A Note on the Theoretical and Practical Security of Block Ciphers

Öznur Mut Sağdıçoğlu[1], Serhat Sağdıçoğlu[2] and Ebru Küçükkubaş[3]

[1] Institute of Applied Mathematics, Middle East Technical University, Turkey
oznurmut@metu.edu.tr
[2] HAVELSAN A.Ş., Turkey
[3] TÜBİTAK BİLGEM, Turkey

Abstract. Differential cryptanalysis is one of the most effective methods for evaluating the security level of block ciphers. For this, an attacker tries to find a differential or a characteristic with a high probability that distinguishes a block cipher from a random permutation to obtain the secret key. Although it is theoretically possible to compute the probability of a differential for a block cipher, there are two problems to compute it practically. The first problem is that it is computationally impossible to compute differential probability by trying all plaintext pairs. The second problem is that the probability of a differential over all choices of the plaintext and key might be different from the probability of the differential over all plaintexts for a fixed key. Thus, to evaluate the security against the differential cryptanalysis, one must assume both the hypothesis of stochastic equivalence and the Markov model. However, the hypothesis of stochastic equivalence does not hold in general. Indeed, we show on simple ciphers that the hypothesis of stochastic equivalence does not hold. Moreover, we observe that the differential probability is not equal to the expected differential probability. For these results, we study plateau characteristics for a 4-bit cipher and a 16-bit super box. As a result, when considering differential cryptanalysis, one must be careful about the gap between the theoretical and the practical security of block ciphers.

Key words: Differential cryptanalysis, Stochastic Equivalence, Markov Ciphers, Midori

1 Introduction

Differential cryptanalysis invented Biham and Shamir is one of the most powerful and popular attack method applied to block ciphers, [1]. It was the first attack faster than brute force for full round DES, [2]. After this discovery, the differential cryptanalysis has became an important security criterion in block cipher design. Differential cryptanalysis consider a

pair of differences (α, β) such that for a given input difference α the output difference after certain number of rounds, say $r > 1$, is β with high probability. In practice, it is usually infeasible to calculate the probability of differential characteristics for an r-round block cipher. The reasonable approach to compute such probability is that to calculate the product of one round differential characteristics in iterative rounds. However, in this case we have to face with two problems to find the real probability of differential characteristics for a block cipher with r rounds.

The first problem is that the probability of such differential characteristic depends on the initial pair of plaintexts and the dependence of the differences in each round, as the round functions are in general not independent. This corresponds to the assumption that for a Markov cipher with uniformly distributed and independent round keys, the probability of an r-round characteristic is the product of the probabilities of the r one-round characteristics, [3]. Markov ciphers are defined as iterated ciphers whose round functions satisfy the condition that the differential probability is independent of the choice of one of the component plaintexts under an appropriate definition of difference. DES and AES with independent subkeys are Markov ciphers when the notion of difference is the exclusive-or operation. Thus, the study of differential cryptanalysis for an r-round Markov cipher is reduced to the study of the transition probabilities created by its round function. Actually, experimental differential analysis of the DES block cipher using $\oplus$ as difference operator demonstrated that the concatenation of 1-round characteristics is a good approximation to the real probability for differential attacks in practice, even when the round subkeys are generated from a deterministic key schedule algorithm.

The second problem is while finding a differential characteristic, the attacker computes differential characteristics independent of the value of the secret key. For this, it is reasonable to assume that the probability of a differential characteristic is independent of the value of the secret key. This assumption is known as the hypothesis of stochastic equivalence. This hypothesis states that the probability of a differential characteristic behave (almost) in the same way for all keys, [3].

When designing a block cipher, we need to give its security proof and hence we need to assume the hypothesis of stochastic equivalence and Markov model. By these assumptions we can calculate the expected differential probability (EDP) of an iterated cipher by taking product of probability of single round characteristics. As a result we can give bounds on the expected data complexity which an attacker uses in her/his attack.

However, since the hypothesis of stochastic equivalence does not hold in ciphers used in practice, it can not be used to calculate the probability of differential characteristic. As an example, it was shown that for the AES there are keys with differential probability (DP) 2^{100} times greater than the expected differential probability (EDP),[4] .

