Differential-like Cryptanalysis of a Class of Substitution-Permutation Networks

Z.G. Chen, A.M. Youssef and S.E. Tavares
Department of Electrical and Computer Engineering
Queen's University at Kingston, Ontario, Canada, K7L 3N6
E-mail: {chenz, amr_y, tavares}@ee.queensu.ca
http://adonis.ee.queensu.ca:8000

Abstract

We introduce a practical differential-like attack on a class of Substitution-Permutation Networks (SPNs). Our attack is effective regardless of the key-scheduling algorithm and more efficient than classical differential cryptanalysis. In addition, it is shown that 64-bit SPNs with 8×8 s-boxes are resistant to our attack after 12 rounds.

1 Introduction

The substitution-permutation encryption network (SPN) was first suggested by Feistel [2] as a simple, effective implementation of a private-key block cipher based on the concept of "confusion" and "diffusion" introduced by Shannon [9]. An SPN is constructed by a number of rounds of nonlinear substitutions (s-boxes) followed by bit permutations. Keying the network can be accomplished by XORing the key bits with the data bits before each round of substitutions and after the last round. The key bits associated with each round are derived from the master key according to the key-scheduling algorithm. An example of a small SPN with N=16, m=n=4 and R=3 is illustrated in Figure 1 where N represents the block size of the SPN consisting of R rounds of $n \times n$ s-boxes and m is the number of s-boxes in each round.

Differential cryptanalysis is one of the most powerful attacks on private-key ciphers such as DES [1]. It exploits a highly probable differential [5] and a large amount of chosen plaintext to sift out the correct key. However, its application to SPNs is based on the best characteristic instead of the best differential [6]. Heys and Tavares [4] derived upper bounds on the most likely differential characteristic as a function of the maximum XOR value and the number of active s-boxes (i.e., the s-boxes whose inputs change in the process of encrypting two plaintexts).

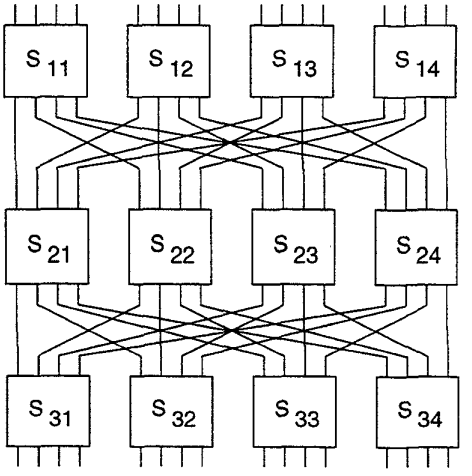

Figure 1: SPN with N=16, m=n=4 and R=3

In this paper, we present a new differential-like attack on the class of SPNs with $m = n$. By modelling the number of active s-boxes in the network using Markov chains [11] we may predict the number of active s-boxes in the second round provided that we make one s-box in the first round (the target s-box) active and know the number of active s-boxes in the last round.

0-7803-4314-X/98/$10.00

This enables us to determine the subkeys of the first round and the subsequent rounds can be attacked similarly.

2 Motivation

Our attack originates from the observation of the avalanche effect (or avalanche characteristic) of SPNs. An SPN is said to have good avalanche effect if on average, a one bit change in the plaintext causes about half of the ciphertext bits to change. When we talk about change and difference, we refer to the XOR operation. A cipher without good avalanche effect is susceptible to certain statistical attacks according to [3]. In fact, our differential-like attack suggests that even a slight deviation will result in a weak cipher. Figure 2 shows two examples of avalanche effect by counting the frequencies of ciphertext bit changes based on 10^7 samples for SPNs with $M = 64, m = n = 8$, $R = 4$ and $R = 5$ respectively. The effect can be explained by the following Markov model (See [11] and [12] for details). Further, the avalanche effect for SPNs with many rounds can be predicted by the model. For example, the predicted avalanche effect for an SPN with 8 rounds is shown in the same figure. It can be seen that an SPN exhibits a better avalanche effect as the number of rounds increases.

