DIFFERENTIAL CRYPTANALYSIS FOR A 3-ROUND SPN

M. Tolga Sakallı Ercan Buluş Andaç Şahin Fatma Büyüksaraçoğlu
e-mail: tolga@trakya.edu.tr. e-mail: ercanb@trakya.edu.tr e-mail: andacs@trakya.edu.tr e-mail: fbuyuksaracoglu@trakya.edu.tr
Trakya University, Faculty of Engineering and Architecture, Department of Computer Engineering
Edirne, Turkey

Key words: Differential cryptanalysis, SPN (Substitution Permutation Network), AES (Advanced Encryption Standard).

ABSTRACT

SPNs (Substitution Permutation Networks) are one of the important architectures used for designing block ciphers. In our study, we applied differential cryptanalysis method for a 3-round SPN. We have used a 16-bit input as plaintext and 16-bit output as ciphertext and chosen the first row of the third S-box of DES (Data Encryption Standard) for the necessary S-box and ShiftRows transformation which is used to permute bytes in AES (Advanced Encryption Standard) for permutation of bits for our SPN. As a result, we have obtained 12-bit key of 16-bit key from the last round of the cipher using differential cryptanalysis method.

I. INTRODUCTION

Encryption algorithms are very important for cryptography and they are used to provide security and privacy. Block ciphers are symmetric algorithms and use one key to encrypt and decrypt the data. SPNs which represent one of the two important architectures are used for designing block ciphers. While AES [6, 10] (Advanced Encryption Standard) which is recent adoption of Rijndael has an SPN architecture, DES [5] (Data Encryption Standard) which was developed in cooperating with IBM and National Security Agency (NSA) in 1974 has a feistel architecture. Square cipher [9] which is the predecessor of AES has also an SPN architecture.

On the other hand, the security of block ciphers depends on cryptanalitic attacks and statistical tests which can give some useful information to the attacker. Key size, substitution boxes and round number, which are important components of encryption algorithm, should be chosen very carefully in order to make the encryption algorithm resistant to the cryptanalytic attacks and to pass it the statistical tests.

Cryptanalysis [1] is the science of breaking ciphers. Successful cryptanalysis may recover the plaintext or the key. From attacker's point of view, it is necessary that he should have the information available to mount his attack. There are four main attack models on cryptosystems according to the information available for the attacker:

- *ciphertext only attack,* when attacker possesses a string of ciphertext y,
- *known plaintext attack*, when attacker possesses a string of plaintext x and the corresponding ciphertext string y,
- *chosen plaintext attack*, when attacker can choose a plaintext string x and constructs the corresponding ciphertext string y,
- *chosen ciphertext attack*, when attacker can choose a ciphertext string y and constructs the corresponding plaintext string x.

There is an important criterion to decide whether cryptanalysis method for block ciphers is successful or not. If the cryptanalysis method breaks a block cipher with an effort less then exhaustive key search, it is then considered as a successful one. In exhaustive search, for any n-bit block cipher with a key size of k, the attacker tries all 2^k possible key values and verifies if he can derive meaningful plaintext.

The two most popular attacks, differential [2, 3] and linear [14] attacks for block ciphers, were developed by Biham in 1991 and Matsui in 1993. These were methods of statistical cryptanalysis and they were used against DES algorithm. There was a mathematical idea behind these attacks and the attacks were a big contribution for designing stronger encryption algorithms. After these attacks, other cryptanalysis methods have been developed, like truncated differential cryptanalysis [13], higher order differential cryptanalysis [13] and impossible differential cryptanalysis [4].

Differential cryptanalysis which was developed by Biham is a chosen plaintext attack and it exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher. The security of SPNs against differential cryptanalysis depends on maximum differential probability (MDP) [11, 12]. To guarantee provable security against differential cryptanalysis, it is necessary to demonstrate that MDP is sufficiently small that corresponding data complexity (the number of chosen plaintext pairs used by the attacker) is prohibitively large.

In our study, we have applied differential attack against the 3-round SPN cipher. As a result, we have obtained 12-bit key used in the last round of the cipher.

