Specifications of BUNNY24

Stefano Martin

University of Trento

23 ottobre 2012

BunnyTN or Bunny24

BunnyTn or *Bunny24* is a block cipher created by Stefano Martin under the supervision of Prof. Sala, as an example of a (toy) block cipher which is susceptible to no known attack faster than brute force.
The set of messages and the set of keys have cardinality 2^{24}.

Notations

Often we switch from the vector space $(\mathbb{F}_2)^6$ to the field $\mathbb{F}_{2^6}$.
We also use the following notations:

$$\mathbb{F} := \mathbb{F}_2$$

e

$$\mathbb{E} := \mathbb{F}_{2^6}$$

The primitive polynomial for the operations in $\mathbb{E}$ is

$$x^6 + x^4 + x^3 + x + 1$$

We call e the primitive element of $\mathbb{E}$.

Input/Output

INPUT:

- m, a message of 24 bits
- k, a key of 24 bits

OUTPUT:

- c, an encrypted message of 24 bit

Key schedule

Before encrypting, a key schedule function gets as input the 24-bit key and return 16 round keys of 24 bits each.
We call the round keys:

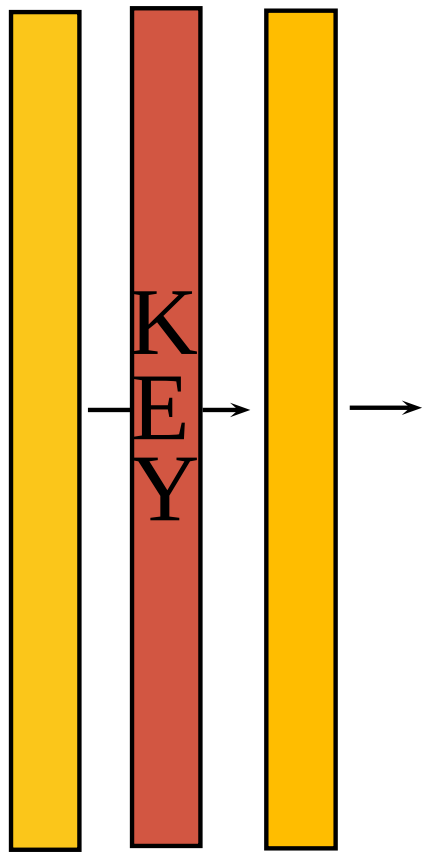
$$k_0, ..., k_{15}$$

This function will be described later.

Block cipher scheme

1. $k_0, \cdots, k_{15} = KeySchedule(k)$
2. $m = m + k_0$ (Whitening operation)
3. for $i = 1, \cdots, 15$ do
   3.1 $m = RoundFunction(m, k_i)$
4. return m

