BunnyTN: a toy cipher

Stefano Martin (mishtir@gmail.com)
Department of Mathematics, University of Trento, Italy

Massimiliano Sala (maxsalacodes@gmail.com)
Department of Mathematics, University of Trento, Italy

Abstract

This article presents the toy cipher BunnyTN and explains the functions which are used in each round.
In each section we give an explanation about the motivations for which we have chosen that function.
In particular we give the definition of the δ-differentially uniformity and MDS Matrix.

Keywords: Cryptography, block cipher.

It is very hard to work with Block Cipher with a big key space and a big message space and to understand the maths that we use to test the Block Cipher.
For this reason we have created "BunnyTN".
It is divided into six sections.

In the first section we will give some definitions and some notations that we are going to use in this article.
In the second section we will present you the toy-cipher BunnyTN.
The third section contains the explanation about the S-Box step and the fundamental valuation that a builder should test: i.e. the invertibiliy, the δ-differential uniformity and the classical non-linearity.
In the fourth section we test the mixing layer and we explain because a MDS-Matrix is a good choice.
The fifth section is dedicated at the key-schedule of BunnyTN.
In the sixth section we will choice the number of typical round to have a block cipher which resists at distinguisher attacks. To choose this number we used the NIST-tests.
In the seventh section there are other tests that we have used to evaluate our block cipher.

1 Preliminaries and notation

$0 \in A$, then $A^* = A \backslash \{0\}$.
We denote by n any integer $n \geq 1$. For any field $\mathbb{K}$, $\mathbb{K}^n$ denotes the n-dimensional vectorial space over $\mathbb{K}$.
We write $\mathbb{F}_q$ for the field with q elements, where q is any power of a prime.
We will use vectorial spaces over $\mathbb{F}_2$ or $\mathbb{F}_{2^6}$. To simplify our notations we write: $\mathbb{F} = \mathbb{F}_2$ and $\mathbb{E} = \mathbb{F}_{2^6}$.
In $\mathbb{F}[x]$ we choose $x^6+x^4+x^3+x+1$ as the primitive polynomial that we use to represent $\mathbb{E}$. We denote with e the primitive element of $\mathbb{E}$ ($e^6 = e^4+e^3+e+1$).
Clearly the vectorial space $\mathbb{F}^6$ is isomorphic to the field $\mathbb{E}$ by:

$$\xi : \mathbb{F}^6 \to \mathbb{E}, \quad \xi(v_0, \ldots, v_5) = \sum_{i=0}^{5} v_i e^i.$$

Thanks to ξ, we can view vectors in $\mathbb{F}^6$ as field element and so we can multiply them. Note that the addition is the XOR.
Also, we can write all functions from $\mathbb{F}^6$ to $\mathbb{F}^6$ as polynomial over $\mathbb{E}$, since it holds [LN97]:
Theorem 1. If $\mathbb{F}_q$ is a finite field and $f : \mathbb{F}_q \to \mathbb{F}_q$ is a function, then f can be represent by a polynomial $\bar{f} \in \mathbb{F}_q[x]$ with $\deg \bar{f} \leq q-1$.

Any vectors over $\mathbb{F}^{24}$ can be divided in four parts of 6 bits each, in this way:

$$\mathrm{div} : \mathbb{F}^{24} \to (\mathbb{F}^6)^4,$$

$$\mathrm{div}(m_0, \ldots, m_{23}) = ((m_0, \ldots, m_5), (m_6, \ldots, m_{11}), (m_{12}, \ldots, m_{18}), (m_{19}, \ldots, m_{23})).$$

We will call each of these parts "word".
We often use the parallel version of xi:

$$\vartheta : (\mathbb{F}^6)^4 \to \mathbb{E}^4, \quad \vartheta(w_1, \ldots, w_4) = (\xi(w_1), \ldots, \xi(w_4)).$$

Definition 2. If $v, w \in \mathbb{F}^n$ then the *Hamming distance* of v and w is

$$\mathrm{d}(v, w) = |\{i : v_i \neq w_i, i \in \{1, \ldots, n\}\}|.$$

The *Hamming weight* of $v \in \mathbb{F}^n$ is $\mathrm{w}(v) = \mathrm{d}(v, 0)$.

