Modelling Avalanche Characteristics of Substitution-Permutation Networks Using Markov Chains

A. M. Youssef and S.E. Tavares
Department Of Electrical and Computer Engineering
Queen's University, Kingston, Ontario, Canada, K7L 3N6
E-mail: tavares@ee.queensu.ca
http://adonis.ee.queensu.ca:8000

Abstract— In this paper we develop an analytical model for the avalanche characteristics of Substitution Permutation encryption Networks (SPNs) with randomly generated substitution boxes (s-boxes) . We consider three general network models, distinguished by their linear interconnection layers. We show that, for the purpose of modelling the avalanche characteristics, the number of active s-boxes (i.e., s-boxes with output changes) at each round can be modelled by an ergodic Markov chain. Our results show that the transition matrices for SPNs with a permutation layer have the slowest convergence, and the transition matrices for SPNs with a wordwise linear transformation layer have the fastest convergence. This implies that the appropriate linear transformation can be used to facilitate the construction of efficient ciphers with fewer rounds.

1. Introduction

Feistel [2] was the first to suggest that a basic substitution-permutation network (SPN) consisting of 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" [10]. Heys and Tavares [6] noted that the permutation layer of an SPN can be considered as a specialized class of the set of linear transformations that may be used to achieve Shannon's diffusion effect. They also showed that another class of invertible linear transformations may be used between rounds of s-boxes to increase the SPN's resistance to differential cryptanalysis [1] and linear cryptanalysis [9]. Letting N represent the block size of an SPN consisting of R rounds of $n \times n$ s-boxes, a simple example of an SPN with $N = 16$, $n = 4$, and $R = 3$ is illustrated in Figure 1. Keying the network is accomplished by XORing the key bits with the data bits before each round of substitution and after the last round.

One advantage of the SPN model is that it is a simple, yet elegant, structure for which it is generally possible to prove security properties such as completeness [8], and as shown in [6], resistance to differential cryptanalysis [1] and linear cryptanalysis [9].

An SPN is considered to display good avalanche characteristics if a one bit change in the plaintext input is expected to cause close to half the ciphertext bits to change. Good avalanche characteristics are important to ensure that a cipher is not susceptible to statistical attacks such as clustering attacks [5]. More formally, the avalanche is defined as follows :

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

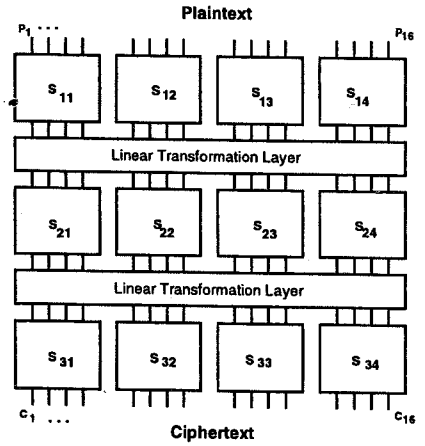

Figure 1: SPN with $N = 16$, $n = 4$, and $R = 3$.

In [7], Heys and Tavares analyzed the avalanche characteristics of SPNs based on two general network models, distinguished by the nature of their permutation layer. In the first model, they considered a network where the permutation between two rounds is modelled as a random variable whose values are equally likely. In the second model, they considered a network which has a specified fixed permutation between rounds. In [4], Heys extended this work and developed a model of the avalanche characteristics of DES-like ciphers.

In this paper we develop analytical models for the avalanche characteristics of other classes of SPNs. In particular, we consider the following three general network models, distinguished by their linear transformation layers:

Model A — In this model we consider SPNs, with $M = n$, in which the interconnection layer is a permutation layer $\pi \in \Omega$, where Ω 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.