Whitening operation

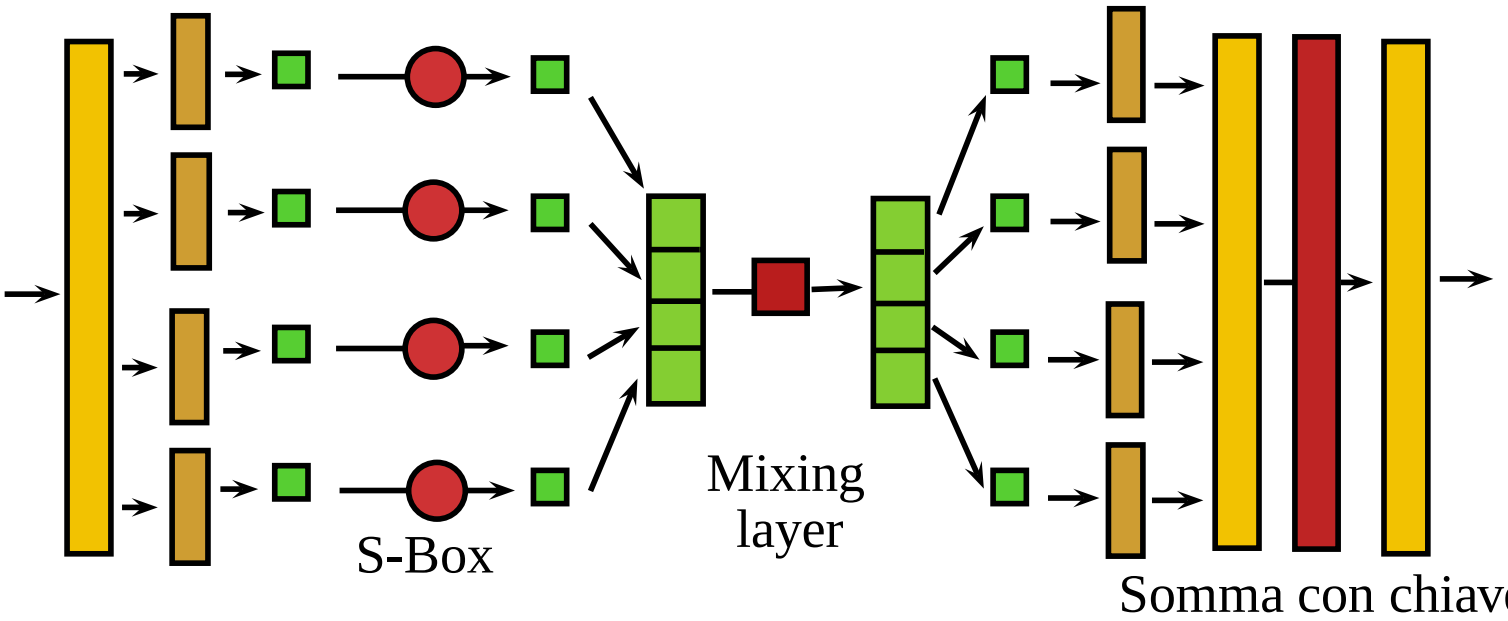


The first operation of Bunny24 is the sum with the first round key.

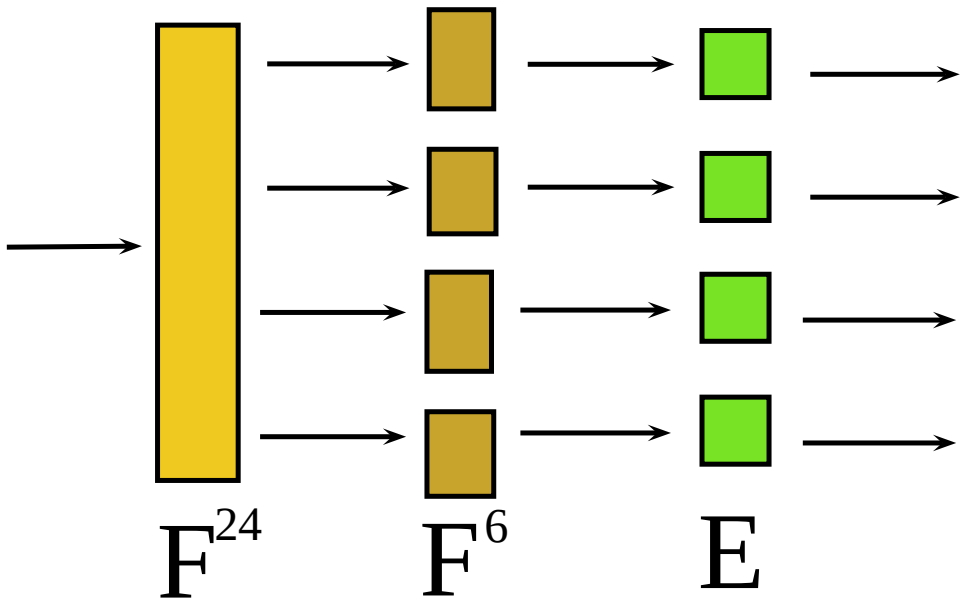
Round structure

The round function is the composition of three different functions (red blocks):

- a non linear function *Sbox*()
- a linear function *MixingLayer*()
- a *xor* with the round key



Change of the input representation



The round input changes from one vector of $\mathbb{F}^{24}$ to four vectors of $\mathbb{F}^{6}$ and to four elements of the field $\mathbb{E}$.

