Saturnin

A suite of lightweight symmetric algorithms for post-quantum security

Anne Canteaut Sébastien Duval Gaëtan Leurent María Naya-Plasencia
Léo Perrin Thomas Pornin André Schrottenloher

FSE 2019 rump session

Design goals

NIST requirements

1. Well studied algorithms
2. Lightweight

Our goals

1. Post-quantum security, including Q2
2. Strong security arguments
3. Efficient in hardware and software

Design choices

- New block cipher design
- 256-bit key and state
- Large key and state
- Carefully selected modes
- SPN cipher
- Wide-trail strategy (AES-like)
- Bitslice design
- Strong mixing from small components

Design goals

NIST requirements

1. Well studied algorithms
2. Lightweight

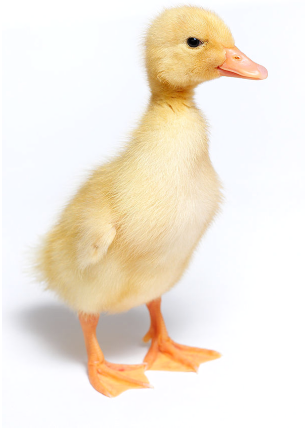
Our goals

1. Post-quantum security, including Q2
2. Strong security arguments
3. Efficient in hardware and software

Design choices

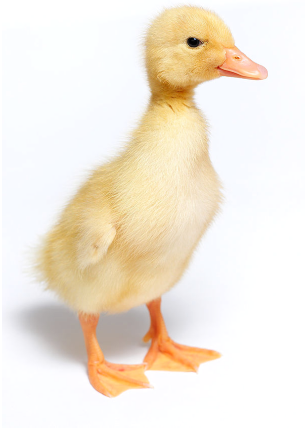
- New block cipher design
- 256-bit key and state
- Large key and state
- Carefully selected modes
- SPN cipher
- Wide-trail strategy (AES-like)
- Bitslice design
- Strong mixing from small components

Why is it called Saturnin?



- The duck is a well known standard of lightweightness
  - *If... she... weighs the same as a duck... she's made of wood.*
  - *And therefore?*
  - *A witch!* [*Monty Python and the Holy Grail*]
- A famous French duck is called Saturnin
  - Kids TV show in the 60's and 70's
- The planet Saturn is associated to the cube
  [Kepler, *Mysterium Cosmographicum*]

Why is it called Saturnin?

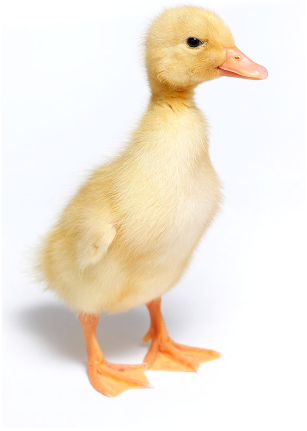


- The duck is a well known standard of lightweightness
  - *If... she... weighs the same as a duck... she's made of wood.*
  - *And therefore?*
  - *A witch!*

  [*Monty Python and the Holy Grail*]
- A famous French duck is called Saturnin
  - Kids TV show in the 60's and 70's
- The planet Saturn is associated to the cube

  [Kepler, *Mysterium Cosmographicum*]

Why is it called Saturnin?

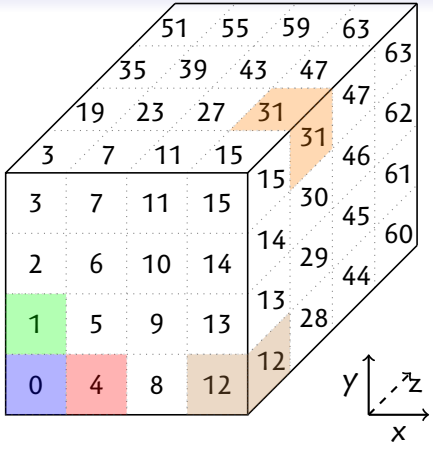


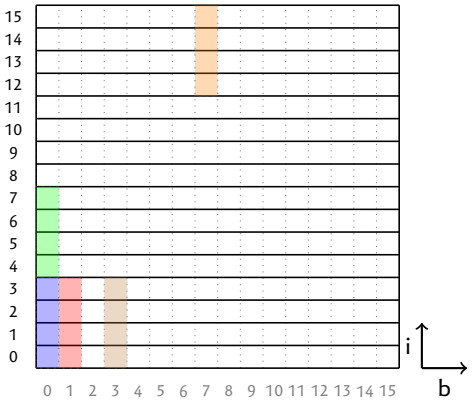
- The duck is a well known standard of lightweightness
  - *If... she... weighs the same as a duck... she's made of wood.*
  - *And therefore?*
  - *A witch!*

  [*Monty Python and the Holy Grail*]
- A famous French duck is called Saturnin
  - Kids TV show in the 60's and 70's
- The planet Saturn is associated to the cube

  [Kepler, *Mysterium Cosmographicum*]

Saturnin state



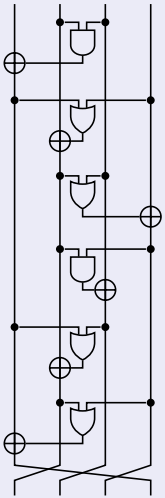


- Cube of $4 \times 4 \times 4$ nibbles
- MixColumn
- SR_{slice}, SR_{sheet}

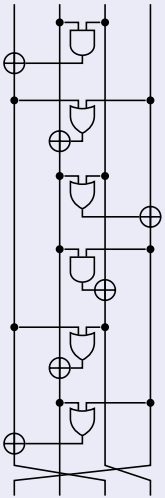
- 16 registers of 16 bits
- Bitslice operations
- Permutation of the bits inside a register

