# Cryptanalysis of mCrypton

<Team Mitnick>

Department of <Computer Science Engineering>
Indian Institute of Technology Bhilai

November 28, 2020

# Outline

# Introduction

**Increasing demand of resource-constrained and compact devices**

1.Low consumption of power
2.Compact size
3.Security for data exchanges

# Introduction to light weight Cryptography

→ As the demand increased, to solve the problems and make things easy lightweight cryptography came into action.
→ There are multiple ciphers in the market are introduced such as SEA, PRESENT, mCrypton, KATAN, etc.
→ mCrypton is one of the best devices overall and its hardware complexity stands at the top of the chain.

# Introduction

**Short details of mCrypton:**

1.It name refers as miniature of Crypton
2.It is a 64-bit block cipher which is also an SPN network with 12 rounds
3.It is available in three key sizes 64, 96, 128 bits for minimal, moderate, standard Securities, respectively.

# Some areas in usage of RFID tags

1.Medical
2.logistics
3.Maintenance
4.Railways

# Introduction

**Some attacks on mCrypton:**

1.Biclique Cryptanalysis
2.Related-key Rectangle attack
3.Related-key impossible differential attack
4.Collision attacks

# Outline

# Specs of mCrypton

## Properties of Cipher

$\rightarrow$ mCrypton is a SPN based block cipher.
$\rightarrow$ mCrypton is a 64-bit block cipher.
$\rightarrow$ It has three Key sizes 64, 96, 128.
$\rightarrow$ The input message for encryption is in the form of 4x4 matrix.

# S-box of mCrypton

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $S_0(x)$ | 4 | $f$ | 3 | 8 | $d$ | $a$ | $c$ | 0 | $b$ | 5 | 7 | $e$ | 2 | 6 | 1 | 9 |
| $S_1(x)$ | 1 | $c$ | 7 | $a$ | 6 | $d$ | 5 | 3 | $f$ | $b$ | 2 | 0 | 8 | 4 | 9 | $e$ |
| $S_2(x)$ | 7 | $e$ | $c$ | 2 | 0 | 9 | $d$ | $a$ | 3 | $f$ | 5 | 8 | 6 | 4 | $b$ | 1 |
| $S_3(x)$ | $b$ | 0 | $a$ | 7 | $d$ | 6 | 4 | 2 | $c$ | $e$ | 3 | 9 | 1 | 5 | $f$ | 8 |

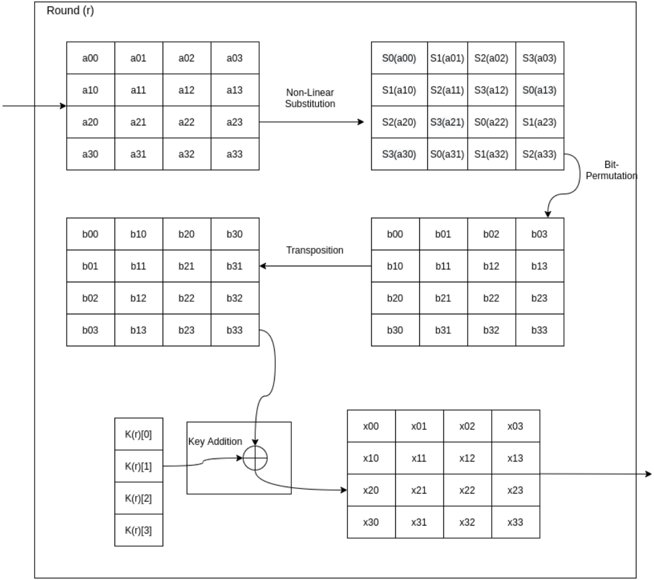
# Encryption Algorithm of mCrypton

→ There are 12 rounds in mCrypton

**There are four major transformations in each round:**

1.Nonlinear substitution $\gamma$
2.Bit permutation $\pi$
3.Column-to-row transposition $\tau$
4.Key addition $\sigma$

