Mysterion-128

[1] Indian Institute of Technology ,Bhilaigadirajusaivenkata@iitbhilai.ac.in
[2] Indian Institute of Technology ,Bhilai, atharvs@iitbhilai.ac.in
[3] Indian Institute of Technology ,Bhilaiashmeshdawande@iitbhilai.ac.in

Contents

Abstract. In this paper we analyze the block cipher mysterion.Mysterion is an instance of XLS-design which is a family of cipher with efficient bitslice implementation against side channel attack.We discuss how combining Super S-boxes with ShiftColumns prevented attacks and gave sufficient security margin to Mysterion through XLS-design. A simple block cipher can still be very much secure against physical attacks.

Keywords: No keywords given.

1 Introduction

The cipher Mysterion has XLS design, that is it contains non-linear bit slice S-boxes and linear diffusion L-boxes along with shift columns operation. The main difference between an LS and XLS design is that XLS design ciphers contain a shift column operation.

Mysterion-128 contains 32 4-bit slice S-boxes and 4 32-bit L boxes based on maximium distance separable(MDS) code.

Then It has ShiftColumn Operation. Then same key is added for each round and at last round constatnt for that round is added.

It has 12 rounds. Also its Security Margin is same as advance encrypted standard(AES) block cipher.

2 Structure Of Mysterion

LS-designs are a family of block ciphers proposed at FSE 2014 with the vision of attaining efficient bitslice implementations. The definition of a-bit S-boxes and b-bit L-boxes directly gives rise to an instance of n = a · b-bit cipher.One advantage of LS-designs is their simplicity.

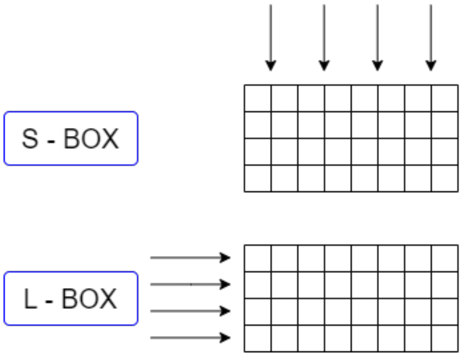


Figure 1: LS-Design

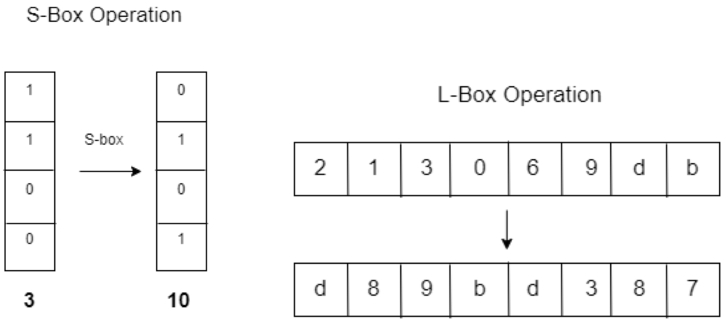


Figure 2: S-box and L-box Operations

The cipher uses the Substitution Permutation Network (SPN) approach and takes 128-bit plaintext as input and key.

But the problem with LS design is that the ciphers which has LS design can be exploited using invarient subspace attack. So we extend LS design and make a XLS-Design which consist of shift columns.It primarily aims to improve the security margins of LS-designs against linear and differential cryptanalysis and invariant subspace attacks.