Model B — In this model we consider SPNs in which the interconnection layer is given by the invertible bitwise linear transformation defined by $\mathbf{V} = \pi(\mathcal{L}(\mathbf{U}))$ where $\mathbf{V} = [V_1 V_2 \cdots V_N]$ is the vector of input bits to a round of s-boxes, $\mathbf{U} = [U_1 U_2 \cdots U_N]$ is the vector of bits from the previous round output, $\mathcal{L}(\mathbf{U}) = [L_1(\mathbf{U}) \cdots L_N(\mathbf{U})]$, $\pi \in \Omega$, where Ω is the set of permutations defined in model A, and

$$L_i(\mathbf{U}) = \bigoplus_{l \neq i} U_l.$$

N is assumed to be even so that the linear transformation is invertible.

Model C— In this model we consider SPNs in which the interconnection layer is given by the invertible wordwise linear transformation defined by

$$\mathbf{Z}_i = \bigoplus_{l=1, l \neq i}^{M} \mathbf{W}_l, \quad 1 \leq i \leq M,$$

where $\mathbf{Z}_i$ represents the i^{th} n-bit output word of the transformation, $\mathbf{W}_i$ is the i^{th} input word, and $M = \frac{N}{n}$ denotes the number of s-boxes. 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 resistance of SPNs, described by the above three models, against linear and differential cryptanalysis is studied in [6][12].

2. Convergence in Markov Chains

A Markov chain is ergodic if it is finite, aperiodic and irreducible. A sufficient condition for a Markov chain with n states and a state transition matrix, P, to be aperiodic is that $P[i,i] > 0$ for some $i, 1 \leq i \leq n$, and it is irreducible if for all i, j there exists r such that $P^r[i,j] > 0, 1 \leq i, j \leq n$.

If P is ergodic, then there exists a unique distribution $\Pi = (\pi_1, \pi_2, \cdots, \pi_n)$ such that

$$\pi_j = \lim_{r \to \infty} P^r[i,j].$$

The distribution Π is said to be the limiting distribution of P. The classical method to determine the rate of convergence towards this limiting distribution is to consider the eigenvalues of P [3].

Suppose that we have a matrix P with distinct and non-zero eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_n$. Let the column vector $\mathbf{x}^{(i)} = \left(x_1^{(i)}, x_2^{(i)}, \cdots, x_n^{(i)}\right)^T$ satisfy

$$P\mathbf{x}^{(i)} = \lambda_i \mathbf{x}^{(i)},$$

and the row vector $\mathbf{y}^{(i)} = \left(y_1^{(i)}, y_2^{(i)}, \cdots, y_n^{(i)}\right)$ satisfy

$$\mathbf{y}^{(i)} P = \lambda_i \mathbf{y}^{(i)},$$

for $i = 1, 2, \cdots, n$. Then

$$P^r = \sum_{i=1}^{n} \lambda_i^r B_{(i)}, \qquad B_{(i)}[j,k] = \frac{x_j^{(i)} y_k^{(i)}}{\mathbf{x}^{(i)} \cdot \mathbf{y}^{(i)}}.$$

It follows that a matrix P with distinct eigenvalues has a limiting distribution if and only if the largest eigenvalue is 1, and the remaining eigenvalues are less than one in modulus. We order the eigenvalues with $1 = \lambda_1 \geq |\lambda_2| \geq |\lambda_3| \geq \cdots \geq |\lambda_n|$.

Powers of a transition matrix can be written as

$$P^r = \sum_{i=1}^{m} \lambda_i^r B_{(i)} = P^* + \sum_{i=2}^{m} \lambda_i^r B_{(i)},$$

where $P^* = [\Pi, \Pi, \cdots, \Pi]^T$, Π is the limiting distribution of P. Thus all entries of P^r converge to their limit exponentially fast as a function of λ_2.

3. Modelling Avalanche in S-boxes

We will use the same s-box model proposed in [7]. Let the s-boxes in the network be defined by a bijective mapping $S : \mathbf{X} \to \mathbf{Y}$. 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., $D = wt(\Delta\mathbf{Y})$ where $\Delta\mathbf{Y}$ is the output change vector of the s-box. We assume that the likelihood of a particular nonzero value for D is given by assuming that all possible values of $\Delta\mathbf{Y}$ belonging to the set of $2^n - 1$ nonzero changes are equally likely. Hence the probability distribution of D is given by

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

and

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

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 bijective s-boxes.