II. SUBSTITUTION-PERMUTATION NETWORKS

An SPN [1, 7, 8, 12] is a special type of iterative cipher. For an *Nr*-round and *N*-bit block SPN, it requires (*Nr*+1) *N*-bit sub-keys $K_1, K_2, ..., K_{Nr}, K_{Nr+1}$. Each round consists of three layers: key mixing, substitution, linear transformation (permutation). In the key mixing layer, *N*-bit round input is XOR-ed with the sub-key for that round. In the substitution layer, the output of mixing layer is partitioned into sub-blocks of size *n* which is the number of bits becoming the input to a bijective *n* x *n* substitution box (S-box), denoted $\pi_S : \{0,1\}^n \rightarrow \{0,1\}^n$. In the permutation layer, the output of substitution layer becomes an input to the permutation - denoted $\pi_P : \{1,.....N\} \rightarrow \{1,.....N\}$ and permutation layer is used to replace *N*-bit with a different set of *N*-bit. In the last round, permutation is omitted since it adds no cryptographic strength.

For decryption, the sub-keys are applied in reverse order. The mappings used in S-boxes are the inverse of the mappings in the encryption network and we should use the inverse linear transformation. In Figure 1, we showed an SPN algorithm which we will use to describe and to apply the differential cryptanalysis.

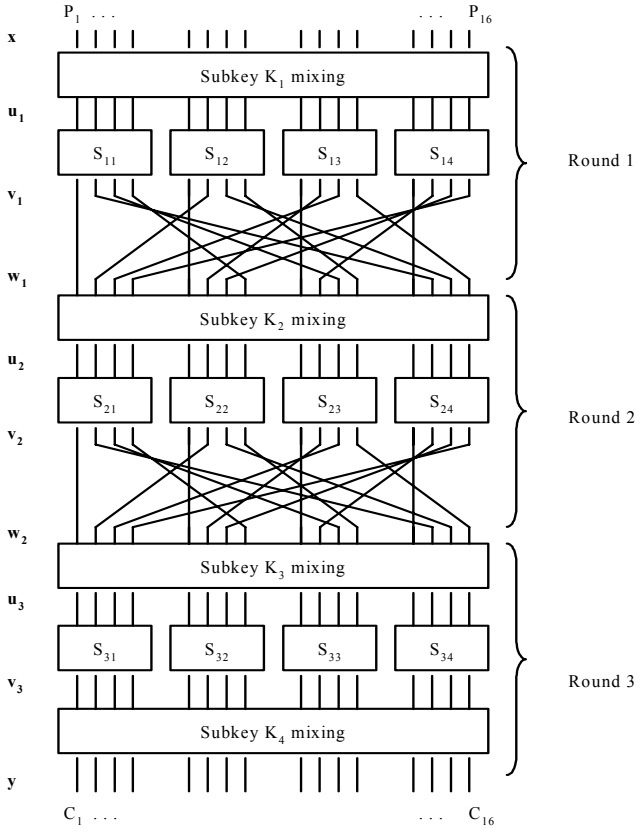

Figure 1. Used SPN Algorithm (*Nr* = 3, *N* = 16, *n* = 4).

In Figure 1, *x, u, v, w,* and *y* values, which are the places when we proceed through the network, will make understandable the SPN algorithm and differential cryptanalysis.

In Table 1 and Table 2, there are displayed the S-box and permutation for the SPN shown in Figure 1. The mapping chosen for our cipher is selected from S-boxes of DES: it is the first row of the third S-box. The values for permutation are selected from ShiftRows transformation of the AES. In AES, ShiftRows transformation is used to permute the bytes of that round. In our cipher, we have used this transformation to permute the bits of that round. AES also includes an additional linear transformation (MixColumns) in each round.

III. DIFFERENTIAL CRYPTANALYSIS

As we have said before differential cryptanalysis [8] is a chosen plaintext attack and it exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher. Attacker can choose plaintext string and construct ciphertext string in an attempt to derive the key. Consider our cipher with input $X = [X_1 X_2 .... X_N]$ and output $Y = [Y_1 Y_2 .... Y_N]$. Differential cryptanalysis seeks to exploit a scenario where a particular ΔY occurs given a particular input difference ΔX with a high probability DP (Differential Probability). The pair $(\Delta X, \Delta Y)$ is referred to as a differential where $X \oplus \Delta X = X'$ or $X \oplus X' = \Delta X$ and $Y \oplus \Delta Y = Y'$ or $Y \oplus Y' = \Delta Y$.

