Mischief in the Cube: A Study of the Saturnin

Kriti Arora 12240880

IIT Bhilai

Table of Contents

Saturnin Basics

Saturnin Cipher Basics

- **Saturnin** is a symmetric block cipher designed with post-quantum security and lightweightness in mind.
- Key features:
  - **256-bit state** and **256-bit key**.
  - Lightweight design suitable implemented using bitsliced operations.
  - Structured similarly to AES, but uses a 3D 4x4x4 nibble cube state.

Post Quantum Motivation

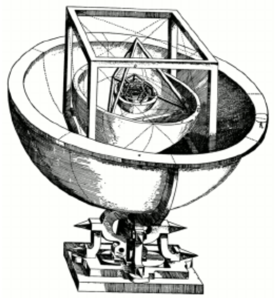
Why Post-Quantum Ciphers?

- Quantum algorithms such as **Shor's algorithm** threaten asymmetric schemes (RSA, ECC).
- Symmetric ciphers are more resistant, but:
  - Grover's algorithm reduces brute-force cost from 2^n to $2^{n/2}$.
  - Hence, to maintain $\sim 2^{128}$ security, block ciphers need **at least 256-bit keys/states**.
- Research into lightweight, quantum-safe symmetric ciphers is therefore ongoing.

Why the name Saturnin?

Why the name Saturnin? Saturnin the Duck. The duck is undeniably a symbol of lightness because it floats. It has been famously used as the reference for lightness throughout the ages. Saturnin the duck is the most famous duck in France.

Kepler found the distance between the five known planets to be calculated by inscribing each Platonic solid inside a sphere. And saturn got associated with the cube.



(b) From Kepler's *Mysterium Cosmographicum*, via Wikipedia.

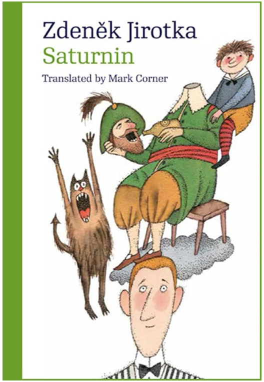
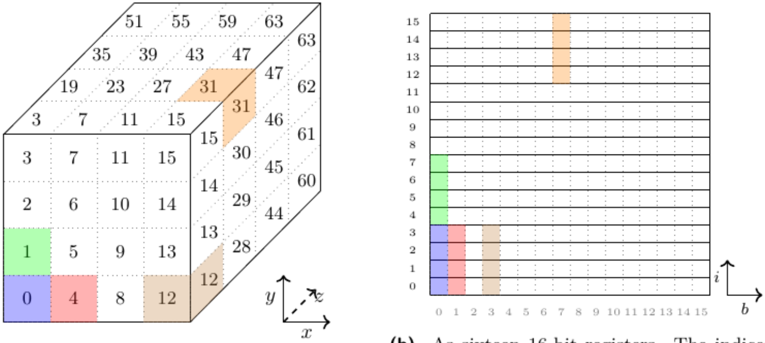


Table of Contents

Saturnin State structure

Saturnin block and register state



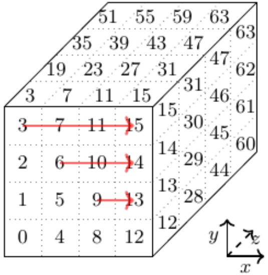
(a) As a $4 \times 4 \times 4$ cube of 4-bit nibbles. The boundaries between the nibbles are in gray.

(b) As sixteen 16-bit registers. The indices and boundaries of the registers are in black, those of the bits are in gray.

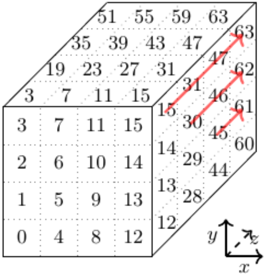
Figure 1: The two representations of the 256-bit state of SATURNIN. Nibbles and their corresponding bits are represented with the same color in each representation.

