Modelling Avalanche Characteristics of a Class of Substitution-Permutation Networks

A.M. Youssef and S.E. Tavares[1]

Abstract

A block cipher is considered to display good avalanche characteristics if one bit change in the plaintext input is expected to result in close to half the ciphertext output changing. Good avalanche characteristics are important to ensure that a cipher is not susceptible to statistical attacks, such as clustering attacks, and the strength of a block cipher's avalanche characteristics may be considered as a measure of the randomness of the ciphertext. Elsewhere, the authors have proposed a special class of Substitution Permutation Networks (SPNs) with the involution property. This class has the important practical advantage that the same network can be used to perform both the encryption and the decryption operations. In this paper, we develop an analytical model for the avalanche characteristics of this class of SPNs.

1. Introduction

Feistel [2] was the first to suggest that a basic substitution-permutation network (SPN) consisting of iterative rounds of nonlinear substitutions (s-boxes) connected by bit permutations was a simple, effective implementation of a private-key block cipher. The SPN structure is directly based on Shannon's principle of a mixing transformation using the concepts of "confusion" and "diffusion" [11]. Letting N represent the block size of a basic SPN consisting of R rounds of $n \times n$ s-boxes, a simple

[1] Department Of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, Canada, K7L 3N6

example of an SPN with $N = 16$, $n = 4$, and $R = 3$ is illustrated in Figure 1.

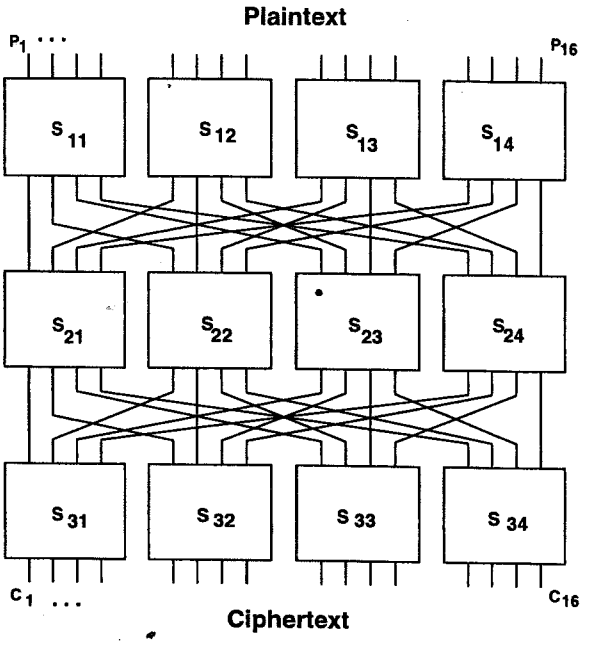

Figure 1: SPN with $N = 16$, $n = 4$, and $R = 3$.

One advantage of the basic SPN model is that it is a simple, yet elegant, structure for which it is generally possible to prove security properties such as completeness [7], and as shown in [5], resistance to differential cryptanalysis [1] and linear cryptanalysis [8].

The basic SPN architecture differs from a DES-like architecture in which the substitutions and permutations, used as a mixing transformation, operate on only half of the block at a time. Since SPNs do not have this last property, in general, SPNs need two different modules for the encryption and the decryption operations. In an SPN, decryption is performed by running the data backwards through the inverse network (i.e., applying the key scheduling algorithm in reverse and using the inverse s-boxes and the inverse permutation layer). In a DES-like cipher, the inverse s-boxes and inverse permutation are not required. Hence, a practical disadvantage of the basic SPN architecture compared with the DES-like architecture is that both the s-boxes and their inverses must be located in the same encryption hardware or software. The resulting extra memory or power consumption requirements may render this solution less attractive in some situations, especially for hardware implementations.

In [13], the authors introduced a special class of substitution-permutation networks. This class has the practical advantage that the same network can be used to perform both the encryption and the decryption operations.

In [6], the avalanche characteristics of basic SPNs are modelled and the effects of varying the cipher parameters are examined. In [3], Heys extended this work and developed a model of the avalanche characteristics of DES-like ciphers. In this paper, we develop an analytical model, supported with some experimental results, for the avalanche characteristics of the self-reciprocal class of SPNs described in [13]. It should be noted that while this paper deals with a topic that is closely related to [6], here we develop a new avalanche model for different SPNs and present the corresponding results. In particular, we consider a more efficient linear transformation layer that runs much faster both in software and in hardware and has improved bounds for the linear approximation and the differential characteristic.