Actually, the fixed key probability of a differential characteristic depend on value of the key. This notion was defined as plateau characteristics by Daemen and Rijmen, [4]. Plateau characteristics are a special type of characteristics whose probability depends on key and can have only 2 values. For a (usually small) subset of the keys it has a non-zero probability and for all other keys its probability is zero. In [4], it is proved that for a large group of ciphers, including the AES, all two-round characteristics are plateau characteristics, [4].

In this paper, we give plateau characteristics for an 4-bit cipher (we call it X cipher), a 16-bit super box with 4 bit S box and 4×4 MDS (Maximum Distance Separable) matrix and finally a 16-bit super box with Midori block cipher's S box, and its almost MDS matrix, [5]. For these ciphers, we show that the hypothesis of stochastic equivalence does not hold and the probability of a differential characteristic is different form the expected differential characteristic probability.

This paper is organized as follows. In Section 2, we give preliminaries of differential cryptanalysis, the definition of probability of characteristics, the expected differential probability and the definiton of plateau characteristic. In Section 3, we give a plateau characteristic for a 4-bit cipher X. Then the definition of super boxes is given Section 4. Finally we give plateau characteristics for a super box with 4-uniform S box and an MDS matrix and for Midori's super box in Section 5 and Section 6, respectively.

2 Definitions

In this section we give some definitions, [6], [4]. Let $\mathbb{F}_2$ be the finite field with two elements. Let $\mathbb{F}_2^n$ be the vector space. A differential of a function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is a pair $(a, b) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ such that

$$f(x) \oplus f(x \oplus a) = b.$$

for some x, [3]. We call a the input difference and b the output difference. The differential probability $DP(a, b)$ of a differential (a, b) (with respect to f) is defined as

$$DP(a, b) = 2^{-n} \#\{x \in \mathbb{F}_2^n : f(x \oplus a) \oplus f(x) = b\}.$$

The difference table of a function f is the matrix containing all the differential probabilities $DT_f[a,b] = DP(a,b)$. When it is clear from the context which function f is meant, we will often drop it from the notation. If f is a function parameterized by a key k, we can also define the parameterized differential probability $DP[k](a,b)$ in a straightforward way.

The expected differential probability (EDP) is the average of the differential probability over all keys. Then EDP of a differential (a,b) is defined as the mean value of $DP[k](a,b)$:

$$EDP(a,b) = \mathbb{E}(DP[k](a,b);k) = 2^{-|\mathcal{K}|}\sum_{k\in\mathcal{K}} DP[k](a,b).$$

Here, k is assumed to be a uniformly distributed random variable taking values in $\mathcal{K}$.

The *weight* of a differential (a,b) or a characteristic Q is minus the binary logarithm of their EDP, [4] :

$$weight(a,b) = -log_2 EDP(a,b)\ ;\ weight(Q) = -log_2 EDP(Q).$$

So for a function parameterized by a key, the difference table consists of the values $DT_f[a,b] = EDP_f(a,b)$.

Let $B[k](x)$ denote a function composed of r steps $f^i[k^i](x)$ parameterized by r keys $k^1, k^2, ..., k^r \in \{0,1\}^n$:

$$B[k](x) = (f^r[k^r] \circ ... \circ f^1[k^1])(x).$$

A characteristic through $B[k](x)$ is a vector $Q = (b^0, b^1, ..., b^r)$ with $b^i \in \{0,1\}^n$ for $i = 0, 1, \ldots, r$. A characteristic $Q = (b^0, b^1, ..., b^r)$ is in a differential (a,b) if $b^0 = a$ and $b^r = b$. If we now consider the following set of equations

$$\begin{aligned} f^1[k^1](x + b^0) &= f^1[k^1](x) + b^1 \\ &\vdots \\ (f^R[k^r] \circ ... \circ f^1[k^1])(x + b^0) &= (f^R[k^r] \circ ... \circ f^1[k^1])(x) + b^r \end{aligned} \qquad (1)$$

then the parameterized differential probability $DP_B[k](Q)$ of a characteristic Q with respect to $B[k](x)$ is defined as

$$DP[k](Q) = 2^{-n}\#\{x \in \mathbb{F}_2^n |\ \text{x satisfies (1)}\}.$$

It is well-known [3] that for Markov ciphers we have

$$DP[k](a,b) = \sum_{Q \in (a,b)} DP[k](Q).$$

and

$$EDP(a,b) = \sum_{Q \in (a,b)} EDP(Q).$$

We now give the definition of plateau characteristics.