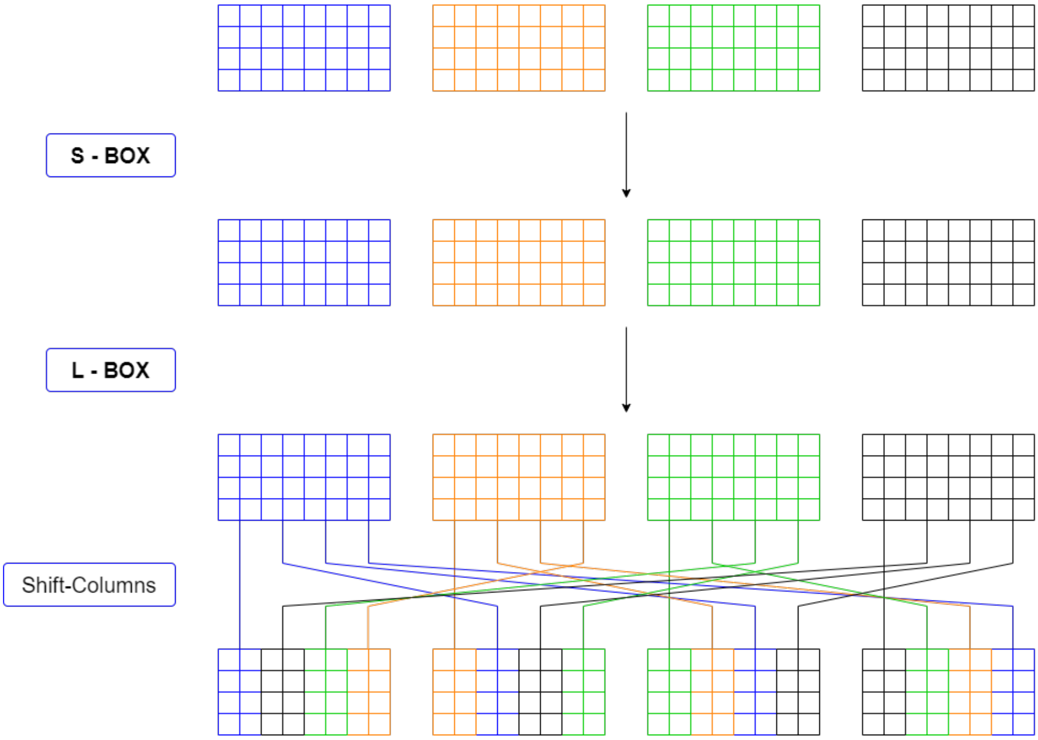
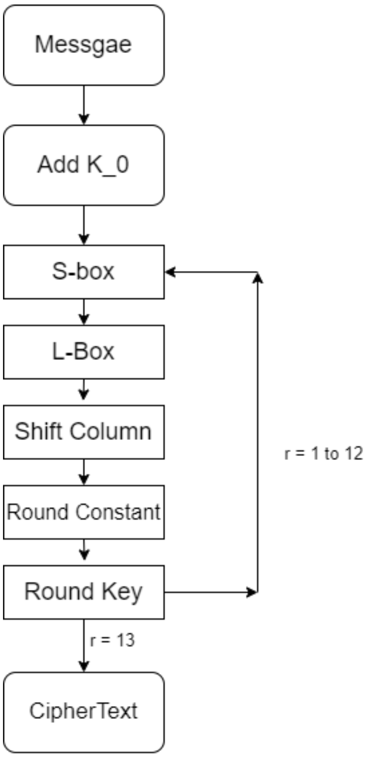


Figure 3: XLS Design



r0.5 Complete Encryption Algorithm.

And Encyption for 12 rounds looks like following:

XLS-design with $l \cdot s$-bit L-boxes, s-bit S-boxes and b blocks

```
$x \leftarrow P \oplus K$
▷$x$ is a s.(l.b) bits matrix

for $0 \leq r < N_r$ do
  for $0 \leq j < b$ do
    for $0 \leq i < l$ do
      $x[j, \star, i] = \mathrm{S}[x[j, \star, i]]$
▷ S-box layer

  for $0 \leq j < b$ do
      $x[j, \star, \star] = \mathrm{L}[x[j, \star, \star]]$
▷ L-box layer

    for $0 \leq k < s$ do
      $x[\star, k, \star] = \mathrm{SC}\ [x[\star, k, \star]]$
▷ ShiftColumns layer

      $x \leftarrow x \oplus K \oplus C(r)$
▷ Key and round constant addition
return $x$
```

3 Components:

3.1 Bitslice S-Box

Mysterion uses has 8 bit slice operation consisiting of AND,XOR and OR gates. Mysterion uses class-13 S box which has 3 AND 1 OR and 4 XOR gates.
input bits :(a_0, a_1, a_2, a_3) output bits :$(b_0, b_1, b_2, b_3) = s(a_0, a_1, a_2, a_3)$
bitwise operations: [s(a_0 and a_1) xor a_2,(b_3 and a_0) xor a_1,(a_1 or a_2) xor a_3,(b_0 and a_3) xor a_0]