Terms and Definitions

- Slice: putting the z axis constant
- Sheet: putting the x axis constant
- Column: putting the x and z as constant



(a) $\mathsf{SR}_{\text{slice}}$ (when $r \equiv 1 \bmod 4$)



(b) $\mathsf{SR}_{\text{sheet}}$ (when $r \equiv 3 \bmod 4$)

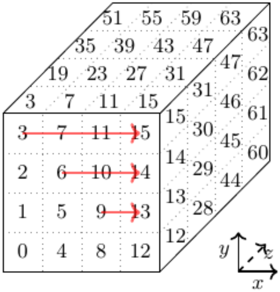
One round of Saturnin

Sbox

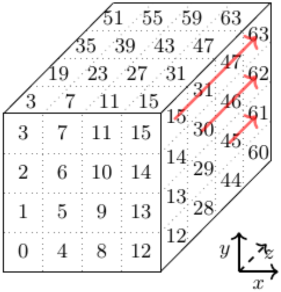
Table 1: The lookup tables of the S-boxes we use.

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\sigma_0(x)$	0	6	14	1	15	4	7	13	9	8	12	5	2	10	3	11
$\sigma_1(x)$	0	9	13	2	15	1	11	7	6	4	5	3	8	12	10	14

Permutation



(a) SR_{slice} (when $r \equiv 1 \bmod 4$)



(b) SR_{sheet} (when $r \equiv 3 \bmod 4$)

Permutation

Initial state:

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

19	23	27	31
18	22	26	30
17	21	25	29
16	20	24	28

35	39	43	47
34	38	42	46
33	37	41	45
32	36	40	44

51	55	59	63
50	54	58	62
49	53	57	61
48	52	56	60

Internal state after SR_r at Rounds r with $r \equiv 1 \bmod 4$, i.e. after $\mathsf{SR}_{\text{slice}}$:

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

23	27	31	19
26	30	18	22
29	17	21	25
16	20	24	28

39	43	47	35
42	46	34	38
45	33	37	41
32	36	40	44

39	43	47	35
42	46	34	38
45	33	37	41
32	36	40	44

Permutation

Initial state:

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

19	23	27	31
18	22	26	30
17	21	25	29
16	20	24	28

35	39	43	47
34	38	42	46
33	37	41	45
32	36	40	44

51	55	59	63
50	54	58	62
49	53	57	61
48	52	56	60

Internal state after SR_r at Rounds r with $r \equiv 3 \bmod 4$, i.e. after $\mathsf{SR}_{\text{sheet}}$:

19	23	27	31
34	38	42	46
49	53	57	61
0	4	8	12

35	39	43	47
50	54	58	62
1	5	9	13
16	20	24	28

51	55	59	63
2	6	10	14
17	21	25	29
32	36	40	44

3	7	11	15
18	22	26	30
33	37	41	45
48	52	56	60

Mixed Columns

$$M : \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \mapsto \begin{pmatrix} \alpha^2(a) \oplus \alpha^2(b) \oplus \alpha(b) \oplus c \oplus d \\ a \oplus \alpha(b) \oplus b \oplus \alpha^2(c) \oplus c \oplus \alpha^2(d) \oplus \alpha(d) \oplus d \\ a \oplus b \oplus \alpha^2(c) \oplus \alpha^2(d) \oplus \alpha(d) \\ \alpha^2(a) \oplus a \oplus \alpha^2(b) \oplus \alpha(b) \oplus b \oplus c \oplus \alpha(d) \oplus d \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} .$$

Round function of Saturnin

- One super-round is defined as two round 2r and 2r+1
- Each round consists of the following transformations:
  1. **S-box layer (S):** Apply σ_0 to even-index nibbles and σ_1 to odd-index nibbles.
  2. **Permutation ($\mathbf{SR}_r$):**
     - Even rounds: Identity
     - Odd rounds, $r \bmod 4 = 1$: $\mathrm{SR}_{\mathrm{slice}}$ (mixes inside slices)
     - Odd rounds, $r \bmod 4 = 3$: $\mathrm{SR}_{\mathrm{sheet}}$ (mixes inside sheets)
  3. **Linear layer (MC):** Apply 4x4 MDS matrix on each column.
  4. **Inverse permutation ($\mathbf{SR}_r^{-1}$):** Undo the SR_r applied earlier.
  5. **Subkey addition:** At the end of each super-round (odd rounds), XOR with round key + round constant.