An SPN is considered to display good avalanche characteristics if a one bit change in the plaintext input is expected to result in close to half the ciphertext bits changing. Good avalanche characteristics are important to ensure that a cipher is not susceptible to statistical attacks such as clustering attacks [4]. More formally, the avalanche is defined as follows :

Definition 1: [2]

A cipher is said to satisfy the avalanche criterion if , for each key, on average half the ciphertext bits change when one plaintext bit is changed.

That is, $E(wt(\triangle \mathbf{C}) \mid wt(\triangle \mathbf{P}) = 1) = N/2$, where $wt(\cdot)$ denotes the hamming weight of the enclosed argument, $\triangle \mathbf{C}$ and $\triangle \mathbf{P}$ denote the ciphertext and the plaintext change vectors, respectively.

An extension to the above definition was proposed by Webster and Tavares [12] and is referred to as the Strict Avalanche Criterion (SAC).

Definition 2: [12]

A cipher is said to satisfy the SAC if, for each key, each ciphertext bit changes with a probability of $1/2$ when a single plaintext bit is changed. That is $P(\triangle C_i = 1 \mid wt(\triangle \mathbf{P}) = 1) = 1/2$ where C_i denotes the i^{th} ciphertext bit, $1 \leq i \leq N$.

It is clear that a network satisfying the SAC must satisfy the avalanche criterion. Satisfaction of the avalanche criterion does not necessarily imply satisfaction of the SAC.

While most SPNs, if treated as randomly selected boolean functions, are expected not to satisfy the SAC [9], most of the SPNs will satisfy the avalanche criterion after sufficiently many rounds. Also, there is no design procedure, to the authors' knowledge, that guarantees that the resulting SPN satisfies the SAC.

It is worth noting that while both the avalanche criterion and the SAC were originally defined for block ciphers, they can be extended, in a natural way, to stream ciphers. For example, one can say that a stream cipher satisfies the SAC if, for all seeds, flipping one bit in the seed results in a key stream that is statistically independent of the original one.

2. SPNs with the Involution Property

It is possible to construct SPNs which do not require inverse s-boxes if the s-boxes in the network belong to the class of functions that we refer to as semi-involution functions. Such functions have the property that their inverses can be easily obtained by a simple XOR operation on the function input and output. Hence, differences between the s-boxes in the encryption network and the decryption network can be accommodated by incorporating the XOR into the application of the round key bits.

A bijective function $\pi : Z_2^n \rightarrow Z_2^n$ is called a semi-involution function if

$$\pi^{-1}(X) = \pi(X \oplus a) \oplus b \tag{1}$$

for some constants $a, b \in Z_2^n$. In [13], the authors discuss different cryptographic properties of this class of functions, such as nonlinearity and the maximum XOR table entry.

In order to use the same SPN to perform both the encryption and the decryption operations, the s-box inter-connection layer should also be an involution mapping. In [5], [13] the authors show that replacing the permutation between rounds by an appropriate linear transformation is effective in improving the cipher security with regard to both linear [8] and differential cryptanalysis [1].

In [13], the authors show that with the use of an efficient involution linear transformation layer, this class of self-reciprocal SPNs is resistant to both the basic linear cryptanalysis [8] and to the differential cryptanalysis [1] based on the best $(R-1)$-round characteristic.

2.1 Modelling Avalanche in Substitution Boxes

The substitution boxes (s-boxes) used in the network belong to the class of semi-involution functions [13]. However, modelling the avalanche properties of such s-boxes is a hard combinatorial problem. Fortunately, experimental results show that the SPN will have the same avalanche properties as an SPN that uses randomly selected bijective s-boxes.