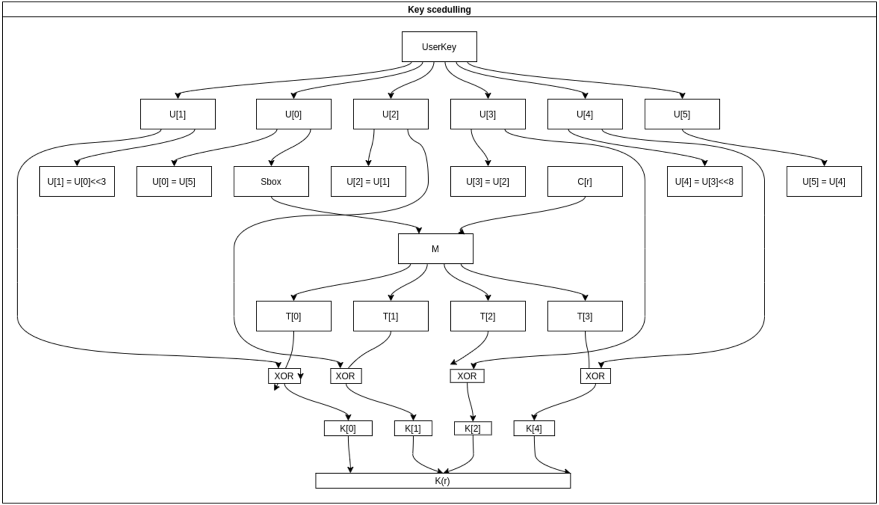
# Pictorial representation of a single round



# Key-scheduling

- Initially we should give a user key, U.
  U = ( U[0], U[1], U[2], U[3], U[4], U[5])
- $T \leftarrow S(U[0]) \oplus C[r]$, $T_i \leftarrow T \bullet M_i$ (S(U[0]) is nibble wise sbox substitution)
  $i = 0, 1, 2, 3$, $M_0$ =0xf000, $M_1$ =0x0f00, $M_2$ =0x00f0, $M_3$ =0x000f
- $K_r \leftarrow (U[1] \oplus T_0, U[2] \oplus T_1, U[3] \oplus T_2, U[4] \oplus T_3)$,
- $U \leftarrow (U[5], U[0]^{<<3}, U[1], U[2], U[3]^{<<8}, U[4])$ ($^{<<3}$ denotes bits are left rotated by 3 places)

# Pictorial representation of Key Scheduling



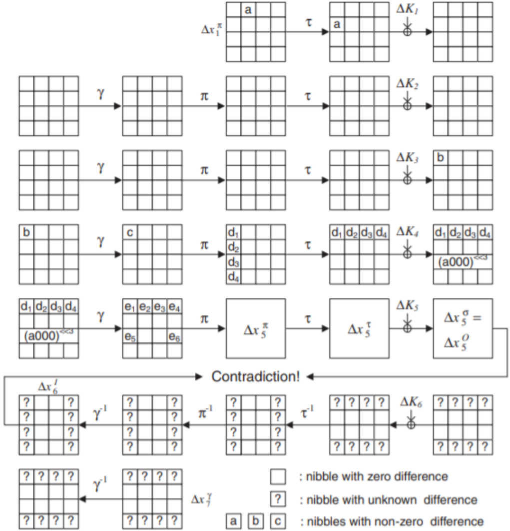
# Outline

# Various attacks on mcrypton

**I mentioned 4 attacks. In which, I will explain more about the related-key impossible differential attack**

1.Short note on Related-key impossible differential attack
2.In this attack, we are going to analyse on 6-round and 9-round mCrypton-96.
3.The attack procedure is similar for 6-round and 9-round mCrypton-128

# Pictorial representation of 6-round related-key differential on mcrypton-96



# 6-round related-key differential on mcrypton-96

## 6-round related-key differential

Assume the two related key differences to be;

$\Delta$ K = K $\oplus$ $K^1$ = $(0000|0000|0000|a000|0000|0000)$

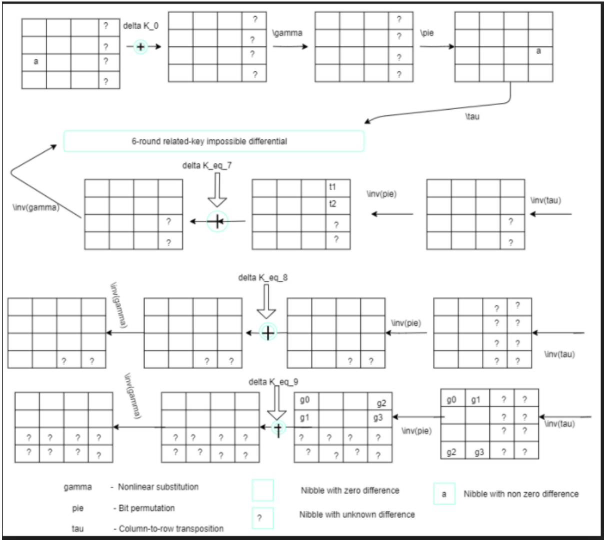
1. A 4.5-round related key differential
2. A 1.5-round related key differential