Table of Contents

Saturnin Security

- Security wise: 1 super round of Saturnin = 1 round of AES
- Therefore, the number of rounds is 20 or 2*10(AES)

Table of Contents

State Representation

- State $=$ 256 bits, represented as 16 words of 16 bits.
- Arranged as a 4×4 matrix:

$$\begin{bmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{bmatrix}$$

- Round functions operate on this structure.

ShiftRow

- Alternate between two permutations:
  - **ShiftRowSheet (even rounds)**
  - **ShiftRowSlice (odd rounds)**

```
rotate_left(&s[4], 1);
rotate_left(&s[8], 2);
rotate_left(&s[12], 3);
```

MDS Diffusion Layer

- State split into 4 groups: A, B, C, D.
- Operation sequence:
  1. $C \leftarrow C \oplus D$
  2. $A \leftarrow A \oplus B$
  3. Apply MUL rotation on B and D.
  4. Cross XOR again: $B \leftarrow B \oplus C$, $D \leftarrow D \oplus A$.
  5. Apply MUL twice on A and C.
- Guarantees **maximum diffusion** (MDS property).

Round Constants

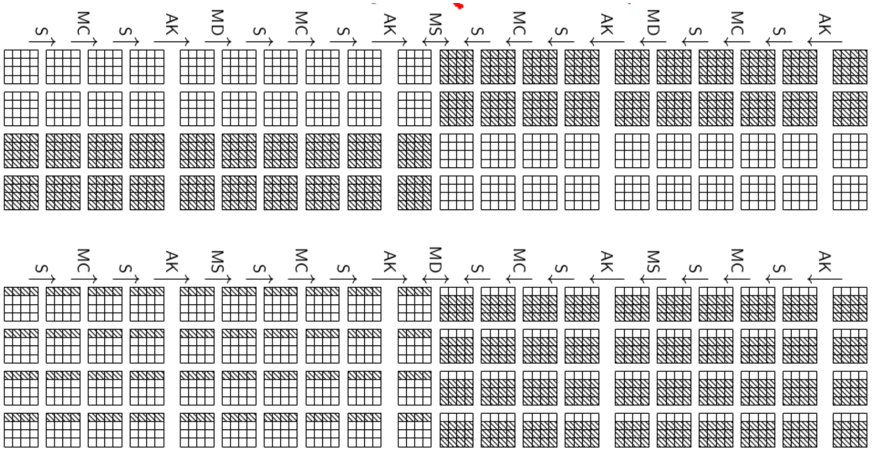
- Two constants RC0, RC1 added each round.
- Generated using an 8-bit LFSR.
- Breaks symmetry and prevents slide attacks.

```
static uint8_t lfsr(uint8_t x) {
    return (x << 1) ^ (0x1B & -(x >> 7));
}

// each round
RC0 = lfsr(RC0);
RC1 = lfsr(RC1);
state[0] ^= RC0;
state[4] ^= RC1;
```

Table of Contents

Two impossible Differential Trails



Differential Trail 1

- Its a 4 round Impossible Differential, meeting in the middle.
- Starts with a small number of active nibbles in the state.
- We start from the left from the top and the MD step which has SR slice diffuses the sboxes only in the slice
- Hence when we start from the bottom, the trail doesnt match with each other.
- So the first round starts from even then $x\%4 = 1$ so 4 5 6 7, becuase we are using SR slice.