Components

SBox

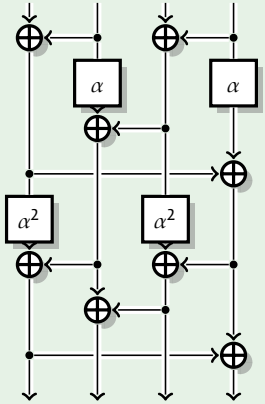


σ_0



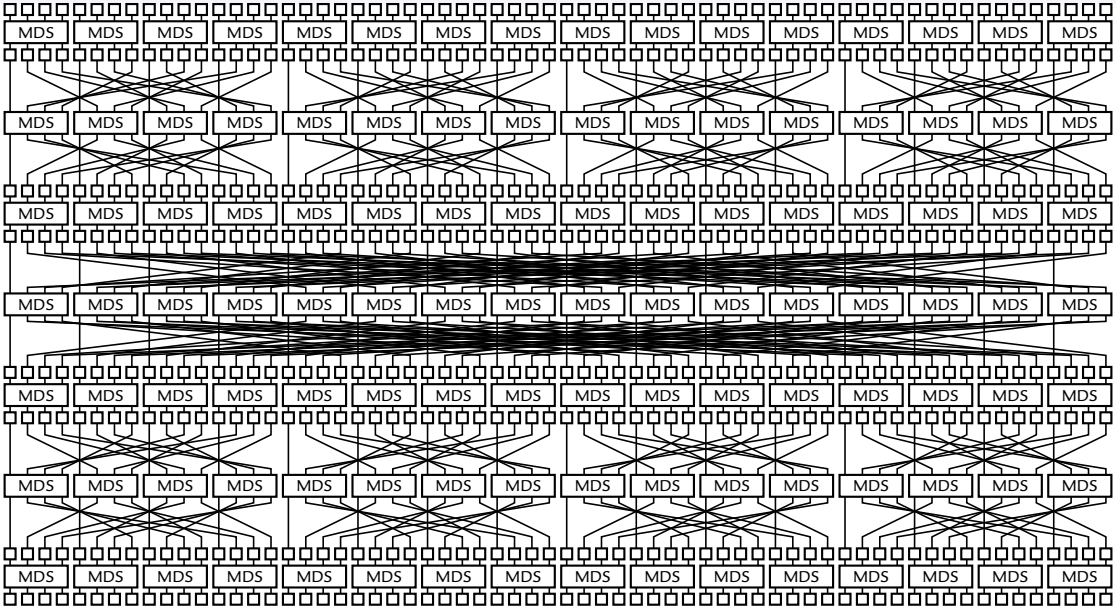
σ_1

MixColumn: MDS matrix

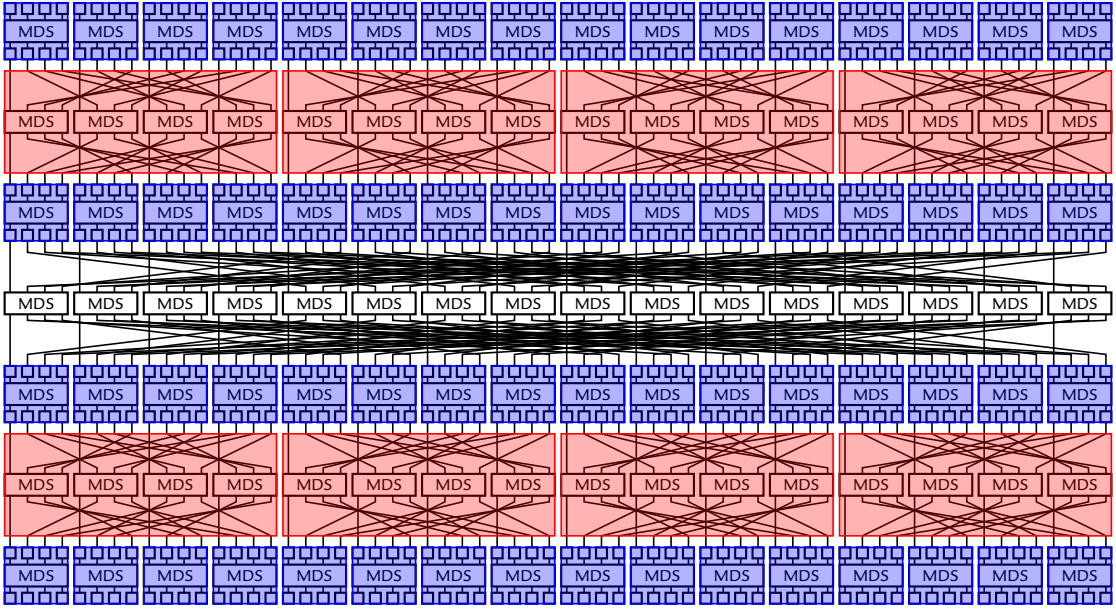


$$\alpha : \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Super-Sbox and Meta-Sbox: 5^3 active S-Boxes



Super-Sbox and Meta-Sbox: 5^3 active S-Boxes



Super-Sbox and Meta-Sbox: 5^3 active S-Boxes