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

$$W_r = \sum_{s=1}^{M} wt(\Delta\mathbf{Y}_{rs}),$$

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

$$E(W_r) = \sum_{i=1}^{M} E(D) i P_{A_r}(A_r = i) = \frac{2^{n-1}n}{(2^n-1)} \sum_{i=1}^{M} i P_{A_r}(A_r = i),$$

where $P_{A_r}(A_r = i)$ denotes the probability of having i active s-boxes in round r, i.e., i s-boxes with nonzero input change vectors.

Thus we have

$$P_{A_r}(A_r = i) = \sum_{j=0}^{M} P_{A_r}(A_r = i | A_{r-1} = j)\, P_{A_{r-1}}(A_{r-1} = j),$$

with the initial condition

$$p_{A_1}(A_1 = j) = \delta(j = 1),$$

where $\delta(a = b) = 1$ if $a = b$ and $\delta(a = b) = 0$ if $a \neq b$.

It is clear that $P_{A_r}(A_r = i | A_{r-1} = j)$ does not depend on r and hence the number of active s-boxes can be modelled by a Markov chain. Now our problem is reduced to calculating the state transition matrix $P = [P_{ji}]$, where $P_{ji} = P_{A_r}(A_r = i | A_{r-1} = j)$ is the probability of having i active s-box in round r given that we have j active s-box in round $r-1$.

4. Modelling the Linear Interconnection Layer

A more complete discussion and proofs of the results below can be found in [11].

4.1 Model A: Fixed Permutation Layer $\pi \in \Omega$

Lemma 1 Assume an SPN with a fixed permutation layer $\pi \in \Omega$ then we have

$$P_{ji} = \frac{1}{(2^n-1)^j} \sum_{l=n-i}^{n} (-1)^{l-n+i} \binom{l}{n-i} \binom{n}{l} \left(2^{n-l}-1\right)^j.$$

4.2 Model B: Linear Transformation Type 1

Lemma 2 Assume an SPN with a linear transformation of type 1. Let $Q = \bigoplus_{j=1}^{N} U_j$, then for $\Delta Q = 0$, the number of arrangements for the output bit changes such that we have i active s-boxes in round r given that we have j active s-box in round $r-1$ is given by

$$A_0(i,j) = \sum_{l=M-i}^{M-1} (-1)^{l-M+i} \binom{l}{M-i} \binom{M}{l} \left(2^{n-l}-1\right)^j \Phi\left(j, \frac{1/2}{1-2^{l-n}}\right),$$

where

$$\Phi(l,p) = \begin{cases} \sum_{i=0}^{\lceil l/2 \rceil} \binom{l}{2i} p^{2i}(1-p)^{l-2i} & 0 < p < 1, \\ 1 & p = 0, \\ \begin{cases} 1, & l \text{ even} \\ 0, & l \text{ odd} \end{cases} & p = 1. \end{cases}$$

Lemma 3 Assume an SPN with a linear transformation of type 1. Let $Q = \bigoplus_{j=1}^{N} U_j$, then for $\Delta Q = 1$, the number of arrangements for the output bit changes such that we have i active s-box in round r given that we have j active s-box in round $r-1$ is given by

$$A_1(i,j) = \begin{cases} N_{A_1}((M-i), M), & j = M, \\ (2^n-1)^j \left(1 - \Phi\left(j, \frac{1/2}{1-2^{-n}}\right)\right), & j \neq M, i = M, \\ 0, & otherwise, \end{cases}$$

where

$$N_{A_1}(i, M) = \sum_{l=i}^{M-1} (-1)^{l-i} \binom{l}{i} \binom{M}{l} \Psi(l),$$

and

$$\Psi(l) = \begin{cases} \frac{(2^{n-l})^M}{2}, & l \neq 0, \\ (2^n-1)^M \left(1 - \Phi\left(M, \frac{1/2}{1-2^{-n}}\right)\right), & l = 0. \end{cases}$$