To realize differential attack against our SPN, we should find a differential characteristic (sequence of input and output differences) for one round with a high probability. We can develop it for the whole cipher that is why output difference from one round corresponds to the input difference for the next round. For *Nr*-round block cipher, we can construct *(N r - 1)*-round differential characteristic and we can derive the key used in the last round of the cipher. To construct a highly likely differential characteristic, we should examine properties of nonlinear part of our cipher, S boxes, to determine the complete differential characteristic.

Let S: $Z_2^n \rightarrow Z_2^n$ be a bijective mapping. Differential Probability [11] for the S is defined in equation (1) where the *a* and *b* are called input and output difference, respectively and they are *n*-bit vectors.

$$DP^S(a,b) = \frac{\#\{x \in Z_2^n \mid S(x) \oplus S(x \oplus a) = b\}}{2^n} \qquad (1)$$

Z_2^n : n dimensional vector over the finite field $Z_2 = GF(2)$

$\#\mathcal{A}$: number of elements in set $\mathcal{A}$

Table 1. S-box Representation for SPN.

Hex.	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Input	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Output	1010	0000	1001	1110	0110	0011	1111	0101	0001	1101	1100	0111	1011	0100	0010	1000
Hex.	A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8

Table 2. Permutation for SPN.

Input	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Output	1	14	11	8	5	2	15	12	9	6	3	16	13	10	7	4

If we calculate input and output differences for all probable (a, b) then we obtain a table which we call difference distribution table. It means that we should calculate $\#\{x \in Z_2^n \mid S(x) \oplus S(x \oplus a) = b\}$ for all probable (a, b) values. Then, we can obtain DP values easily by dividing values in the difference distribution table to 2^n. The difference distribution table for the S-box of Table 1 is given in Table 3.

Table 3. Difference Distribution Table

	Output Difference															
Input Difference	a,b	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	2	0	2	0	0	6	2	2	0	0	2
	2	0	0	0	2	0	0	2	0	0	4	2	0	2	2	2	0
	3	0	2	0	4	2	0	4	0	0	2	0	0	2	0	0	0
	4	0	0	0	2	0	0	2	0	0	2	2	2	2	0	2	2
	5	0	2	0	0	2	4	4	0	0	2	0	0	2	0	0	0
	6	0	0	0	4	0	6	0	2	0	0	0	0	0	2	0	2
	7	0	0	0	0	0	0	0	0	4	2	2	0	2	0	0	6
	8	0	0	0	0	0	2	0	2	0	2	0	2	0	8	0	0
	9	0	2	4	0	0	0	0	6	2	0	0	0	0	0	2	0
	A	0	2	0	2	4	0	2	2	2	0	0	2	0	0	0	0
	B	0	2	0	0	2	0	0	0	0	0	0	2	2	2	4	2
	C	0	2	2	2	2	0	2	2	0	0	0	2	0	0	2	0
	D	0	2	2	0	0	0	0	0	2	2	0	4	2	0	2	0
	E	0	0	2	0	2	0	0	0	6	0	4	0	0	0	2	0
	F	0	2	6	0	2	2	0	0	0	0	0	0	0	2	0	2

IV. DIFFERENTIAL CRYPTANALYSIS FOR A 3-ROUND SPN

To derive the key in the last round of the cipher, we should construct a differential characteristic with a high DP so that we use a small number of plaintext pairs. For 3-round SPN, we can construct a 2-round differential characteristic and attack sub-key K_4. In Figure 2, a sample differential characteristic we will use is shown.