Let the s-boxes in the network be defined by a bijective mapping $S : X \rightarrow Y$. Assume that any set of one or more input bit changes to an s-box results in a number of output bit changes represented by the random variable D, i.e., $D = wt(\triangle Y)$ where $\triangle Y$ is the output change vector of the s-box. We assume the likelihood of a particular nonzero value for D is given by assuming that all possible values of $\triangle Y$ belonging to the set of $2^n - 1$ nonzero changes are equally likely. Hence the probability

distribution of D is given by

$$P_D(D=0) = \begin{cases} 1 & , wt(\Delta X) = 0 \\ 0 & , wt(\Delta X) \geq 1 \end{cases} \tag{2}$$

and

$$P_D(D=d) = \begin{cases} 0 & , wt(\Delta X) = 0 \\ \frac{\binom{n}{d}}{2^n - 1} & , wt(\Delta X) \geq 1 \end{cases} \tag{3}$$

for $1 \leq d \leq n$. Note that the above s-box model essentially represents an average over all randomly selected s-boxes and is not intended to characterize the behavior of an actual physically realizable s-box. However, as experimental evidence suggests, modelling the number of output changes of each s-box as a random variable is a suitable approximation when considering an SPN constructed using randomly selected fixed semi-involution s-boxes.

2.2 Interconnection Layer

In order to use the same SPN to perform both the encryption and the decryption operations, the s-box inter-connection layer should also be an involution mapping. One interconnection layer with nice cryptographic properties is the linear transformation described by [13]

$$z(i) = \bigoplus_{l=1, l \neq i}^{M} w(l), \quad 1 \leq i \leq M \tag{4}$$

where $z(i)$ represents the i^{th} n-bit output word of the transformation, $w(i)$ is the i^{th} input word, $M = \frac{N}{n}$ denotes the number of s-boxes, and $\oplus$ denotes a bit-wise XOR operation. It is assumed that M is even so that the linear transformation is invertible. For 8×8 s-boxes this is a byte oriented operation. The linear transformation described above may be efficiently implemented by noting that each $z(i)$ could be simply determined by XORing $w(i)$ with the XOR sum of all $z(j)$, $1 \leq j \leq M$, i.e.,

$$z(i) = Q \oplus w(i), \tag{5}$$

where

$$Q = \bigoplus_{l=1}^{M} w(l). \tag{6}$$

Remark: The above class of linear transformations can be generalized further as follows:

$$z(i) = \bigoplus_{l=1}^{k} w(i \boxplus l), \quad 3 \leq k \leq M-1, k \; is \; odd. \tag{7}$$

where $z(i)$ represents the i^{th} output word of the transformation, $w(i)$ is the i^{th} input word and $\boxplus$ denotes addition mod M. The fact that k is odd ensures that the transformation is invertible for even M. While smaller values of k might be attractive for fast hardware implementations, only the case $k = M$ is an involution mapping and our theoretical avalanche model is concerned with this case only.

3. Modelling Avalanche

Let W_r represent the random variable corresponding to the number of bit changes after round r given one bit plaintext change, *i.e.*,

$$W_r = \sum_{s=1}^{M} wt(\triangle Y_{rs}) \tag{8}$$

where $\triangle Y_{rs}$ denotes the output change vector of the s^{th} s-box in round r. Hence, the expected value of W_r is given by

$$E(W_r) = \sum_{a=1}^{M} \frac{2^{n-1}na}{(2^n-1)} P(l_r = a) \tag{9}$$

where $P(l_r = a)$ denotes the probability of having a active s-boxes in round r, i.e., a s-boxes with nonzero input change vectors. From the total probability theory, we have

$$P(l_r = a) = \sum_{b=0}^{M} P(l_r = a | l_{r-1} = b)\, P(l_{r-1} = b). \tag{10}$$

with the initial conditions

$$p(l_1 = b) = \begin{cases} 1, & b = 1 \\ 0, & otherwise. \end{cases} \tag{11}$$

Now our problem is reduced to calculating the conditional probability $P(l_r = a | l_{r-1} = b)$, i.e., the probability of having a active s-boxes in round r given that we have b active s-boxes in round $r-1$. This is equivalent to calculating $P(t_y = a \mid t_x = b)$ in the following problem:

Let $Y = AX$ where $Y^t = (Y_1, Y_2, ..., Y_m), Y_i \in \mathrm{Z}_2^n$, $X^t = (X_1, X_2, ..., X_m), X_i \in \mathrm{Z}_2^n$ and A is an $m \times m$ matrix in which all elements are ones except the diagonal elements are all zeroes. Let $t_y = \#\{i \mid Y_i \neq \mathbf{0}\}$, $t_x = \#\{i \mid X_i \neq \mathbf{0}\}$, and $0 \leq i \leq m$. The probability $P(t_y = a \mid t_x = b)$ could be computed by examining all possible values of X. However, for most SPNs of practical size, this is very computationally intensive since there are $2^{n \times m}$ possible values of X. Lemmas 1 and 2 below show how this probability can be efficiently calculated.