From vector to field element

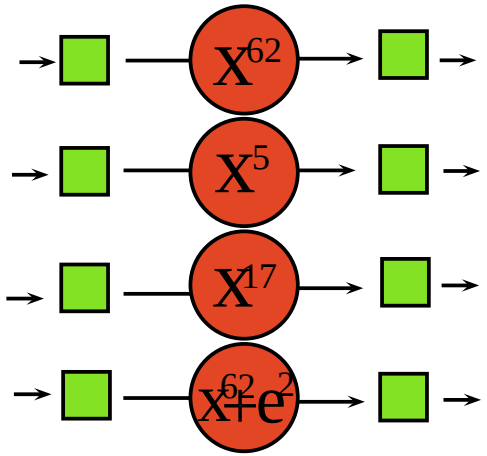
We use the convention that the leftmost bit rapresents the coefficient of the monomial with highest degree.
So, the vector:

$$(100011)$$

corresponds the field element:

$$x^5 + x + 1$$

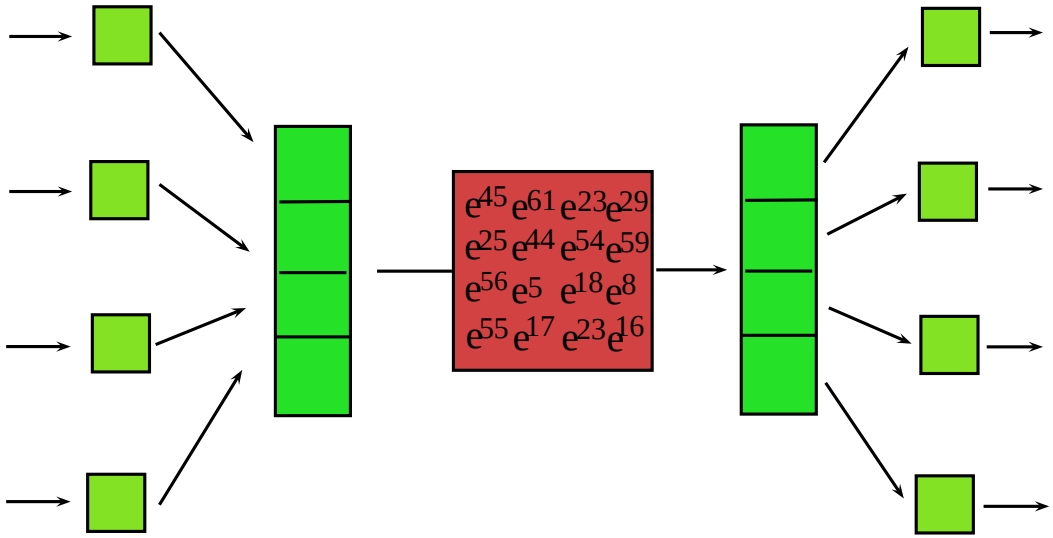
S-Box



The four values of $\mathbb{E}$ are input of four different substitution boxes, also called *S-boxes*, SB_1, SB_2, SB_3, SB_4.They perform the following operation in the field $\mathbb{E}$:

- x^{62}
- x^5
- x^{17}
- $x^{62} + e^2$

Mixing Layer



We multiply the input vector v of $\mathbb{E}^4$ (obtained from the output of the four S-boxes) by a matrix λ, 4×4, over $\mathbb{E}$; we obtain another vector of $\mathbb{E}^4$.

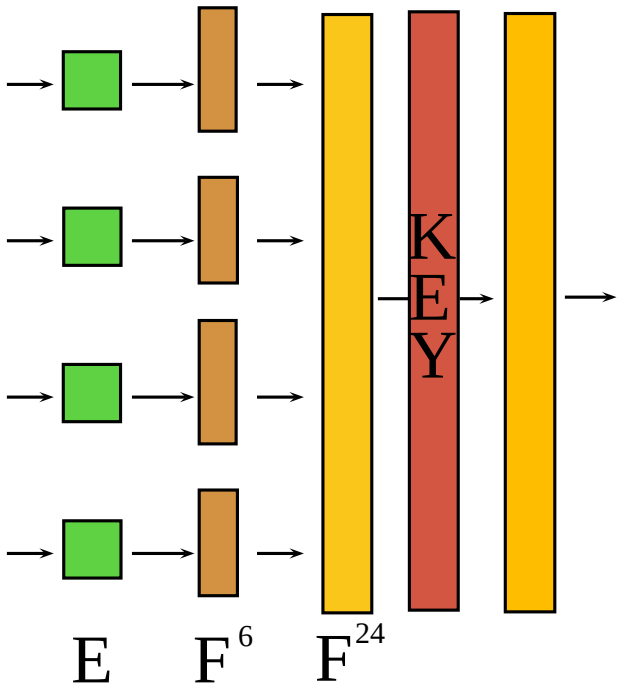
$$v \cdot \lambda$$

Mixing Layer inverse matrix

The inverse matrix of λ is:

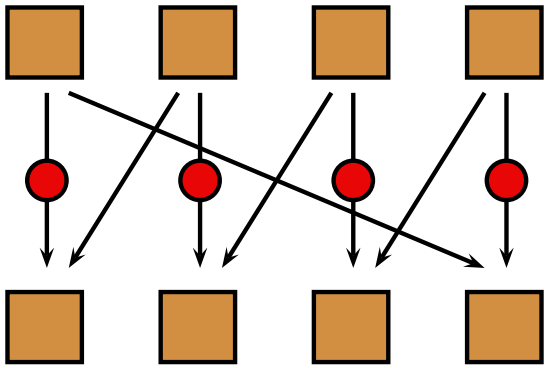
$$\begin{matrix} e^{46} & e^{56} & e^{53} & e^{31} \\ e^{35} & e^{48} & e^{38} & e^{29} \\ e^{20} & e^{18} & e^{11} & e^{58} \\ e^{50} & e^{47} & e^{25} & e^{12} \end{matrix}$$

Sum with the round key

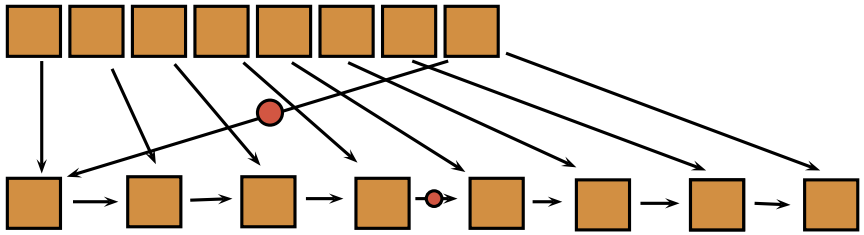


Key-Schedule - Step 1

We perform three steps in the key schedule.
Given the key k in $\mathbb{F}^{24}$ we split it in four words of 6 bits each: $W_1, \ldots, W_4$.
Then we generate $W_5, \ldots, W_8$ in this way:
$W_i = SB_{(i-4)}(W_{i-4}) + W_{i-3} \quad i = 5, 6, 7$
$W_8 = SB_4(W_4) + W_1$.

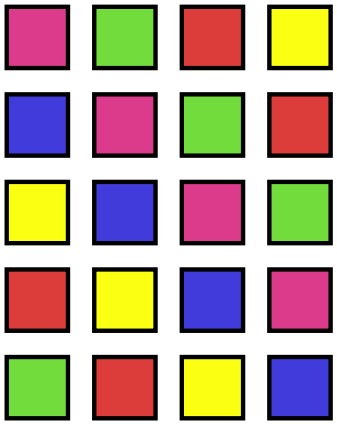


Key-schedule - Step 2

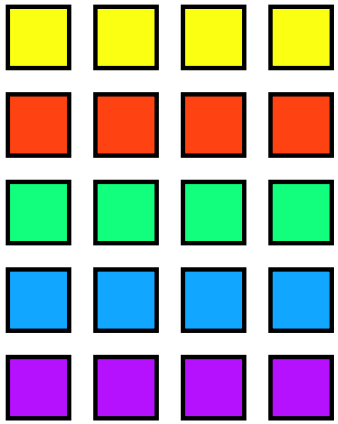


From $W_1, \ldots, W_8$ we proceed as follows:
$W_i = W_{i-8} + W_{i-1}$ if $i \bmod 4 \neq 1$
$W_i = W_{i-8} + SB_2(RB(W_{i-1})) + (1,0,1,0,1,0)$ if $i \bmod 8 = 1$
$W_i = W_{i-8} + SB_3(W_{i-1})$ if $i \bmod 8 = 5$.
Where SB_2 is x^5 and SB_3 is x^{17}.
RB is the left-rotation of one bit.

Key-schedule - Step 3



BunnyTN



AES

We build a rectangle with each group of 20 consecutive words (the first four word of the twenty are the first row, the second four words form the second row, and so on...).
Then we take the round keys starting from the upper-leftmost word of the rectangle and following the “diagonal”.
This way each rectangle generates 5 round key.