Definition 3. If A is a square matrix, the determinant of a square submatrix of A is called a *minor* of A.

For example, if $A = \begin{bmatrix} 2 & 4 & 2 & 1 \\ 3 & 3 & 1 & 0 \\ 9 & 2 & 2 & 1 \\ 1 & 3 & 6 & 2 \end{bmatrix}$, a minor of A could be:

$$\det(A^{1,4}_{2,3}) = \left| \begin{bmatrix} 4 & 2 \\ 3 & 6 \end{bmatrix} \right| = 18$$

$A^{1,4}_{2,3}$ is obtained from matrix A by removing two rows, the first and the fourth, and two columns, the second and the third.

Definition 4. A square-matrix A is *MDS* (Maximum Distance Separable) if each minor of A is non-zero.

2 The toy-cipher BunnyTN

BunnyTN is a "toy cipher" in the sense that we know a priori that it is not secure. In fact, it has a small key space (with only 2^{24} keys) and so a key-search is easy to implement.
However, BunnyTN has been built with the hope that no attack exists faster than the brute force.
Other toy ciphers were created with similar goal such as small scale variants of the AES, [CMR05], the stream ciphers of the FLURRY family [CW09] or the cipher CTC [Cou07].

2.1 Structure

The key space is $\mathcal{K} = \mathbb{F}^{24}$. Any key induces a permutation φ_k on $\mathbb{F}^{24}$, $\varphi_k \in \mathrm{Sym}(\mathbb{F}^{24})\ \forall k \in \mathcal{K}$.
In traditional terminology, we say that the plaintext space coincides with the ciphertext space, i.e. $\mathcal{P} = \mathcal{C} = \mathbb{F}^{24}$.
For any $v \in \mathbb{F}^{24}$, σ_v is the sum (the XOR), i.e. if $v = (v_0, v_1, \ldots, v_{23})$ and $m = (m_0, m_1, \ldots, m_{23})$ then

$$\sigma_v : \mathbb{F}^{24} \to \mathbb{F}^{24}, \quad \sigma_v(m) = (m_0 + v_0, m_1 + v_1, \ldots, m_{23} + v_{23})$$

where $+$ is the usual bit addition.

We consider 16 round keys $\{k_0, \ldots, k_{15}\}$ and they are generated by the key scheduling, which is explained in Section 5.
We denote with γ the non-linear part of the block cipher (S-Box). It is explained in Section 3.
The linear function λ (Mixing Layer) is always the same for all typical rounds. We explain it in Section 4.
Given a round key k, a typical round ρ_k is the composition of these three operations:

$$\rho_k : \mathbb{F}^{24} \to \mathbb{F}^{24}, \quad \rho_k = \sigma_k \circ \lambda \circ \gamma.$$

BunnyTN has 15 typical rounds ρ_{k_i}, $i \in \{1, \ldots, 15\}$, plus the *whitening* $\rho_{k_0} = \sigma_{k_0}$, that is, for any session key k, we have:

$$\varphi_k = \rho_{k_{15}} \circ \cdots \circ \rho_{k_1} \circ \rho_{k_0}.$$

Note that BunnyTN is a translation based cipher [CDS09], similar to AES [DR02], SERPENT [ABK98] and PRESENT [AKL+07].

