Linear and Differential Cyptanalysis of Sailing Sea Monkey

CS13B027 Hemanth Kumar Tirupati

CS13B046 Aravind Krishna

CS13B062 Shreyas Harish

March 10, 2016

Abstract

In this paper we give formal mathematical proof for the resistance of Sailing Sea Monkey against general attacks on block ciphers *viz* Linear and Differential Cryptanalysis. We provide a lower bound on minimum number of Plain Text and Cipher Text pairs needed for cracking the proposed cipher with *sufficient* confidence. These lower bounds turn out to be much higher than number of key verfications (i.e, 2^{128})required by brute force and therefore are not viable attacks on the cipher.$\diamondsuit$

1 Introduction

Let the input to our cipher be $\boxed{a}\boxed{b}\boxed{c}\boxed{d}$

Represented in matrix form, $Input = \begin{bmatrix} a & c \\ b & d \end{bmatrix}$

The output of Sbox be

$S = SBox(Input) = \begin{bmatrix} A & C \\ B & D \end{bmatrix}$

After SBox layer, we perform shift-rows operations and multiplication with MDS matrix $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$.

Therefore final output of the first layer would be $O_1 = \begin{bmatrix} A+2D & B+2C \\ A+3D & B+3C \end{bmatrix}$

$\implies O_1 = \boxed{A+2D}\boxed{A+3D}\boxed{B+2C}\boxed{B+3C}$

$\implies$ Disturbing one bit of input (say A) disturbs first two bytes input to next round.

Additionally it can also be seen that disturbing first two bytes (A and B) of input to a round disturbs all the output bytes.

Following table summarizes the working of cipher.

	Round 1			
Input Plaintext	a	b	c	d
Key XORing and SBoxing	A	B	C	D
Shift Rows	A	D	C	B
Mix Columns	$A+2D$	$A+3D$	$B+2C$	$B+3C$

Output of *Round 1* would be as input to passed to *Round 2*

	Round 2			
Round 2 input	$A+2D$	$A+3D$	$B+2C$	$B+3C$
Key XORing and SBoxing	$f_1(A,D)=X$	$f_2(A,D)=Y$	$f_3(B,C)=Z$	$f_4(B,C)=W$
Shift Rows	X	Z	W	Y
Mix Columns	$X+2Z$	$X+3Z$	$Y+2W$	$Y+3W$

2 Resistance to Linear Cryptanalysis

Proposition 1. *Total Bias of linear approximation involving n SBoxes is decreasing function in n.*

Inorder to maximize bias of a linear combination, the adversary must choose a path such that total bias of linear approximation (involving n SBoxes) $\epsilon = 2^{n-1}\epsilon_1\epsilon_2...\epsilon_n$ is maximized.

$\implies \epsilon \leq 2^{n-1}\epsilon_0^n$ where ϵ_0 is maximum bias possible for any linear approximation of SBox.

$\implies$ $2^{n-1}\epsilon_0^n$ is the maximum bias that adversary can squeeze out of any linear approximation involving n SBoxes.

In our cipher $\epsilon_0 = 0.0625 \implies 2\epsilon_0 < 1 \implies$ total bias is decreasing function in terms of number of SBoxes involved.$\diamondsuit$

So, maximizing possible bias ,$2^{n-1}\epsilon_0^n$ is same as minimizing n, the number of SBoxes involved.

Proposition 2. *Any linear trail on the cipher involves a minimum of 31 SBoxes.*

Proof. In order to construct any linear trail □

- Choose bits of input plain text that are going to be part of final linear approximation
- Construct a linear trail by tracing through linear approximation of these bits to next round.

  This trace through invloves finding all active SBoxes that depend on output bits corresponding to

linear approximation involving the chosen bits.

