# Mysteries of Mysterion

CrypTrio


Department of <Computer Science>
Indian Institute of Technology Bhilai

November 28, 2020

# Outline

# Introduction

- Block Cipher
- XLS design
- It's security margins is similar with AES cipher
- It has 4-bit S-boxes and 32-bit L-boxes and Shift Columns operation.

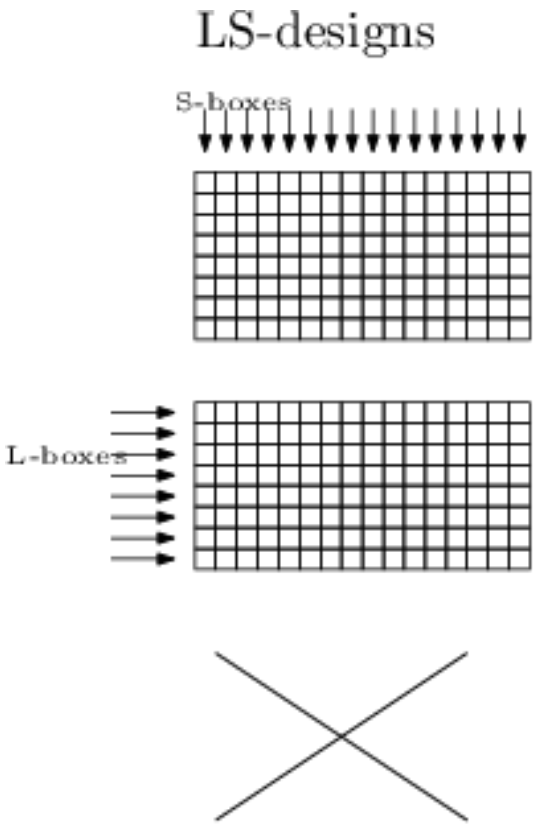
# Bit-Slicing

- Converting the cipher into bit-wise operations (like the way we'd implement it in hardware)
- Carrying out those bit wise operations in parallel

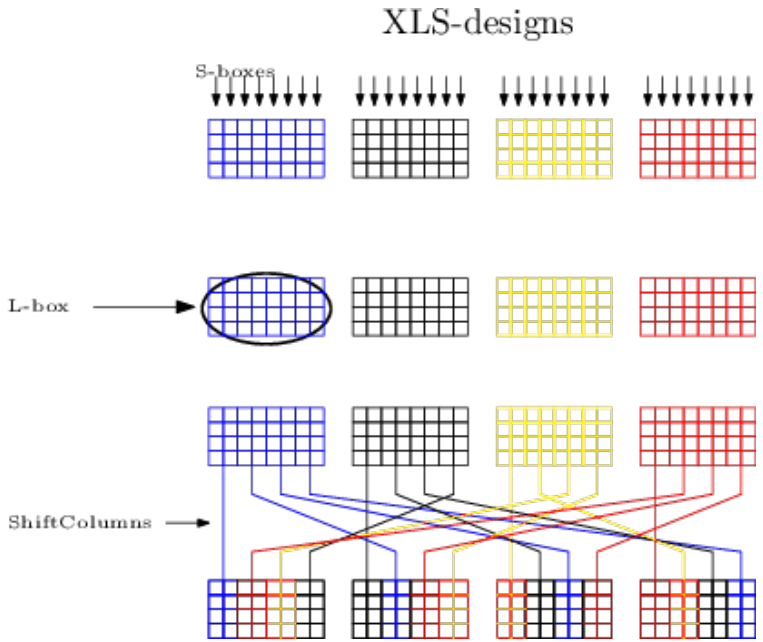
# XLS-Design

- LS Designs are a combination of linear diffusion L-boxes and non-linear bitslice S-boxes.
- These are susceptible to invariant subspace attacks.
- So, XLS (eXtended LS) Designs model is developed by adding the Shiftcolumns operation to LS design models
- XLS-design comprises of SuperS-boxes, made of optimal components - 4-bit S-boxes and 32-bit L-boxes, and ShiftColumns operation.