Combining the results above, we have

$$P_{ji} = \frac{A_0(i,j) + A_1(i,j)}{(2^n-1)^j}.$$

4.3 Model C: Linear Transformation Type 2

Lemma 4 Assume an SPN with a linear transformation of type 2. Let $\mathbf{Q} = \bigoplus_{l=1}^{M} \mathbf{W}_l$. then we have

$$P_{ji} = (\Phi_1 + \Phi_2)/(2^n-1)^j$$

where

$$\Phi_1 = \Psi(n,j)\delta(i=j),$$

$$\Phi_2 = \Psi(n-1, i+j-M) \binom{j}{M-i} (2^n-1) \times \left(2^{i+j-M-1} + \frac{1}{2}(-1)^{j-1}\delta(i+j=M)\right),$$

and

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

5. Discussion and Conclusion

For $N = 64$ and $M = n = 8$ (a practical size of SPN) the transition matrices for SPNs based on the three models

above were calculated and checked for the ergodic property [11]. The limiting distribution and the eigenvalues of these matrices is also given in [11]. Let

$$\epsilon = \lim_{r \to \infty} |E(W_r) - N/2|,$$

i.e., ϵ denotes the deviation of the limiting avalanche characteristics from the ideal characteristics. For such SPNs, $\epsilon < 2^{-44}$ for the three models above. Table 1 shows the value of the second largest eigenvalue for the three models.

	Model A	Model B	Model C
λ_2	3.185×10^{-2}	4.439×10^{-3}	3.922×10^{-3}

Table 1 : The Second Largest Eigenvalues for SPNs with $N = 64, M = n = 8$.

From Table 1, it is clear that the transition matrices for SPNs with a permutation layer have the slowest convergence (largest second eigenvalue), and the transition matrices for SPNs with a wordwise linear transformation layer have the fastest convergence (smallest second eigenvalue). It is also clear that the linear transformation is effective in improving the avalanche characteristics of SPNs. Figure 2 shows how the experimental results agrees with our theoretical model for SPNs with $N = 64$, $n = M = 8$.

Figure 2 : Theoretical and Experimental Avalanche for SPN with $N = 64$, $n = M = 8$.

While the s-box model used throughout this paper is suitable for studying the avalanche characteristics of SPNs, it can not be used to determine the resistance of the network to differential cryptanalysis, where the analysis should be performed on a specified set of s-boxes. However, from the transition matrix, we can calculate the minimum number of s-boxes involved in any 2 rounds of a differential characteristic. This number will be greater than or equal to $2, 3, 4$ for model A, B and C, respectively. These numbers are independent of n, N for even $M \geq 4$ and they can be used to obtain a lower bound on the number of chosen plaintext-ciphertext pairs required for the differential cryptanalysis based on the best $(R-1)$-round characteristic [6],[12].

In summary, we have presented analytical models for the avalanche characteristics of three general classes of substitution-permutation encryption networks. The results show that using an appropriate diffusive linear transformation between rounds can improve the avalanche characteristics of the network. This facilitates the construction of efficient ciphers with fewer rounds.

Acknowledgments

The authors are grateful to Dr. R. Stong and Dr. D. Gregory for providing two different proofs for Lemma 4.

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] W. Feller. *An Introduction to Probability Theory with Applications, Vol. I, 3rd edition.* John Wiley and Sons, New York, 1968.

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

[5] 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.

[6] 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.

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

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

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

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

[11] A.M. Youssef and S.E. Tavares. Modelling avalanche characteristics of substitution-permutation networks using markov chains. Technical report, Department of Electrical and Computer Engineering, Queen's University, Kingston, Ontario, September, 1996.

[12] A.M. Youssef, S.E. Tavares, and H.M. Heys. A new class of substitution-permutation networks. *Workshop on Selected Areas in Cryptography, SAC '96, Workshop Record, pp.132–147*, 1996.