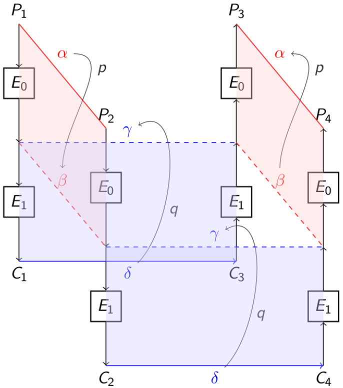
Differential Trail 2

- Starts with a small number of active nibbles in the state.
- We start from the left from the top and here the MS step diffuses differences across sheets.
- When traced from the bottom, the activity propagates differently — this time the trail aligns better due to stronger diffusion.
- So the first round starts from even then $x\%4 = 3$ so 2 3 4 5, because we are using SR sheet.

Table of Contents

Boomerang Attack — Overview

Goal: Combine two short differential characteristics to build a longer, high-probability distinguisher.



Probability of distinguisher: p^2q^2

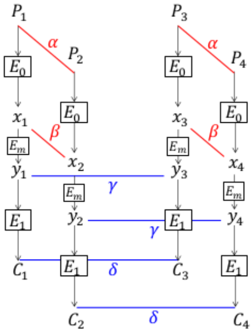


Fig. 2. Sandwich attack

BCT of Even and Odd S-boxes

σ_0 (Boomerang Connectivity Table):

a\b	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	6	0	2	2	0	4	6	0	0	0	0	0	0	2	2
2	16	0	4	2	0	2	2	2	6	0	4	0	0	0	0	2
3	16	2	0	4	2	2	2	0	2	4	4	0	0	0	2	0
4	16	0	0	0	4	2	0	2	6	2	0	0	6	0	0	2
5	16	0	2	4	0	0	0	2	2	6	6	0	0	0	2	0
6	16	6	2	0	0	0	8	4	0	0	0	4	0	6	2	0
7	16	6	0	0	0	2	4	4	0	0	6	4	6	6	0	2
8	16	6	2	0	6	0	0	2	4	0	0	0	8	4	0	0
9	16	4	2	2	0	0	4	0	0	0	4	8	0	4	2	2
A	16	0	0	2	0	2	2	2	0	0	0	2	0	2	2	2
B	16	2	0	4	2	2	2	0	0	4	4	2	0	2	0	0
C	16	0	4	0	6	2	0	0	8	0	6	2	4	0	0	0
D	16	0	2	4	2	0	0	0	0	4	4	2	2	0	2	2
E	16	4	4	8	0	0	0	0	4	10	10	4	2	0	0	2
F	16	4	2	0	0	2	4	0	0	2	0	4	4	8	2	0

Even S-box BCT

σ_1 (Boomerang Connectivity Table):

a\b	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	6	6	4	0	0	0	4	0	0	0	4	10	4	4	6
2	16	4	0	0	0	0	6	6	4	6	0	2	0	2	6	4
3	16	0	4	0	0	8	2	6	0	0	6	2	0	0	0	4
4	16	8	2	0	0	0	2	0	6	4	0	0	6	4	0	0
5	16	4	0	4	0	0	0	0	0	2	2	0	4	10	6	0
6	16	6	0	6	2	0	2	0	8	4	0	4	0	0	0	0
7	16	0	0	6	10	0	0	4	2	0	4	0	0	0	4	2
8	16	0	0	0	4	6	2	0	0	0	8	0	0	2	6	4
9	16	2	0	0	0	2	4	0	2	6	2	0	0	0	0	6
A	16	0	0	10	6	0	0	4	6	0	0	4	4	4	4	6
B	16	0	2	6	2	4	6	0	0	4	4	0	6	0	0	6
C	16	0	0	4	0	2	0	6	4	2	0	10	4	0	0	0
D	16	0	4	4	4	6	0	10	0	6	0	6	4	0	4	0
E	16	2	10	0	0	4	0	4	0	0	0	0	6	0	4	2
F	16	0	4	4	4	0	0	4	0	6	6	0	4	6	10	0