Definition 1 *(**Plateau characteristic**, [4]) A characteristic Q is a plateau characteristic with height $height(Q)$ if and only if both of the followings hold:*

1. *For a fraction $2^{n_b-(weight(Q)+height(Q))}$ of the keys $DP[k](Q) = 2^{height(q)-n_b}$.*
2. *For all other keys $DP[k](Q) = 0$.*

Here height is the number of right pairs for a characteristic in binary logarithm.

3 A Plateau Characteristic for X Cipher

In this section we present a plateau characteristic for the X cipher. X is a 4-bit block cipher containing only S boxes and 4 bit key addition. X cipher is depicted in Figure 1.

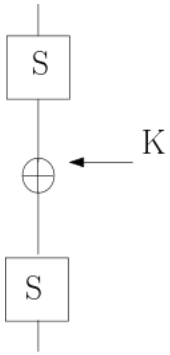

Fig. 1. X Cipher

X uses Midori's s box (given in Table 1), it is a 4-uniform s box, [5]. Namely, the maximum value in the difference distribution table is 4. Since

X satisfies the criteria of Two-Round Plateau Characteristic Theorem in [4], all characteristics Q in X are plateau characteristics. To present a plateau characteristic for X, we first give the Difference Distribution Table (DDT) in Table 2 of Midori's s box.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S(x)	12	10	13	3	14	11	15	7	8	9	1	5	0	2	4	6

Table 1. Midori's s box

	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	2	4	0	2	2	2	0	2	0	0	0	0	0	2	0
2	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0	0
3	0	0	0	0	2	0	4	2	2	2	0	0	0	2	0	2
4	0	2	4	2	2	2	0	0	2	0	0	2	0	0	0	0
5	0	2	0	0	2	0	0	4	0	2	4	0	2	0	0	0
6	0	2	0	4	0	0	0	2	2	0	0	0	2	2	0	2
7	0	0	0	2	0	4	2	0	0	0	0	2	0	4	2	0
8	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
9	0	0	4	2	0	2	0	0	2	2	0	2	2	0	0	0
a	0	0	0	0	0	4	0	0	0	0	4	0	0	4	0	4
b	0	0	0	0	2	0	0	2	2	2	0	4	0	2	0	2
c	0	0	4	0	0	2	2	0	2	2	0	0	2	0	2	0
d	0	0	0	2	0	0	2	4	0	0	4	2	0	0	2	0
e	0	2	0	0	0	0	0	2	2	0	0	0	2	2	4	2
f	0	0	0	2	0	0	2	0	0	0	4	2	0	0	2	4

Table 2. DDT for Midori S box

We consider a characteristic with the input difference $0x0a$ and the output difference $0x01$. By Table 2, the expected differential probability (EDP) of this characteristics is $EDP = \frac{4}{16} \times \frac{2}{16} = 2^{-5}$. Because the difference path in the characteristic is

$$Q : 0x0a \to 0x05 \to 0x01.$$

Let P be an input and K be a key. We consider the pairs $S(S(P) \oplus K)$ and $S(S(P \oplus 0x0a) \oplus K)$ for all input values P and all key values K. Then we look at the outputs that satisfies the difference $0x01$. Thus we calculate right pairs that satisfy the characteristic $0x0a \to 0x05 \to 0x01$.

We see that for some keys, actually a quarter of all keys, $DP[k]$ is nonzero, and equal to $\frac{2}{16}$ in Table 3.