# LS Design Model



# XLS Design Model



# Outline

# S-box

- Mysterion uses S-boxes that has bitslice representation with a combination of AND (also OR) and XOR gates.
- It has a bitslice representation of 4 AND (precisely 3 AND and 1 OR) gates and 4 XOR gates
- It has a differential probability of $2^{-2}$ and linear probability $2^{-1}$

# DDT & LAT

**Table 1:** DDT of Sbox

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

**Table 2:** LAT of Sbox

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

## Observations

$$\text{Differential probability} = \frac{4}{16} = 2^{-2}$$

$$\text{Linear probability} = \frac{4}{8} = 2^{-1}$$

# L-box

- Its purpose is to diffuse changes in the state.
- linear transformation
- The algorithm which finds recursive MDS diffusion layers using shortened BCH codes from paper []
- When this is run using Magma code paper [] with $k = 8$ and $s = 4$ as input gives polynomials whose companion matrix $C_m$ raised to power 8 $\implies$ $C_m^8$ gives us the MDS matrix

# Shift Columns

- In Mysterion-128, as there are 4 blocks (with each block having 8 columns) ShiftColumns acts on columns two by two.
- In Mysterion-256 as there are 8 blocks (with each block having 8 columns) ShiftColumns acts on columns one by one

# Diagrams

Figure: Shift Columns-128

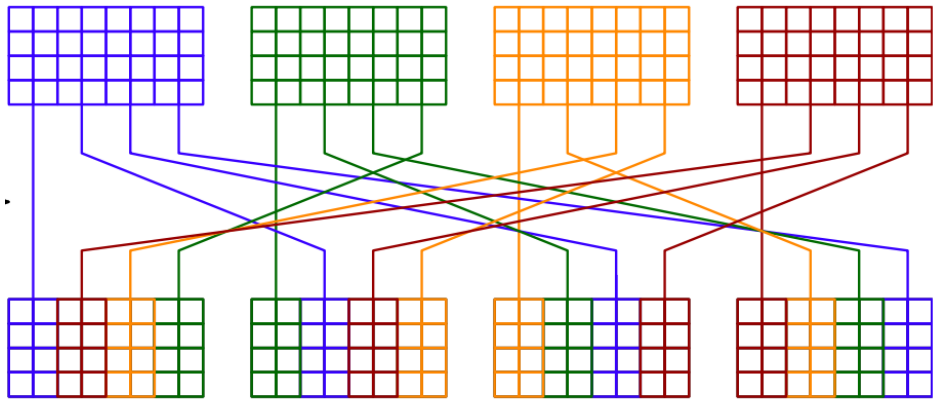
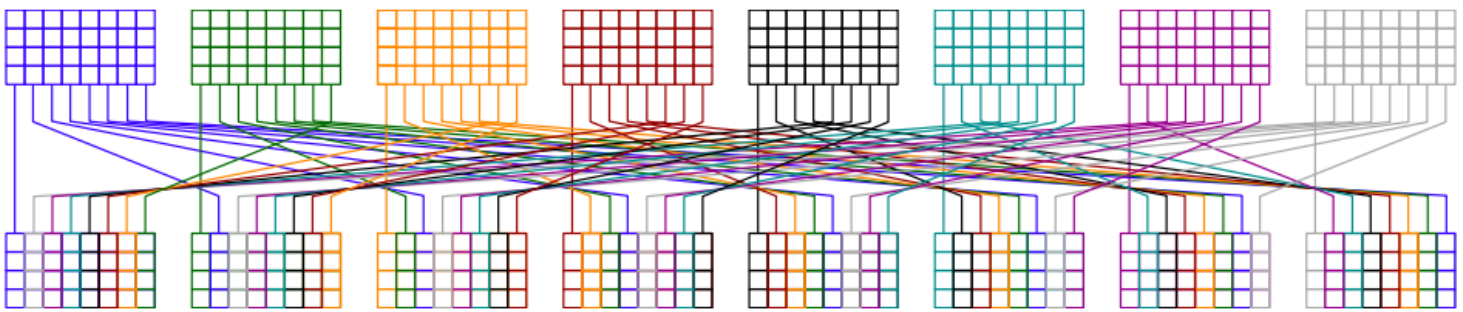