Odd S-box BCT

DDT of Saturnin S-box

DDT[dx][dy] = count where S(x) ⊕ S(x ⊕ dx) = dy

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

Top Performing Pairs

Top 5 Boomerang Pairs

α (Input Δ)	δ (Output ∇)
E	A
E	9

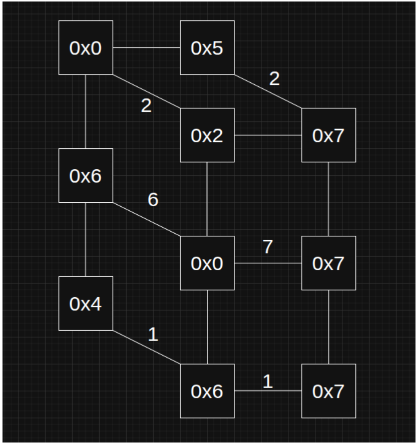
- Multiple pairs reach the same high probability of 10/16.

Detailed View: Best Pair

Boomerang Pair

P_1	P_2	C_1	C_2	C_3	C_4	P_3	P_4	$P_3 \oplus P_4$
0	2	4	6	5	7	5	7	2

Trail using just the Sbox



Incompatibility: DDT Pair Analysis

Parameters: $\Delta = 0x1$, $\beta = 0x3$

x	**x'**	**y**	**y'**
0x6	0x7	0x4	0x7
0x7	0x6	0x7	0x4

Total DDT pairs: 2

BCT Pair Analysis and Overlap Check

Parameters: $\Delta = 0x1$, $\nabla = 0x1$

x	x'	y	y'
0x0	0x1	0x6	0x9
0x1	0x0	0x9	0x6
0x8	0x9	0xB	0xD
0x9	0x8	0xD	0xB
0xE	0xF	0xC	0xA
0xF	0xE	0xA	0xC

Total BCT pairs: 6

Overlap Check:

DDT x values: [0x6, 0x7]
BCT x values: [0x0, 0x1, 0x8, 0x9, 0xE, 0xF]
Overlap: None

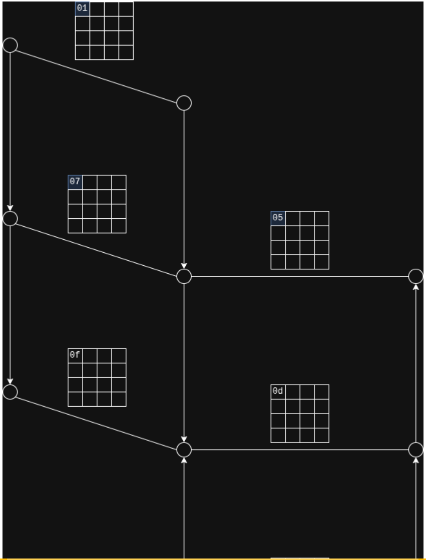
Inference:
The DDT and BCT input pairs are disjoint, showing no overlap in input differences.

Compatible Boomerang Trail Found

Key Parameters:

- Active nibble (top): 4
- Active nibble (bottom): 4
- p_1 nibble: 0x0
- Δ_{in}: 0x1
- Δ_{bottom}: 0x2
- Δ_{out}: 0x5
- $BCT[0x1][0x5] = 5$

Trail diagram



Probability p

Differential Probabilities:

- $P(\Delta_{in} = 0x1 \rightarrow \Delta_{out} = 0x7) = \frac{1}{8}$
- $P(\nabla_{in} = 0x2 \rightarrow \nabla_{out} = 0x7) = \frac{1}{8}$

Boomerang Probability:

$$P_B = P^2 \times Q^2 = \left(\frac{1}{8}\right)^2 \times \left(\frac{1}{8}\right)^2 = \frac{1}{4096}$$

Table of Contents

Q&A

Thank You!

I will now be taking questions.