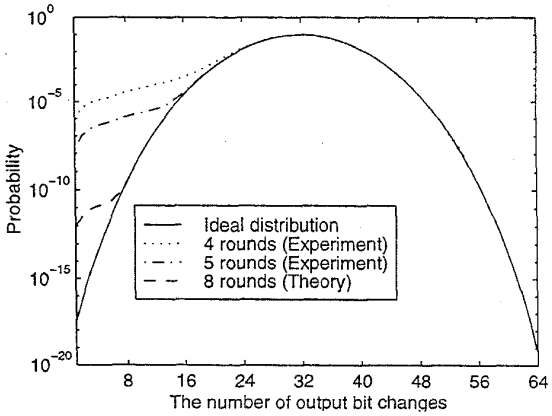

Figure 2: Probability distribution of output bit changes for the SPN with M=64, m=n=8

Lemma 1 [12] *(Markov model) For an N-bit SPN with $n \times n$ s-boxes ($N = n^2, m = n$), if we denote the probability of j active s-boxes in round $r+1$ given i active s-boxes in round r by p_{ij}, then the transition matrix is defined by $\mathbf{P} = [p_{ij}]$ where $1 \leq i, j \leq n$ and*

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

3 Principle of the Attack

In this section we describe a cryptanalytic attack which can be applied to the SPNs with a large number of rounds. Based on the Markov model in the previous section, we show that if making the target s-box active leads to a small number of active s-boxes in the last round, then it is most likely that only one s-box is active in the second round.

Consider a r-round SPN with n_i representing the number of active s-boxes in round i ($1 \leq i \leq r$), the probability of k active s-boxes in round r given one active s-box in the first round is denoted by $Pr(n_r = k | n_1 = 1)$. Actually, it is a transition probability of $r-1$ rounds. Now the selection matrix is defined by $\mathbf{S} = \left[s_{jk}^{(r)}\right]$ where

$$s_{jk}^{(r)} = \frac{Pr(n_r = k; n_2 = j | n_1 = 1)}{Pr(n_r = k | n_1 = 1)}. \quad (2)$$

In other words, $s_{jk}^{(r)}$ is the probability of having j active s-boxes in the second round given that there is one active s-box in the first round and k active s-boxes in the last round.

Now from the matrix $\mathbf{S}$ we may predict the number of active s-boxes in the second round by selecting those $s_{jk}^{(r)}$ greater than 50% . If we know how many s-boxes are active in the second round, then we know the output changes of the target s-box. Since the exact inputs to the target s-box are known, we can increment the counters of possible subkeys according to the XOR table of the target s-box. After we examine a number

of chosen plaintext pairs, the correct subkey will be counted more often than all the others. The same method is used to derive all subkeys in the first round. If the first round is broken, then we can break the subsequent rounds in the same manner.

We find that it is highly probable that only one s-box in the second round is active if a small number of s-boxes are active in the last round. This also conforms to our intuition. So only the first row of the matrix **S** is important. If we define the selection set of the r-round SPN as $\mathcal{T}_r = \{k | s_{1k}^{(r)} > 0.5\}$, then the algorithm for attacking the target s-box in the first round of the r-round SPN is:

1. Encrypt a pair of random plaintexts such that only the target s-box is active. If the number of active s-boxes in the last round is not in the set $\mathcal{T}_r$, then go to 1.

2. Increment the counters of possible subkeys according to those XOR table entries which make only one s-box in the second round active. If there is no such subkey with counter greater than all the others by a threshold value (e.g., 2), then go to 1.

3. Stop. The subkey of the target s-box is found.

The number of chosen plaintext pairs required to determine the subkeys in the first round may be approximated by $N_P = c/P_d$, where c is a constant which may be approximated by $6m$, i.e., six times the number of s-boxes in one round (similar to the results in [1]), and

$$P_d = \sum_{i \in \mathcal{T}_r} Pr(n_r = i | n_1 = 1). \qquad (3)$$

The threshold value corresponds to the confidence level of success. The higher the value, the more confidence we have that the subkey is correct and the more chosen plaintext pairs we need. The selection set may be empty for SPNs with a large number of rounds. This suggests that these SPNs are immune to our attack. In addition, the use of s-boxes with a high diffusion order [4] could thwart our attack effectively.

4 Experimental Results

Our results for the 64-bit SPN with randomly selected 8×8 s-boxes are shown in Table 1. Here we define the complexity as the number of chosen plaintext pairs required to determine the first round subkeys according to the calculation of N_P and choose $c = 50$. Our attack is effective for up to 11-round SPNs. Moreover, if we guess the 8-bit subkey associated with the target s-box in the first round, we may attack one more round with complexity increased 2^8 times. But this is not efficient in that the required plaintext pairs for 12 rounds is almost beyond the total number of plaintext pairs available for a 64-bit SPN.

