryptanalysis.

Consequently, with an appropriate selection of S-boxes and linear transformations between rounds of substitutions, security in relation to differential and linear cryptanalysis can be improved, resulting in an efficient implementation with fewer rounds required to provide adequate security.

References

[1] H. Feistel, "Cryptography and computer privacy," *Scientific American*, vol. 228, no. 5, pp. 15–23, 1973.

[2] H. Feistel, W. A. Notz, and J. L. Smith, "Some cryptographic techniques for machine-to-machine data communications," *Proceedings of the IEEE*, vol. 63, no. 11, pp. 1545–1554, 1975.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[4] "National Bureau of Standards - Data Encryption Standard," *Federal Information Processing Standard Publication 46*, 1977.

[5] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, 1991.

[6] M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology: Proceedings of EUROCRYPT '93*, Springer-Verlag, Berlin, pp. 386–397, 1994.

[7] K. Nyberg, "On the construction of highly nonlinear permutations," *Advances in Cryptology: Proceedings of EUROCRYPT '92*, Springer-Verlag, Berlin, pp. 92–98, 1992.

[8] E. Biham and A. Shamir, "Differential cryptanalysis of FEAL and N-Hash," *Advances in Cryptology: Proceedings of EUROCRYPT '91*, Springer-Verlag, Berlin, pp. 1–16, 1991.

[9] E. Biham and A. Shamir, "Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI, and Lucifer," *Advances in Cryptology: Proceedings of CRYPTO '91*, Springer-Verlag, Berlin, pp. 156–171, 1992.

[10] E. Biham and A. Shamir, "Differential cryptanalysis of the full 16–round DES," *Advances in Cryptology: Proceedings of CRYPTO '92*, Springer-Verlag, Berlin, pp. 487–496, 1993.

[11] L. J. O'Connor, "On the distribution of characteristics in bijective mappings," *Advances in Cryptology: Proceedings of EUROCRYPT '93*, Springer-Verlag, Berlin, pp. 360–370, 1994.

[12] E. F. Brickell, J. H. Moore, and M. R. Purtill, "Structures in the S-boxes of DES," *Advances in Cryptology: Proceedings of CRYPTO '86*, Springer-Verlag, Berlin, pp. 3–8, 1987.

[13] K. Nyberg, "Differentially uniform mappings for cryptography," *Advances in Cryptology: Proceedings of EUROCRYPT '93*, Springer-Verlag, Berlin, pp. 55–64, 1994.

[14] L. O'Connor, *An Analysis of Product Ciphers Based On the Properties of Boolean Functions.* PhD thesis, University of Waterloo, Canada, 1992.