Key value	Number of Right Pairs
0	0
1	0
2	0
3	**2**
4	0
5	0
6	**2**
7	0
8	0
9	**2**
10	0
11	0
12	**2**
13	0
14	0
15	0

Table 3. DP values of the characteristic $0x0a \rightarrow 0x05 \rightarrow 0x01$ for X cipher

This is a plateau characteristics with height $height(Q) = 1$. Namely, for nonzero DP values there are 2 right pairs for the characteristic. For example, when the key value is 3, there are 2 right pairs (namely, (2,8) and (8,2)) for the characteristic Q. Therefore the height is $log_2 2 = 1$. Thus Q is a plateau characteristic with height 1, by the Definition 4 in [4]. For the key value $k \in \{3, 6, 9, 12\}$, the probability $DP[k]$ is nonzero and equal to $DP[k] = 2^{height(Q)-4} = 2^{1-4} = 2^{-3}$ from the Table 3.

In cipher X, we observe that the hypothesis of stochastic equivalence does not hold since $EDP \neq DP[k](Q)$, actually $DP[k](Q) = 4 \times EDP(Q)$ for the keys $k \in \{3, 6, 9, 12\}$.

4 Definiton of super boxes

In [4], it is given the definition of the super box.

Definition 2 *A super box maps an array a of n_t elements a_i to an array e of n_t elements e_i. Each of the elements has size n_s. A super box takes a key k of size $n_t \times n_s = n_b$. It consists of the sequence of four transformation :*

- $b_i = S[a_i]$*: n_t parallel applications of a n_s-bit S-box.*

– $c = M(b)$*: a linear map with branch number* $n_t + 1$
– $d = c \oplus k$*: key addition*
– $e_i = S[d_i]$*:* n_t *parallel applications of a* n_s*-bit S-box.*

For a one-to-one S-box with input difference zero, we have zero output difference. Then, it has probability 1 in a super box. Thus, we consider the S boxes with nonzero input difference. They are called active S-boxes.

In [4], the height of a super box is defined in Thereom 2. In [4], it is shown that all two-round characteristics of AES are plateau characteristics. Also, they show that for the AES the vast majority of characteristics over 4 or more rounds are plateau characteristics. Moreover, they classify characteristics with heights and give a table for that.

In this paper, we consider two kind of super boxes one of which has an MDS matrix and other has an almost MDS matrix as a linear transformation. We observe that all differential characteristics of these two super boxes are plateau characteristics. Moreover, we present plateau characteristics for both types of super boxes.

5 A Plateau Characteristic for a Super Box with 4-uniform S Box and an MDS matrix

In this section, we build a 16-bit super box with Midori's S-box and a 4×4 MDS matrix over $\mathbb{F}_{2^4}$. We give this super box in Figure 2. All S boxes are the same and it is Midori cipher's S-box in Table 1. M is an MDS matrix over $\mathbb{F}_{2^4}$ (it is a finite field over $\mathbb{F}$ and extended by using irreducible polynomial $x^4 + x + 1$) :

$$M = \begin{bmatrix} 1 & 4 & 9 & 13 \\ 4 & 1 & 13 & 9 \\ 9 & 13 & 1 & 4 \\ 13 & 9 & 4 & 1 \end{bmatrix}.$$

Like in AES, all characteristics for this super box is a plateau characteristic, [4, Thereom 2]. Now we give a plateau characteristic for this super box by using Table 2.

$$1000 \xrightarrow[SSSS]{prob=\frac{2}{16}} 4000 \xrightarrow[M]{prob=1} 4321 \xrightarrow[SSSS]{prob=(\frac{2}{16})^2 \times \frac{4}{16}} 1446.$$

Here the numbers represent 4-bit values. After implementing the super box we see that the differential probability of this characteristic is $\frac{8}{2^{16}} = 2^{-13}$. Thus, the height is 3. We also observe that for some keys,

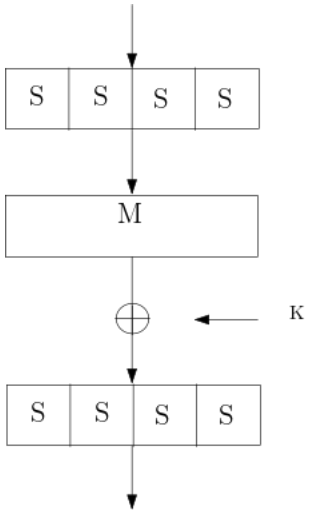

Fig. 2. A super box with an MDS matrix

actually for the half of keys, the differential probability is zero. By Table 2, $EDP = (2^{-3})^4 \times 2^{-2} = 2^{-14}$. Thus, $DP[k] = 2 \times EDP$, in other words the hypothesis of stochastic equivalence does not hold in this super box.