Rounds	Complexity (N_P)
2	2^{11}
3	2^{12}
4	2^{14}
5	2^{19}
6	2^{25}
7	2^{30}
8	2^{36}
9	2^{43}
10	2^{47}
11	2^{55}
12	2^{63}

Table 1: Differential-like cryptanalysis of a 64-bit SPN with 8×8 s-boxes

A simulation program was run to attack a 64-bit SPN composed of 8×8 s-boxes with maximum XOR table entry $XOR^* = 4$. The experimental results for up to 8 rounds[1] are plotted in Figure 3 which also shows the theoretical complexity of our new attack and classical differential cryptanalysis. Note that the example seems unfavourable to differential cryptanalysis since we use a set of s-boxes with small XOR^* which are generated from [7] and [10]. The expected XOR^* value of a randomly selected 8×8 s-box is upper bounded by 16 [8]. But in practice, the value is about 12 and the highly probable char-

[1]The experiment for 8 rounds takes about 20 days on a Sun-ULTRA 1 machine.

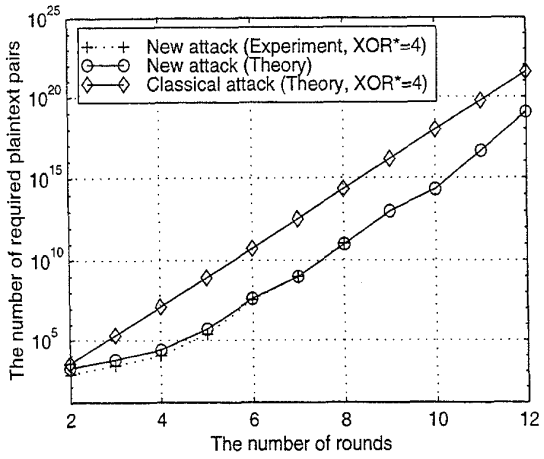

Figure 3: Comparison of classical differential cryptanalysis and our new attack on a 64-bit SPN with 8×8 s-boxes

acteristic can not always make use of all of these large values. So our attack outperforms the classical differential attack in a practical sense.

5 Conclusion

We have presented a new differential-like attack on a class of SPNs based on the Markov model of the networks. Our attack has the following properties: (1) easy implementation, (2) minimal preliminary analysis, (3) insensitive to the key-scheduling algorithm (also valid for differential attacks). Theoretical and experimental results suggest that our new attack is more efficient than classical differential cryptanalysis. On the other hand, it is also shown that 64-bit SPNs are resistant to our attack after 12 rounds.

References

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

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

[3] H.M. Heys and S.E. Tavares. Avalanche characteristics of substitution-permutation encryption networks. *IEEE Trans. on Computers,* vol.44, no.9, pp.1131-1139, 1995

[4] H.M. Heys and S.E. Tavares. Substitution-permutation networks resistant to differential and linear cryptanalysis. *J. of Cryptology,* vol.9, no.1, pp.1-19, 1996

[5] X. Lai, J.L. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. *Advances in Cryptology: Proc. of EUROCRYPT '91,* Springer-Verlag, pp.17-38, 1991

[6] K. Nyberg and L.R. Knudsen. Provable security against differential cryptanalysis. *Advances in Cryptology: Proc. of CRYPTO '92,* Springer-Verlag, pp.566-574, 1993

[7] K. Nyberg. Differentially uniform mappings for cryptography. *Advances in Cryptology: Proc. of EUROCRYPT '93,* Springer-Verlag, Berling, pp.55-64, 1994

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

[9] C.E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal,* Vol.28, pp.656-715, 1949

[10] A.M. Youssef, Z.G. Chen, and S.E. Tavares. Construction of highly nonlinear injective s-boxes with application to CAST-like encryption algorithm. *Proc. of the Canadian Conference on Electrical and Computer Engineering (CCECE '97),* pp.330-333, 1997

[11] A.M. Youssef and S.E. Tavares. Modelling avalanche characteristics of substitution-permutation networks using Markov chains. *Proc. of the 5th Canadian Workshop on Information Theory,* pp.45-48, Toronto, June 3-6, 1997

[12] A.M. Youssef. *Analysis and Design of Block Ciphers.* PhD thesis, Queen's University, Kingston, Canada, 1997