Lemma 1

Let $\Psi(n, k)$ be the number of choices of k nonzero elements of Z_2^n which sum to zero, then

$$\Psi(n,k) = (-1)^k + \sum_{r=0}^{k-1} (-1)^r \binom{k}{r} 2^{n(k-r-1)} \tag{12}$$

Proof: Let $\Omega(n, k, r)$ denote the number of ways to choose k elements of Z_2^n which sum to zero such that r or more of them are zero. Thus

$$\Omega(n,k,r) = \begin{cases} \binom{k}{r} 2^{n(k-r-1)} & , 0 \leq r < k \\ 1 & , r = k. \end{cases} \tag{13}$$

Using the inclusion exclusion principle [10], we have

$$\Psi(n,k) = \sum_{r=0}^{k} (-1)^r \Omega(n,k,r) \tag{14}$$

which proves the Lemma □

Lemma 2

$$P\{t_y = a \mid t_x = b\} = (\Phi_1 + \Phi_2)/(2^n - 1)^b \tag{15}$$

where

$$\Phi_1 = \Psi(n,b)\delta(a=b)\ , \tag{16}$$

and

$$\Phi_2 = \Psi\Big(n-1, a+b-m\Big)\binom{b}{m-a}(2^n-1)\Big(2^{a+b-m-1} + \frac{1}{2}(-1)^{b-1}\delta(a+b=m)\Big). \tag{17}$$

Proof: Since any choice which b x's are nonzero is equally likely we may assume the first b are nonzero. Thus the last $(m-b)$ y's are all the same. Φ_1 counts the number of ways this could give rise to the last $(m-b)$ y 's being zero. If the last $(m-b)$ y's are not zero then we are basically reduced to considering the first b y's and basically we need to compute $p(t_y = a+b-m | t_x = b)$ for $m = b$. In this case we have $\binom{b}{m-a}$ ways to choose which $(m-a)$ of the remaining b y's should be zero. These must correspond to equal values of x and we have (2^n-1) ways to choose which value they have. Call this value w and split Z_2^n as $< w > + \mathrm{Z}_2^{n-1}$. The remaining x's cannot be $\mathbf{0}$ or w so they must have nonzero projection on Z_2^{n-1} which add to $\mathbf{0}$. Finally the projections of the remaining x's on $< w >$ must add to $(b-1)w$. There are 2^{a+b-m} choices for the projections onto $< w >$ and if $a+b \neq m$ then exactly half of these will have the correct sum. If $a+b=m$ the sum will always be $\mathbf{0}$ which is only correct if b is odd. Thus we have $2^{a+b-m-1} + \frac{1}{2}(-1)^{b-1}\delta(a+b=m)$ ways to choose the remaining x's. The conditional probability is obtained by dividing by the total number, $(2^n-1)^b$, of nonzero x's .

□

By numerical substitution in the formula above, one can show that the for a 64-bit SPN with $M = n = 8$, the expected number of bit changes after the third round is given by $32 - 2^{-35}$ which implies that the SPN avalanche characteristics are almost ideal after three rounds.