3 S-Box step

The parallel S-Box step represents the non-linear part of BunnyTN.
The parallel function γ is constituted by four functions, each working on words: $F_1(x_1) = x_1^{62}$, $F_2(x_2) = x_2^5$, $F_3(x_3) = x_3^{17}$, $F_4(x_4) = x_4^{62} + e^2$. In this way:

$$\gamma' : \mathbb{E}^4 \to \mathbb{E}^4, \quad \gamma'(x_1, x_2, x_3, x_4) = (x_1^{62}, x_2^5, x_3^{17}, x_4^{62} + e^2)$$

and so:

$$\gamma : \mathbb{F}^{24} \to \mathbb{F}^{24}, \quad \gamma(x) = \mathrm{div}^{-1} \circ \vartheta^{-1} \circ \gamma' \circ \vartheta \circ \mathrm{div}(x)$$

We note that f_1 is the patched inversion in $\mathbb{E}$ because $x^{62} \cdot x = x^{63} = x^{2^6-1} = 1$ $\forall x \in \mathbb{E}^*$.

We have chosen F_1, F_2, F_3, F_4 in such way that they are:

- invertible;
- 4-differential uniform;
- highly non-linear (with the classical notion).

3.1 Invertibility

For the block cipher structure we use, inversion is required to decrypt.

The inverse of F_4 can be easily determined $F_4^{-1}(x) = (x + e^2)^{62}$.
For the other S-Boxes we apply the following corollary; obtained easily from Theorem 1.15 [LN97]:

Corollary 5. If $\mathbb{F}_q$ is a finite field with primitive element e and $f : \mathbb{F}_q \to \mathbb{F}_q$ is $f(x) = x^k$, then f is invertible if and only if e^k generate $\mathbb{F}_q$. The inverse of $f(x) = x^k$ is $f^{-1}(x) = x^t$ such that $kt = 1 \bmod (q-1)$.

Since e^5, e^{17} and e^{62} generate $\mathbb{E}$, so x^5, x^{17} and x^{62} are invertible.
The inverse of F_2 is $F_2^{-1}(x) = x^{38}$.
The inverse of F_3 is $F_3^{-1}(x) = x^{26}$.

3.2 δ-differential uniformity

There are many criteria to evaluate the non-linearity of vectorial Boolean functions: one of these is the δ-differential uniformity.

Definition 6. A function $\mathbb{F}^n : \mathbb{E} \to \mathbb{F}^n$ is *δ-differential uniform* if $\forall \alpha \in (\mathbb{F}^n)^*$ and $\forall \beta \in \mathbb{F}^n \ |\{x \in \mathbb{F}^n : f(x) + f(x+\alpha) = \beta\}| \leq \delta$.
A function which is 2-differentially uniform is called *APN* (Almost Perfectly Nonlinear).

A Block Cipher with high differential uniformity might be attacked by a differential attack, so it is desirable that δ is small. Invertible APN functions are very difficult to find (we do not know even if any exists over $\mathbb{F}_{2^k}$ with $k \geq 8$ even). We claim that F_1, F_2, F_3, F_4 are are 4-differential uniform.

Theorem 7 (Proposition 3, [Nyb94]). Let $f(x) = x^{2^k+1}$ be a power polynomial in $\mathbb{F}_{2^n}$ and let $s = \gcd(k, n)$. Then f is differentially 2^s-uniform.

If we choose $k = 2$ and $k = 4$, we can apply the previous theorem, with $n = 6$ (so $s = 2$), and x^5 and x^{17} are differentially 4-uniform.

The inversion x^{62} is 4-differentially uniform due to the following result:
Theorem 8 (Proposition 6, [Nyb94]). For any finite field $\mathbb{F}_q$, the inversion is 4-differentially uniform.

The inversion over $\mathbb{E}$ translated by e^2 is obviously 4-differential uniform, because the δ-differential uniformity is invariant w.r.t. translations.