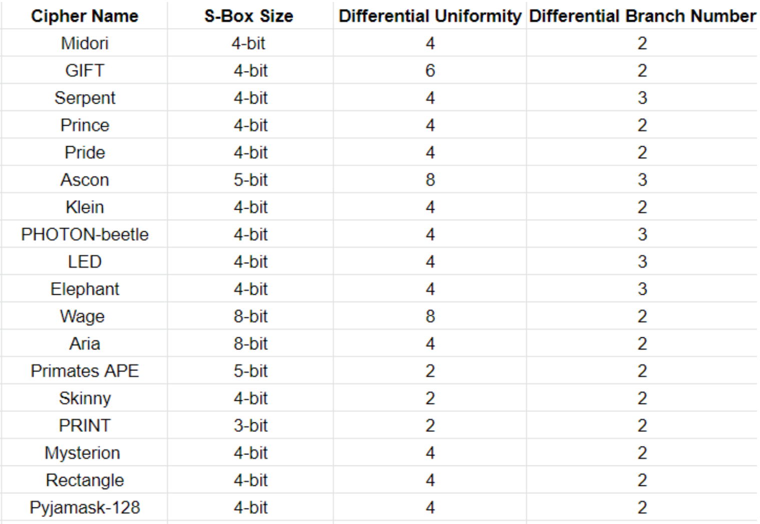
0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	2	a	9	6	4	e	d	1	7	f	8	b	c	3	5

An S-box or a function f is called differentially δ uniform and δ is called the differential uniformity of f if the equation f(x + i) + f(x) = j has at most δ solutions for every nonzero i and every j
The branch number is calculated based on the minimum number of hamming weight sum of input and output in the difference distribution table(DDT) or linearity approximation table (LAT) of the sbox.

3.1.1 DTT

S-box size - 4 bits.
Differential uniformity - 4
Differential branch number- 2.
Maximum Differential probability -4/16=2^{-2}

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



Cipher Name	S-Box Size	Differential Uniformity	Differential Branch Number
Midori	4-bit	4	2
GIFT	4-bit	6	2
Serpent	4-bit	4	3
Prince	4-bit	4	2
Pride	4-bit	4	2
Ascon	5-bit	8	3
Klein	4-bit	4	2
PHOTON-beetle	4-bit	4	3
LED	4-bit	4	3
Elephant	4-bit	4	3
Wage	8-bit	8	2
Aria	8-bit	4	2
Primates APE	5-bit	2	2
Skinny	4-bit	2	2
PRINT	3-bit	2	2
Mysterion	4-bit	4	2
Rectangle	4-bit	4	2
Pyjamask-128	4-bit	4	2

Figure 4: S-box Parameters Comparison

3.1.2 LAT

Linear Branch Number- 2

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	-4	0	2	-2	2	2	2	0	0	4	2	-2	2	2
2	0	2	0	2	0	-2	0	-2	4	2	0	-2	0	2	4	-2
3	0	-2	4	-2	2	0	2	4	0	2	0	-2	-2	0	2	0
4	0	0	0	0	4	4	4	-4	0	0	0	0	0	0	0	0
5	0	0	4	0	-2	2	-2	-2	0	0	4	0	2	-2	2	2
6	0	-2	0	-2	0	2	0	2	4	-2	0	2	4	2	0	-2
7	0	2	4	2	2	-4	2	0	0	-2	0	2	2	0	-2	0
8	0	4	0	-4	0	0	0	0	0	4	0	4	0	0	0	0
9	0	4	0	0	-2	2	2	2	0	-4	0	0	-2	2	2	2
a	0	2	0	2	0	2	0	2	4	2	0	-2	0	-2	-4	2
b	0	-2	0	2	-2	0	2	0	0	2	-4	2	2	0	2	4
c	0	0	0	0	4	0	-4	0	0	0	0	0	0	4	0	4
d	0	0	0	4	2	2	-2	2	0	0	0	4	-2	-2	2	-2
e	0	2	0	2	0	2	0	2	-4	2	0	-2	4	2	0	-2
f	0	-2	0	2	-2	0	2	0	0	2	4	2	-2	4	-2	0

4 L-box

Mysterion L-box uses linear transformation.There is a algorithm which finds recursive MDS diffusion layers using shortened BCH codes. this algorithm takes degree of polynomial k which is the size of companion matrices,and the field size $q = 2^s$ as parameters, and provides all the polynomials of degree k over F_2s such as their companion matrices raised to the power k gives MDS diffusion layers. Selected polynomial, obtained after this is run using Magma code with parameters k = 8 and s = 4, has its coefficients in F_2^4 is P(X) = $X^8 + \alpha^3 * X^7 + \alpha^4 * X^6 + \alpha^12 * X^5 + \alpha^8 * X^4 + \alpha^12 * X^3 + \alpha^4 * X^2 + \alpha^3 * X + 1$. Its differential and linear branch number equal to 9.