We use the following difference pairs of the S-box:

$$S_{12} : a = E \rightarrow b = 8 \; with \; DP = \frac{6}{16}$$

$$S_{22} : a = 8 \rightarrow b = D \; with \; DP = \frac{8}{16}$$

In Figure 3, while we proceed through the network, it is shown that we obtain a relation between ΔP and Δu_3 with DP $= \frac{6}{16} \times \frac{8}{16} = \frac{48}{256} \cong 0{,}19$. In addition to that we can obtain 12-bit key of 16-bit key, K_4, using differential cryptanalysis. Because we are interested in non-zero differences in differential output, Δu_3 *or* ΔY. We refer to 12-bit key [$K_{4,1}$, $K_{4,2}$,....$K_{4,12}$], which we will attack to derive, as target partial sub-key. To realize differential attack for our cipher, we should construct some number of chosen plaintext pairs in which a pair contains (P, P', Y, Y') (2 plaintexts: P and P', 2 ciphertexts: Y and Y') where $P' = P \oplus \Delta P$ or $\Delta P = P \oplus P'$. After that, a partial decryption of the last round which involves the XOR of ciphertexts with the target partial sub-key bits and running data backwards through the S boxes, where all possible values for the target key bits would be tried is executed.

For our cipher, a count is incremented for all possible target sub-key values when Δu_3 is obtained as "481" in hexadecimal notation for a pair. This process is executed for all possible target partial sub-keys and for all chosen plaintext pairs and the partial sub-key value which has the largest count is assumed to indicate the correct values of the sub-key bits. N_D value which is the number of chosen plaintext pairs can be found for our cipher using equation (2). In equation (2), c is a small constant and DP is differential probability for *(Nr - 1)* round differential characteristic.

$$N_D = \frac{c}{DP} \tag{2}$$

In our study, if we choose c = 10 then N_D value is found as $\frac{10}{0{,}19} = 52 \cong 50$. We have simulated our attack using 50 chosen plaintext pairs.

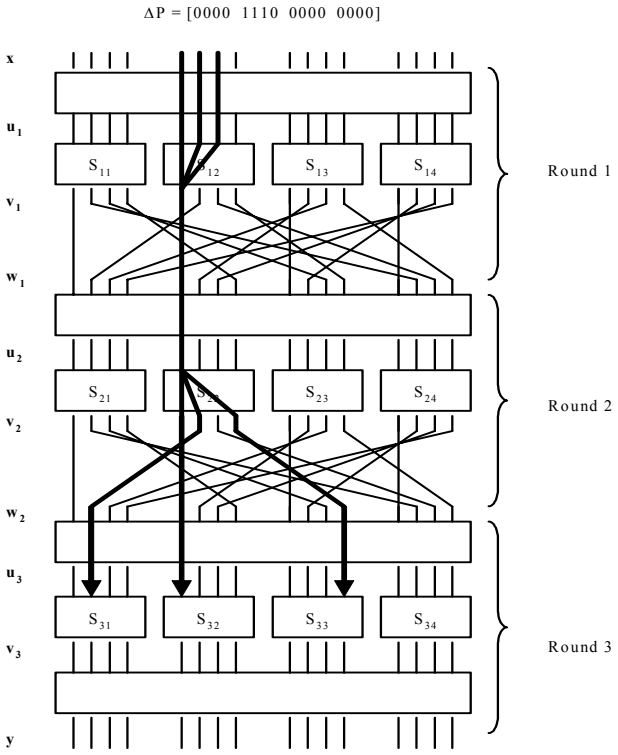

Figure 2. Sample Differential Characteristic

$\Delta P = [0000\ 1110\ 0000\ 0000]$

$\Delta u_1 = [0000\ 1110\ 0000\ 0000]$

$\Delta v_1 = [0000\ 1000\ 0000\ 0000]$

$\Delta w_1 = [0000\ 1000\ 0000\ 0000]$

$\Delta u_2 = [0000\ 1000\ 0000\ 0000]$

$\Delta v_2 = [0000\ 1101\ 0000\ 0000]$

$\Delta w_2 = [0100\ 1000\ 0001\ 0000]$

$\Delta u_3 = [0100\ 1000\ 0001\ 0000]$

Figure 3. Relation between ΔP and Δu_3

During the cryptanalysis process, we will generate 50 chosen plaintext pairs for which

$$\Delta P = [0000\ 1110\ 0000\ 0000]$$

and differential characteristic illustrated will occur with high probability, DP = 0,19. We call such pairs for ΔP as right pairs. On the contrary, chosen plaintext pairs for which the differential characteristic (That means Δu_3 is "481" in hexadecimal notation for our sample differential characteristic) does not occur are referred to as wrong pairs. Estimated probability of the occurrences of right pairs for the candidate partial sub-key can be derived from equation (3).