3.3 Classical non-linearity

Another of the classical criteria to evaluate the non-linearity of a Boolean function f is the Hamming distance from the set of the affine functions, where the distance is defined as follows:
Definition 9. Let f, g: $\mathbb{F}^n \to \mathbb{F}$, then

$$\mathrm{d}(f, g) = |\{v : f(v) \neq g(v), v \in \mathbb{F}^n\}| .$$

If A is a set of functions from $\mathbb{F}^n$ to $\mathbb{F}$, then $\mathrm{d}(f, A) = \min_{g \in A} \mathrm{d}(f, g)$.
If B is another set of functions from $\mathbb{F}^n$ to $\mathbb{F}$, then $\mathrm{d}(A, B) = \min_{f \in A} \mathrm{d}(f, B)$.
$f : \mathbb{F}^n \to \mathbb{F}$ is called affine function if $\exists w \in \mathbb{F}^n$ and $\exists c \in \mathbb{F}$ such that $f(v) = v \cdot w + c$.
If $\mathbb{A}$ is the set of affine functions from $\mathbb{F}^n$ to $\mathbb{F}$, then we define the *classical non-linearity* of a function $f : \mathbb{F}^n \to \mathbb{F}$ as:

$$N(f) = d(f, \mathbb{A}).$$

To evaluate the non-linearity of vectorial Boolean functions, we use the non-linearity of Boolean functions.
Let $G : \mathbb{F}^n \to \mathbb{F}^n$, we define $g_i : \mathbb{F}^n \to \mathbb{F}$, $i \in \{1, \ldots, n\}$, such that
$G(x_1, \ldots, x_n) = (g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n))$.
Then we can define the non-linearity of G as the minimum of the non linearity of all combinations og g_i's, that is:

$$N(G) = \min_{(\lambda_1,\ldots,\lambda_n)\in\mathbb{F}^n} \mathrm{d}(\sum_{i=1}^{n} \lambda_i g_i, \mathbb{A}). \tag{1}$$

A low non-linearity is dangerous. For example, if $N(G) = 0$ we have the worst case, since there is a combination of g_i's, $w \in \mathbb{F}^6$ and $b \in \mathbb{F}$ such that $\sum_{i=1}^{n} \lambda_i g_i(v) = v \cdot w + b$.
To find w and b is very easy, the attacker needs only $v = 0$ to find b and a basis of $\mathbb{F}^6$ to find w.
Even if $N(G) > 0$ but $N(G)$ is low, then the attacker can easily find an affine function α and a combination β of g_i's such that $\mathrm{d}(\alpha, \beta)$ is minimal in order to approximate β accurately.

The maximum that w can have from a Boolean function $f : \mathbb{F}^6 \to \mathbb{F}$ is 24 (see [PJ99]). In BunnyTN all our functions enjoy
$N(F_1) = N(F_2) = N(F_3) = N(F_4) = 24$.

3.4 Other observations

We took the fourth S-Box f_4 adding a translation to f_1, so γ has no fixed points.
If we had chosen $f_4(x) = x^{62}$ then we would have had 16 fixed points for γ, because each of x^{62}, x^5 and x^{17} has 2 fixed points (0 and 1).

4 Mixing Layer

The Mixing Layer is the linear part of a typical round. We want an invertible matrix which "mixes" the output words of the S-Box step. As Mixing Layer we could have chosen $A \in \mathrm{GL}(24, \mathbb{F})$ but we choose a matrix $A \in \mathrm{GL}(4, \mathbb{E})$, which is a byte-control. The operation of the Mixing Layer is:

$$\lambda : \mathbb{F}^{24} \to \mathbb{F}^{24}, \quad \lambda(x) = \mathrm{div}^{-1} \circ \vartheta^{-1} \circ \lambda' \circ \vartheta \circ \mathrm{div}(x)$$

where

$$\lambda' : \mathbb{E}^4 \to \mathbb{E}^4, \quad \lambda'(v) = vA$$

$$A = \begin{bmatrix} e^{45} & e^{61} & e^{23} & e^{29} \\ e^{25} & e^{44} & e^{54} & e^{59} \\ e^{56} & e^{5} & e^{18} & e^{8} \\ e^{55} & e^{17} & e^{23} & e^{16} \end{bmatrix}$$

We have chosen this Matrix A with the MDS property.
A brutal search of an MDS matrix in the group $\mathrm{GL}(\mathbb{E}, 4)$ is hard, because the set of MDS matrices is very small. To select an MDS matrix we have used the generating matrix of a Reed Solomon code.