L-box's purpose is to diffuse changes in the state.Because of the L-box,difference of some bits will propagate and spread.(see fig 6)

4.1 Shift Column

Shift Column Further Adds the round of confusion by doing permutation on state and for Mysterion Permutation Matrix is as following:
(0,5,10,15,4,9,14,3,8,13,2,7,12,1,6,11)

4.2 Round Constants and Key

There is no key-expansion in Mysterion, same key is used for key-addition in each round, For Mysterion Following Round Constants are used:
(0,1,2,4,8,16,32,64,128,27,54,108,40)

5 Security Analysis

5.1 Invariant Subspace Attack

Let us consider an n-bit iterative block cipher, with round function R_k where, R$_k$: $\mathbb{F}_2^n$X$\mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$,such that $R_k(x) = E(x + k)$, with E as an n-bit permutation. If there exists

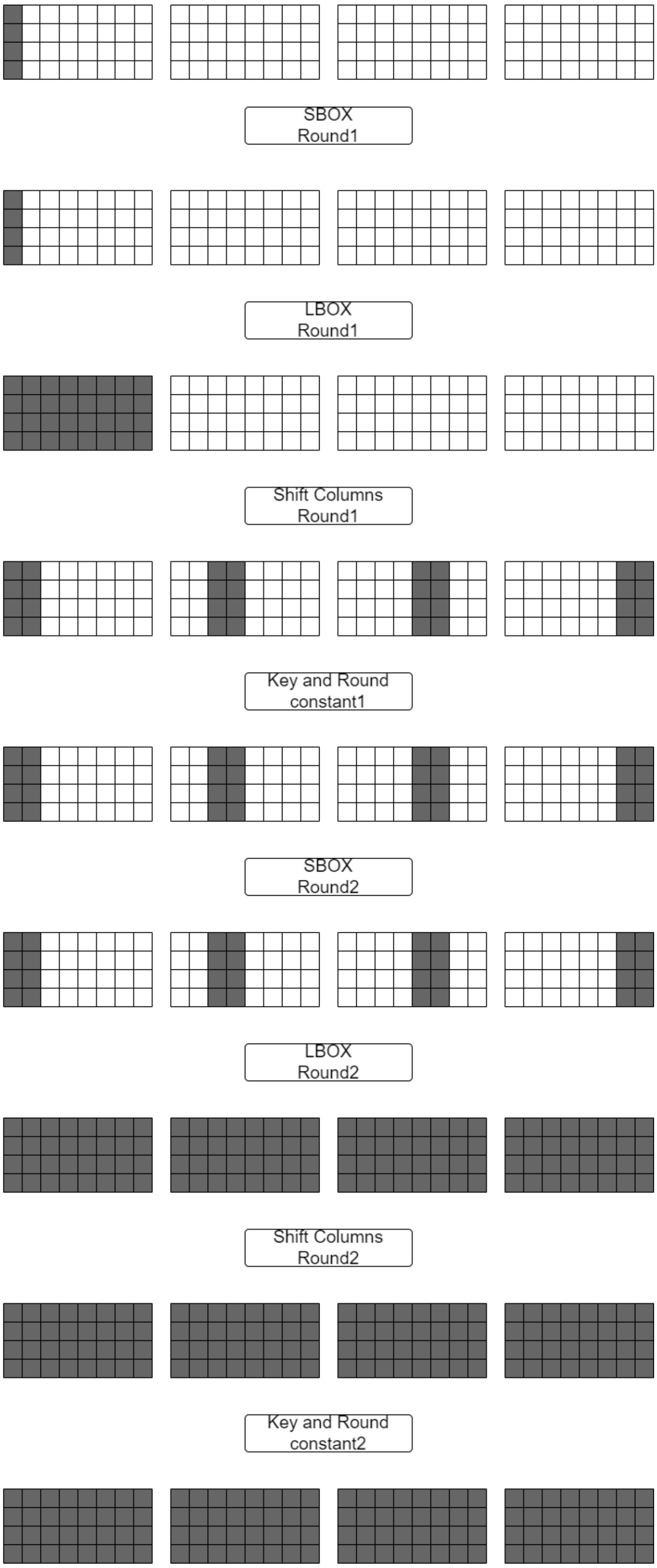


Figure 5: Difference Propagation

a subspace U $\subseteq \mathbb{F}_2^n$ and two constants $c, d \in \mathbb{F}_2^n$ such that $E(U+c) = U+d$, then for a round key $k = u + c + d$ with $u \in U$, the following holds:

$$R_k(U+d) = E((U+d) + (u+c+d)) = E(u+c) = U+d$$

i.e. the round function maps the affine subspace $U + d$ onto itself. If all round keys are in $k \in U + (c+d)$, then this property is iterative over arbitrary number of rounds.
Models from LS Design are susceptible to this attack. This was discovered after a thorough examination of a 32 bit block. This attack can no longer be carried out by introducing the Shift columns operation to LS design models (also known as XLS models). Because the shift columns operation very likely inhibits the subspace discovered for the L-box from propagating. So even with sparse round constants, Mysterion, an XLS design model, may withstand invariant subspace attacks.

5.2 Boomerang Attack

The boomerang attack is a special type of differential cryptanalysis, where the main idea is to divide a cipher E into two sub-ciphers E_0 and E_1 such that $E = E_0 \circ E_1$. The attacker then constructs two relatively short differentials for E_0 and E_1 instead of finding a long differential for the cipher E. This may improve the results since shorter differentials usually have better probabilities. We know from Theorem 1 that four rounds of Mysterion128 has at least 45 active S-boxes. If we use two four-round characteristics for E_0 and E_1, then the best differential probability of a boomerang distinguisher becomes $2^{-45\cdot 2} \cdot 2^{-45\cdot 2} = 2^{-180}$, which is smaller than $2^{-n} = 2^{-128}$. Therefore, we can deduce that any boomerang distinguisher with eight rounds or more will not work against Mysterion-128.