$$p = \frac{count}{50} \tag{3}$$

Table 4. Experimental Results for Differential Attack in which Probability (p) > 0.05 for Partial Sub-key Values

Partial sub-key (Hex.)	Number of right pairs for the candidate partial sub-key (count)	Probability > 0,05 (p)
617	5	0,10
620	4	0,08
625	4	0,08
627	**11**	**0,22**
628	4	0,08
62C	3	0,06
62D	4	0,08
62F	4	0,08
647	3	0,06
655	3	0,06
657	5	0,10
65D	3	0,06
65F	3	0,06
667	3	0,06
675	3	0,06
677	6	0,12
678	3	0,06
67D	3	0,06
67F	3	0,06
685	3	0,06
687	4	0,08
68D	3	0,06
68F	3	0,06
697	4	0,08
6A5	3	0,06
6A7	4	0,08
6AD	3	0,06
6AF	3	0,06
6B7	3	0,06
6C7	5	0,10
6F0	3	0,06
6F5	4	0,08
6F7	7	0,14
6FD	4	0,08
6FF	4	0,08
920	3	0,06
927	3	0,06
9F0	3	0,06
9F7	3	0,06

In Table 4, experimental results for differential attack in which probability (p) > 0,05 for partial sub-key values are shown. In our study, we have tried 2^{12} probable partial sub-key values and showed some partial sub-key values which satisfy p > 0,05. As a result, partial sub-key value which is "627" in hexadecimal notation is the largest count value (or probability) and the correct sub-key value. In addition to that we would expect the probability of the occurrences of the right pair to be DP = 0,19 and we found experimentally the probability for the sub-key value "627" gave p = 0,22. Other large count values like p = 0,14 for the sub-key value "6F7" may be occurred for the reason of the S-box properties.

V. CONCLUSION

In our study, we applied differential cryptanalysis method for 3-round SPN and obtained 12-bit key [$K_{4,1}$, $K_{4,2}$,....$K_{4,12}$], which is "627" in hexadecimal notation, from the last round of the cipher. Roughly speaking, second linear transformation used in AES - MixColumns which is 32-bit additional linear transformation when it is compared with an SPN structure - is very important and it makes impossible to find differential characteristics for differential cryptanalysis and linear approximations for linear cryptanalysis that involve few active S-boxes (active S boxes - S boxes involved in the differential characteristic or in the linear approximation).

REFERENCES

1. D. R. Stinson, *Cryptography: Theory and Practice*, Second Edition, CRC Press, 2002.
2. E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, Vol 4, No 1, pp. 3-72, 1991.
3. E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.
4. E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of Skipjack reduced to 31 rounds using Impossible Differentials*, Advances in Cryptology-Eurocrypt'99, Springer-Verlag, pp. 55-64, 1996.
5. FIPS 46-3, *Data Encryption Standard*, Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., October 25, 1999.
6. FIPS 197, *Advanced Encryption Standard*, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November 26, 2001.
7. H. M. Heys, S. E. Tavares, *Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis*, Journal of Cryptology, Vol 9, No 1, pp. 1-19, 1996.
8. H. M. Heys, *A Tutorial on Linear and Differential Cryptanalysis*, Cryptologia, Vol 26, No 3 pp. 189-221, 2002.
9. J. Daemen, L. R. Knudsen, and V. Rijmen, *The Block cipher Square*, Proceedings of Fast Software Encryption, New York: Springer Verlag, pp. 149-165, 1997.
10. J. Daemen, V. Rijmen, *AES Proposal: Rijndael*, First Advanced Encryption Conference, California, 1998.
11. K. Chun, S. Kim, S. Lee, S. H. Sung, S. Yoon, *Differential and linear cryptanalysis for 2-round SPNs*, Information Processing Letters, Elsevier, 2002.
12. L. Keliher, *Linear Cryptanalysis of Substitution-Permutation Networks*, PHd Thesis, 2003.
13. L. R. Knudsen, *Truncated and Higher Order Differentials, Fast Software Encryption*, Springer-Verlag, pp. 196-211, 1995.
14. M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology - Eurocrypt '93, Springer-Verlag, pp. 386-397, 1994.