Definition 10 ([MS77]). Let α be a primitive element of $\mathbb{F}_q$, then we can define an evaluation function:

$$\mathrm{ev} : \mathbb{F}_q[x] \to (\mathbb{F}_q)^{q-1} \quad \mathrm{ev}(p) = (p(\alpha), \ldots, p(\alpha^{q-1}))$$

For any $0 \leq \Delta \leq q-1$, the *Reed Solomon code*

$$\mathrm{RS}(q, \Delta) = \{\mathrm{ev}(p) : \deg p \leq \Delta, p \in \mathbb{F}_q[x]\}$$

.

Let G be a systematic generating matrix for $\mathrm{RS}(q, \Delta)$. It is well-known in coding theory that any square sub-matrix in the non-systematic part of G is an MDS matrix. In our case it is enough to consider $\mathrm{RS}(2^6, 3)$, so that G is a 4×63 matrix.

In this case its branch number is 5.

Definition 11. An $n \times n$ matrix over $\mathbb{K}$ A has *branch number* k if k is the

maximal integer such that $\forall x, y \in (\mathbb{K}^n)^*$ and $x \neq y$ then

$$\mathrm{d}(x, y) + \mathrm{d}(Ax, Ay) \geq k$$

Theorem 12 ([BR00]). An $n \times n$ MDS matrix A over $\mathbb{K}$ has branch number $n + 1$.

It easy to see that $n + 1$ is the maximal branch number possible for a matrix in $\mathrm{GL}(n, \mathbb{K})$. In fact if we choose c with weight 1,
$d(0, c) + d(A(0), A(c)) = 1 + d(0, A(c))$ and so our branch number will be less than $1 + \mathrm{w}(A(c)) \leq 1 + n$.

Our 4×4 matrix A is MDS, so its branch number is 5. This ensures high diffusion between the words of the message.

5 Key-schedule

In this section, to simplify our notation, we do not write explicitly the isomorphism φ.
The Key-schedule of BunnyTN is divided into three steps.

5.1 First step: creation of $W_{-8}, \ldots, W_{-1}$

The first step of the Key-Schedule is to divide the session key with the usual subdivision $\mathrm{div} : \mathbb{F}^{24} \to (\mathbb{F}^6)^4$ to obtain four words: $W_{-8}, W_{-7}, W_{-6}, W_{-5} \in \mathbb{F}^6$. To create $W_{-4}, W_{-3}, W_{-2}, W_{-1}$ we proceed as follows:

$$W_{-4} = {W_{-8}}^{62} + W_{-7}$$

$$W_{-3} = {W_{-7}}^{5} + W_{-6}$$
$$W_{-2} = {W_{-6}}^{17} + W_{-5}$$
$$W_{-1} = {W_{-5}}^{62} + e^2 + W_{-8}$$

In other words we use the S-Boxes.

5.2 Second step: creation of $W_1, \ldots, W_{80}$

The second step takes as input $W_{-8}, \ldots, W_{-1}$ and returns as output the W_i's to create the round-key.

$$W_i = W_{i-8} + W_{i-1} \text{ if } i \bmod 4 \neq 1$$

$$W_i = W_{i-8} + \mathrm{RB}(W_{i-1})^5 + (1,0,1,0,1,0) \text{ if } i \bmod 8 = 1$$
$$W_i = W_{i-8} + W_{i-1}^{17} \text{ if } i \bmod 8 = 5$$
$$i = \{0,1,\ldots,80\}$$