5.3 Integral Attack

For AES, we may discover integral property up to 4 rounds, and depending on the key size, we can mount this attack from 7-9 rounds. However, as Mysterion-128 has 12 rounds, even if we discover integral property for 4 rounds, we still have enough security margin such that cipher can't be broken.

6 Conclusion

Mysterion is Very Strong Cipher, Secure Against Differential and Integral Attacks ,Mainly Due to Higher number of rounds and extra shift column operation than it’s LS Counterparts, it was simple to implement due to it’s simple and straightforward structure and is very fast so can be used for lightweight purposes.

7 References:

1] https://electricdusk.com/mysterion.html
2] https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/sbox.html
3] https://en.wikipedia.org/wiki/Finite-field
4] https://perso.uclouvain.be/fstandae/PUBLIS/157.pdf 5] https://en.wikipedia.org/wiki/MDS-matrix

7.1 Implementation Links:

1] Google Colab:
https://colab.research.google.com/drive/15xyVQ9CFzxwXafe5e3n6qUrdOA7K6jYx?usp=sharing
2]Github:
https://github.com/Ragzz258/Mysterion-128

8 Appendix

8.1 MDS matrix

An MDS matrix (Maximum Distance Separable) is a matrix representing a function with certain diffusion properties that have useful applications in cryptography.
A m x n matrix A over a field K is a MDS matrix if its the transformation matrix of linear transformation $f(x) = A.x$ from K^n to K^m such that no two different (m+n) tupples of the form $(x, f(x))$ coincide in n or more components.
So, the set of $(m + n)$tupples $(x, f(x))$ is a MDS code

8.2 Galois Field

GF(p) is called the prime field of order p, and is the field of residue classes modulo p, where the p elements are denoted 0, 1, ..., p-1. a=b in GF(p) means the same as a=b (mod p). Note, however, that 2×2=0 (mod 4) in the ring of residues modulo 4, so 2 has no reciprocal, and the ring of residues modulo 4 is distinct from the finite field with four elements. Finite fields are therefore denoted GF(p^n), instead of GF(k), where k=p^n