Example. Say in input $x_1x_2.....x_{32}$, we tried to construct a linear trail involving x_3, x_4, x_5 and linear approximation we use is $x_3 \oplus x_4 \oplus x_5 \oplus y_1 = 0 \implies$ in further rounds, we must include all SBoxes that depend on $y_1$as part of linear approximation.

In our cipher, diffusion optimality occurs after 2 rounds of encryption i.e, after two rounds, all 4 SBoxes in a round become part of linear combination.

So, minimum number of SBoxes that would contribute to final bias $= \underbrace{1}_{round1} + \underbrace{2}_{round2} + \underbrace{4 \times 7}_{rounds\,3-9} =$ $31\diamondsuit$.

Using Propositions 1 and 2 we can say any linear approximation, adversary can get bias that is bounded above by

$$\epsilon_{threshold} = 2^{31-1} \times \epsilon_0^{31} \approx 5.05 \times 10^{-29}$$

Inorder to guess partial key bits of penultimate round, we need $\mathcal{O}(\frac{1}{\epsilon^2})$ known plain-text cipher-text pairs[1] $\implies \geq 3.92 \times 10^{56}$KPT's are required to guess last round partial key bits.

So, a brute force verification of $2^{128} keys = 3.40 \times 10^{38}$ has lower complexity than linear cryptanalysis.

So, linear cryptanalysis is not a viable attack on Sea Monkey.

3 Resistance to Differential Cryptanalysis

Propositions 1 and *2* have similar extensions for differential cryptanalysis.

Proposition 3. *Total propagation ratio of differential involving n SBoxes is decreasing function in n.*

Proof. □

- Propagation ratio p for the differential trail is the product of the propagation ratio for each of the SBoxes involved in the trail.
- $\implies p = p_1p_2....p_n$ where p_i denotes propagation ratio of i^{th} SBox.
- In our cipher, maximum propagation ratio is bounded above by $0.015625 < 1. \implies p$ is decreasing function in number of SBoxes involved in differential trail.

Proposition 4. *Any differential trail on the cipher involves a minimum of 31 SBoxes.*

Proof. □

[1]From Matsui Linear Cryptanalysis

- This would involve a similar proof as the minimum number of SBoxes that get involved in any linear trail.
- Choose a set of input bits as the starting point of the differential trail.
- This would involve atleast one sbox in the first round.
- So, two SBoxes in round 2 would be part of the differential trail. For higher rounds, all *4* SBoxes would be part of the differential trail (reason explained above in *Proposition 2*).
- So, minimum number of SBoxes that would contribute to final propagation ratio

$$= \underbrace{1}_{round1} + \underbrace{2}_{round2} + \underbrace{4 \times 7}_{rounds\,3-9} = 31\diamondsuit.$$

As mentioned earlier, in case of differential cryptanalysis, the total propagation ratio involving n SBoxes is given by $p = p_1 p_2 ....p_n$.

This propagation will be bounded above by p_0^n where p_0 is maximum propagation value of any SBox.

Value of p_0 in our Sboxes is 0.015625.

By *Proposition 4*, n$\geq$31 $\implies$ $p \leq 1.02 \times 10^{-56}$.

$\therefore$ We would require $\mathcal{O}(\frac{1}{p}) \approx 9.80 \times 10^{55}$ chosen plain texts to find target partial key bits of penultimate round which is much higher than $2^{128} \approx 3.40 \times 10^{38}$ key verifications needed in case of a brute force attack.

Remark. So, we proved the security of Sailing Sea Monkey against Linear Cryptanalysis and Differential Cryptanalysis.$\diamondsuit$

Verification of ϵ_0 and p_0 values

Values of ϵ_0 and p_0 for SBoxes have been calculated by enumerating the Linear Approximation Table and Differential Distribution Table.

In order to verify these values use

```
$make maxbias
$make maxpropratio
$./maxbias
e = 0.062500000000000
$./maxpropratio
p = 0.015625000000000
```

Modifications to Previous Submission

We *are* not making any changes to our originally proposed encryption algorithm.