6 A Plateau Characteristics for Midori's Super Box

In this section we consider the super box of Midori. Namely, we have a super box using the s box and almost MDS matrix of Midori. As Midori' s box is 4-uniform, all characteristic of Midori's super box is plateau by Theorem 1 in [4]. The super box for Midori is given in Figure 3. In this figure, S boxes are all same and they are Midori's s box (Table 1). The matrix M' is an almost MDS matrix.

$$M' = \begin{bmatrix} 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \\ 1\,1\,1\,0 \end{bmatrix}.$$

For this super box, we find a plateau characteristic with differential probability $DP[k] = \frac{2^7}{2^{16}} = 2^{-9}$ for some keys, actually $\frac{1}{8}$ of all keys.

$$1000 \overset{prob=\frac{2}{16}}{\underset{SSSS}{\longrightarrow}} 1000 \overset{prob=1}{\underset{M'}{\longrightarrow}} 0111 \overset{prob=(\frac{2}{16})^2\times\frac{4}{16}}{\underset{SSSS}{\longrightarrow}} 0111.$$

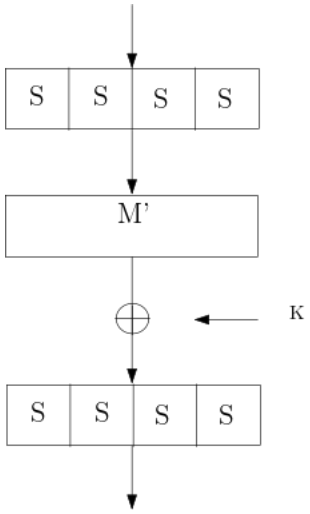

Fig. 3. A super box with an MDS matrix

Here numbers represent 4-bit values. The expected differential probability of this characteristic, calculated by using differential distribution table 2, is $(2^{-3})^4 = 2^{-12}$. Thus for a nonzero DP values $DP[k] = 8 \times EDP$. For this super box, we observe that the stochastic equivalence hypothesis does not hold.

7 Conclusion

Since it is not easy to calcuate the probability of a differential characteristic with a secret key and it is in general not possible to try all input pairs for a block cipher with r rounds, it is reasonable to assume Markov model and the hypothesis of stochastic equivalence. Under the assumptions that the cipher is a Markov cipher and round keys are random and independent, the probability of a differential characteristic is estimated by the product of the probability in each round, which is the expected differential probability (EDP) of the characteristic, i.e., the averaged probability over all independent round keys. By this assumptions the designer can give a security proof against the differential cryptanalysis.

However, we observe that ciphers used in practice usually do not satify this hypothesis of stochastic equivalence even if they satisfies the Markov model. Thus, the expected probability will be different from the differential probability. As a result, when designing a block cipher one must

be careful for evaluating theoretical and practical security against the differential cryptanalysis.

References

1. Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.
2. Eli Biham and Adi Shamir. Differential cryptanalysis of the full 16-round DES. In Ernest F. Brickell, editor, *Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings*, volume 740 of *Lecture Notes in Computer Science*, pages 487–496. Springer, 1992.
3. Xuejia Lai, James L. Massey, and Sean Murphy. Markov ciphers and differential cryptanalysis. In Donald W. Davies, editor, *Advances in Cryptology - EUROCRYPT '91, Workshop on the Theory and Application of of Cryptographic Techniques, Brighton, UK, April 8-11, 1991, Proceedings*, volume 547 of *Lecture Notes in Computer Science*, pages 17–38. Springer, 1991.
4. Joan Daemen and Vincent Rijmen. Plateau characteristics. *IET Inf. Secur.*, 1(1):11–17, 2007.
5. Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy (extended version). *IACR Cryptol. ePrint Arch.*, page 1142, 2015.
6. Joan Daemen, Mario Lamberger, Norbert Pramstaller, Vincent Rijmen, and Frederik Vercauteren. Computational aspects of the expected differential probability of 4-round AES and aes-like ciphers. *Computing*, 85(1-2):85–104, 2009.