Figure: Shift Columns-256



# Round constant and Key

- Up until now, we have done nothing to make the ciphertext dependent on the key. So to do this, we add the key to the state.
- The Mysterion block cipher has no key schedule. In every round, the same key is added to the state.

# Outline

# Boomerang Attack

- Special Differential Cryptanalysis
- two differentials for the two sub ciphers $C_0$ and $C_1$ obtained from cipher $C$
- $C = C_0 \circ C_1$
- shorter differentials have more better probabilities $\Longrightarrow$ improved results

## Theorems

**Theorem 1:** Four rounds of Mysterion-128 has at least 45 active S-boxes.

**Theorem 2:** Four rounds of Mysterion-256 has at least 81 active S-boxes.

# Boomerang Attack

1. For 128 bit :
   We use the Theorem 1 to find the max differential prob that can be obtained :

$$\Pr_{diff}(4R) \leq \Pr_{diff}^{max}(Sbox)^{45} = (2^{-2})^{45} = 2^{-90}$$

$$\implies \Pr_{diff}^{max}(8R) = \Pr_{diff}(4R) * \Pr_{diff}(4R) = 2^{-90} * 2^{-90} = 2^{-180}$$

   the Pr obtained is way less that brute force probability ($2^{-128}$).

# Boomerang Attack

1. For 256 bit:
   We use the Theorem 2 to find the max differential prob that can be obtained :

   $$\Pr_{diff}^{max}(8R) = \Pr_{diff}(4R) * \Pr_{diff}(4R) = 2^{-81*2} * 2^{-81*2} = 2^{-324}$$

   the Pr obtained is way less that brute force probability ($2^{-256}$).

# Integral Attack

- Integral attacks tries to extract information about the key by observing the sum of ciphertext values.
- We may find integral property upto 4 rounds, and then we can mount this attack from 7-9 rounds depending on the key size.
- Sufficient security margin for the full cipher, since there are 12 and 16 rounds for Mysterion -128 and Mysterion-256.

**Division Property - EUROCRYPT 2015** It allows to construct more efficient integral distinguishers exploiting the limited algebraic degree of reduced ciphers.

# Invariant subspace Attack

- LS Design models are vulnerable to this attack
- This was identified by performing an exhaustive analysis on a 32 bit block
- Addition of Shiftcolumns operation to LS design models (which are called as XLS models) ,this attack can no longer be done
- Shiftcolumns operation prevents the propagation of subspace found for the L-box with high probability

# Outline

# Juypter Notebook & Online tool

1. Juypter Notebook
   1. Fully interactive
   2. Complete Mysterion-128 implementation
   3. Inverse of Mysterion-128 implemented
   4. Implemented Inverse of sbox, Ibox and shift columns-128 and 256
   5. DDT and LAT analysis
   6. Example run of all functions used
2. Hosted first ever Mysterion online tool at :
   `https://mysterion-tool.herokuapp.com/`

# Outline

# Simple yet Secure

- Simple heuristics
- Security margin for physical attacks
- Efficient XLS-design

# Links

- Implementation Source Code Link:
  `https://github.com/Meghana-12/Mysterion`
- Google Collab Link:
  `https://colab.research.google.com/drive/1bmUl7wT4U13XY6n8cB2sV-f5cAsr0_vV?usp=sharing`
- Online Tool Link:
  `https://mysterion-tool.herokuapp.com/`
- Online Tool Source code:
  `https://github.com/RotonEvan/mysterious-ions`

# Thanks

## Team Members

- Gundu Shreya
- Varanasi Meghana
- Debajyoti Halder