Mischief in the Cube: A Study of the Saturnin

Kriti Arora 12240880

IIT Bhilai

Table of Contents

1. Introduction to Saturnin
   - Saturnin Basics
   - Post Quantum Motivation
   - Why the name Saturnin?
2. Saturnin
   - Saturnin State structure
   - One round of Saturnin
3. Security
4. Summing Up

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

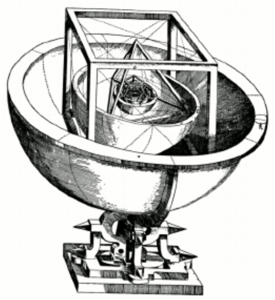
Why Post-Quantum Ciphers?

- 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.

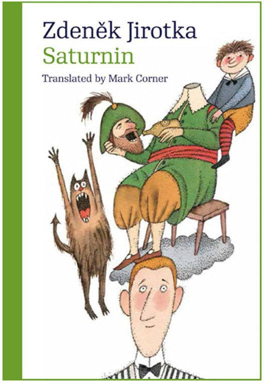
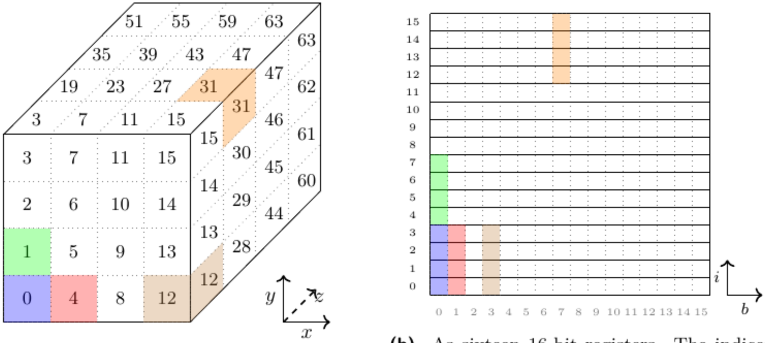


Table of Contents

1. Introduction to Saturnin
   - Saturnin Basics
   - Post Quantum Motivation
   - Why the name Saturnin?
2. Saturnin
   - Saturnin State structure
   - One round of Saturnin
3. Security
4. Summing Up

Saturnin State structure

Saturnin block and register state



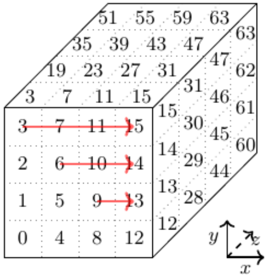
(a) As a 4 × 4 × 4 cube of 4-bit nibbles. The boundaries between the nibbles are in gray.

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

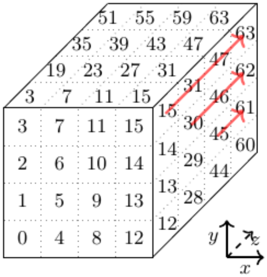
Figure 1: The two representations of the 256-bit state of Saturnin. Nibbles and their corresponding bits are represented with the same color in each representation.

Terms and Definitions

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



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



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

One round of Saturnin

Sbox

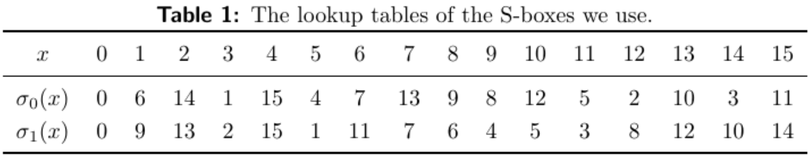
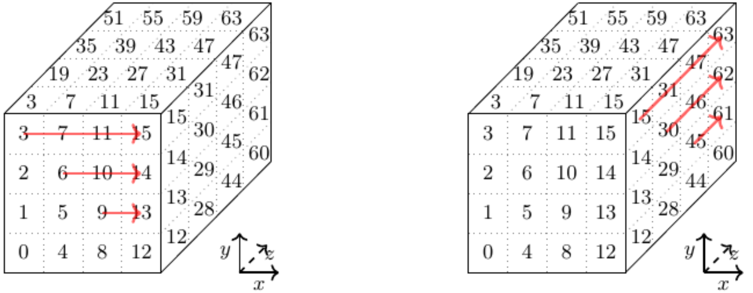


Table 1: The lookup tables of the S-boxes we use.

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) $\mathrm{SR}_{\mathrm{slice}}$ (when $r \equiv 1 \bmod 4$)

(b) $\mathrm{SR}_{\mathrm{sheet}}$ (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

1 Introduction to Saturnin
- Saturnin Basics
- Post Quantum Motivation
- Why the name Saturnin?

2 Saturnin
- Saturnin State structure
- One round of Saturnin

3 Security

4 Summing Up

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

Q&A

Thank You!

I will now be taking questions.