# Table 1:Sub Key Differences of 9 rounds

| Round$(i)$ | $\delta K_(i, row(0))$ | $\delta K_(i, row(1))$ | $\delta K_(i, row(2))$ | $\delta K_(i, row(3))$ |
|---|---|---|---|---|
| 0 | $(0000)$ | $(0000)$ | $(a000)$ | $(0000)$ |
| 1 | $(0000)$ | $(0000)$ | $(0000)$ | $(00a\ 0)$ |
| 2 | $(0000)$ | $(0000)$ | $(0000)$ | $(0000)$ |
| 3 | $(0000)$ | $(0000)$ | $(00b0)$ | $(0000)$ |
| 4 | $(a000^{<<11})$ | $(0000)$ | $(0000)$ | $(0000)$ |
| 5 | $(0000)$ | $(a000^{<<11})$ | $(0000)$ | $(0000)$ |
| 6 | $(0000)$ | $(0000)$ | $(a000^{<<11})$ | $(0000)$ |
| 7 | $(0000)$ | $(0000)$ | $(0000)$ | $(a000^{<<3})$ |
| 8 | $(0000)$ | $(0000)$ | $(0000)$ | $(0000)$ |
| 9 | $(b'000)$ | $(0000)$ | $(0000)$ | $(000b'')$ |

$a$, $b$ and at least one of $b'$ and $b''$ are non-zero nibble differences.

# Pictorial representation of 9-round related-key impossible differential attack on mcrypton-96



# 9-round related-key impossible differential attack on mcrypton-128

- Using the 6-round distinguisher from the previous slides, we present a related-key impossible differential attack on 9-round mCrypton-96.
- To reduce Time complexity, in rounds 7-9 we changed the order from $\sigma$, $\tau$, $\pi$ to $\tau$, $\pi$, $\sigma$.
- Due to change in order, $K_i$ key of ith round changes, as its equivalent key($k_i^{eq}$) is $\pi(\tau(k_i))$.
- In this we use 16 related-keys $K^0$,...,$K^{15}$, having a relation $K_i \oplus K_j = (0000|0000|0000(i \oplus j)000|0000|0000)$

# 9-round related-key impossible differential attack on mcrypton-128

- The attacker can choose the value of a, values of b' and b" in round 9 are from s-boxes which are unknown.
- The attack is briefly explained in the term paper

# Complexity of the attack

There are a total of 7 steps in calculating the complexity which are explained in the term paper. Following are the complexities involved in the 7 steps:

- step 1: $2^{n+20} = 2^{59.9}$
- step 2: $1/8 \times 2^{n+19} \times (4x64 + 8) \approx 2^{63.9}$
- step 3: $2^{n+11}x2^{8} = 2^{58.9}$
- step 4: $2 \times 1/9 \times 1/4 \times 2^{n+11} \times 2^{8+16} \approx 2^{70.7}$
- step 5: $2 \times 1/9 \times 1/4 \times 2^{n-1} \times 2^{24+16} \approx 2^{74.7}$
- step 6: $2 \times 1/9 \times 1/4 \times 2^{n-13} \times 2^{40+8} \approx 2^{70.7}$
- step 7: $2 \times 2^{n-19.4} \times 2^{48} = 2^{69.5}$

# Complexity of the attack

- In the 7 steps, step 4, 5, 6 are dominant part of the time complexity as the total complexity will be the sum of these 3 steps.
  $2^{70.7} + 2^{74.7} + 2^{70.7} \approx 2^{74.9}$ encryptions.
- The memory required for step 2 is dominant over all other steps as it is $2^{74.7}$
- The above attack procedure is similar for mCrypton-128.

# Outline

# Brownie points

- Visualizations like Encryption algorithm and Key Scheduling were added for better understanding
- Secure against differential and linear cryptanalysis
- Properties like S-box and Bit-permutation are analyzed
- It has a better hardware architecture than most of the other lightweight cryptography

# Outline

# Conclusion

- Lightweight cryptography
- Advantages of Lightweight Cryptography
- Encryption Algorithm of mCrypton
- Various attacks on mCrypton
- Explained the related-key impossible differentiable attack on 6-round and 9-round mCrypton-96
- Complexities of the related-key impossible differential attack
- Explained Uniqueness of mCrypton over other lightweight cryptographic ciphers

# Thanking You

## Team Members

- Tumma Manohar Sai, 11841170
- Goolla Abhijith, 11840510
- Anugu Rakesh Reddy, 11840200

## Implementation Info

- Github Link:
  github.com/Manohar-Sai/mCrypton—lightweight-block-cipher