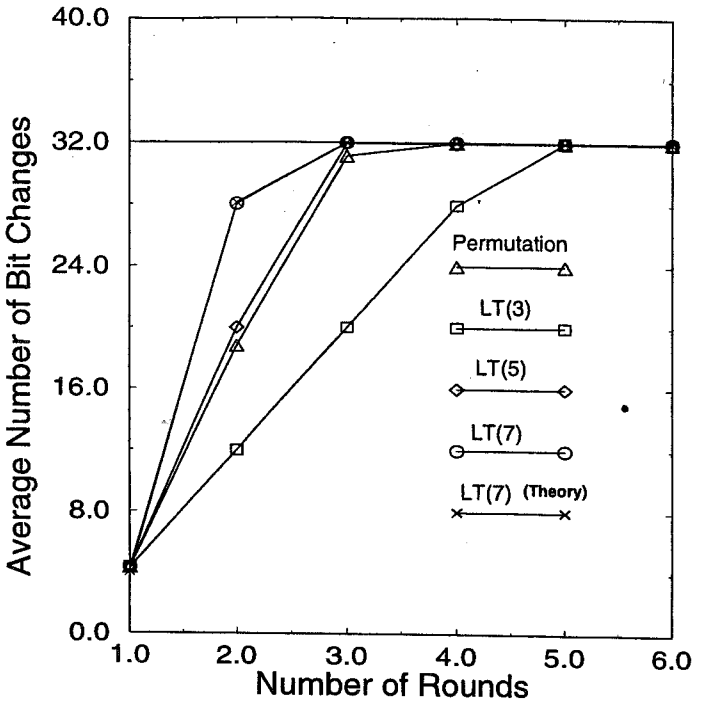

Figure 2 : Average Number of Bit Changes Versus the Number of Rounds for a *64*–bit SPN

Figure 2 shows the experimental results for the average number of output bit changes as a function of the number of rounds for a 64-bit SPN with permutation layers or linear transformation layers. One thousand random chosen input pairs, different in one randomly selected bit, were used to obtain the result. The SPN used for the experiments employed 8×8 random involution s-boxes, nonlinearity of 96, maximum XOR table entry of 10. The permutation layer used in the experiment is described by: output bit i of s-box j at round r is connected to input bit j of s-box i at round $r+1$. In Figure 2, $LT(k)$ denotes a linear transformation in equation (7) with parameter k. Figure 2 also shows the expected value estimated from our model. Both the theoretical and experimental curves overlap, which confirms the accuracy of the model. They also show that the appropriate linear transformation significantly improves the avalanche characteristics of the cipher after a small number of rounds. Experimental results also show that, after four rounds and for different inter-connection layers, the probability distributions of the number of bit changes are almost indistinguishable. They all follow closely a binomial distribution with mean ≈ 32 and variance ≈ 4.

4. Conclusion

We have presented an analytical model for the avalanche characteristics of a new class of substitution-permutation network. The results indicate that networks using a diffusive linear transformation between rounds achieves good avalanche characteristics in fewer rounds. Moreover, the result shows that, for a *64*–bit SPN using 8×8 s-boxes, the avalanche characteristics are almost ideal after three rounds.

Acknowledgments

The authors are grateful to Dr. R. Stong and Dr. D. Gregory for providing two different proofs for Lemma 2.

References

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

[2] H. Feistel. Cryptography and computer privacy. *Scientific American, 228, pp. 15–23*, 1973.

[3] H.M. Heys. Modelling avalanche characteristics in DES-like ciphers. *Workshop on Selected Areas in Cryptography, SAC '96, Workshop Record, pp.77–94*, 1996.

[4] H.M. Heys and S.E. Tavares. Key clustering in substitution-permutation network cryptosystems. *Workshop on Selected Areas in Cryptography, SAC '94, Workshop Record, pp.134–145*, 1994.

[5] H.M. Heys and S.E. Tavares. The design of product ciphers resistant to differential and linear cryptanalysis. *Journal of Cryptology, Vol. 9, no. 1, pp. 1–19*, 1996.

[6] H.M. Heys and S.E. Tavares. Avalanche characteristics of substitution-permutation encryption networks. *IEEE Trans. Comp., Vol. 44, pp.1131–1139*, Sept. 1995.

[7] J.B. Kam and G.I. Davida. Structured design of substitution-permutation encryption networks. *IEEE Trans. Comp. C-28, pp.747–753*, 1979.

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

[9] L.J. O'Connor. An upper bound on the number of functions satisfying the Strict Avalanche Criterion. *Information Processing Letters, 52, pp.325–327*, 1994.

[10]F.S. Roberts. *Applied Combinatorics*. Englewood Cliffs, N.J.: Prentice-Hall, 1984.

[11]C.E. Shannon. Communication theory of secrecy systems. *Bell Systems Technical Journal, Vol.28, pp. 656–715*, 1949.

[12]A.F. Webster and S.E. Tavares. On the design of S-boxes. *Advances in Cryptology : Proc. of CRYPTO '85 , Springer-Verlag, pp. 523–534*, 1986.

[13]A.M. Youssef, S.E. Tavares, and H.M. Heys. A new class of substitution-permutation networks. Technical report, Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, December, 1995.