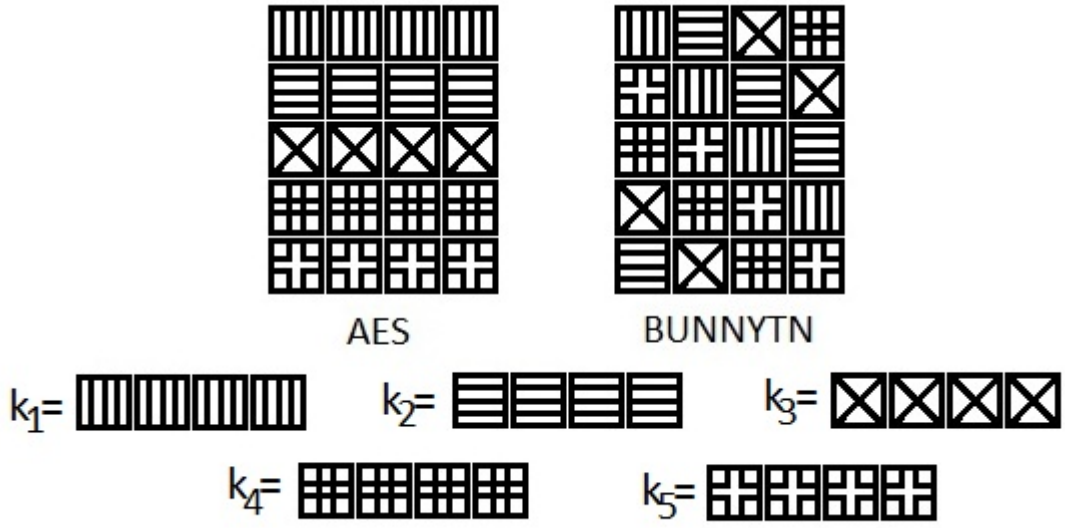
where RB is the rotation of six bits in a word to the left:

$$\mathrm{RB} : \mathbb{F}^6 \to \mathbb{F}^6, \quad \mathrm{RB}((x_5,x_4,x_3,x_2,x_1,x_0)) = (x_4,x_3,x_2,x_1,x_0,x_5).$$

5.3 Third step: creation of the round keys

At the last step we create the round keys.
We discard the $W_{-8},\ldots,W_{-1}$.
We use this algorithm:

$$k_i = \mathrm{div}^{-1}(W_{i \bmod 5+20\lfloor i/5\rfloor}, W_{i \bmod 5+20\lfloor i/5\rfloor+5}, W_{i \bmod 5+20\lfloor i/5\rfloor+10}, W_{i \bmod 5+20\lfloor i/5\rfloor+15})$$
$$i = \{0,\ldots,15\}$$



Note that we use rectangular blocks with 20 W_i's. For this reason in the previous step i goes to 80 which is a multiple of 20. This algorithm picks the W_i's in diagonal in each block to build each round key.

This picking guarantees a higher security than, for example, the key-schedule of AES, since we reduce the mutual information between all round keys. In AES, the algorithm takes the W_i horizontally, but if an attacker finds a round key, he can discover a lot of information on the previous round key, and so it is easier to discover all the round keys. In BunnyTN, this is not possible for the structure given in Step 3, in fact the structure of our round key is diagonal and an attacker cannot use the inverse of the Step 2 to find some information about the previous key.

For this reason, in the classification of security of the key schedules (see [CDN98]), BunnyTN is 2A, instead of AES128 which is 1C.

5.4 Other observation

Again, in the Step 2 the use of the translation helps to avoid fix points. In fact x^5 and x^{17} have two fix points (0 and 1) and a fix point of the key-schedule could be dangerous.

6 Number of rounds

The choice of the number of rounds is important: too few rounds can give bad security, too many rounds need expensive computations. So the design usually starts from a low number of rounds and checks the robustness of the resulting cipher. A way to check the robustness of a cipher is to too see if the encrypted ciphers are similar to random messages. If the encryption looks random, then it is impossible to predict its behavior. If an algorithm is distinguishable from a random oracle, it may b attackable. That is, there may exist a relation between different outputs, or between input and output, which can be used by an attacker.

Fifteen distinguishers are proposed by the National Institute of Standard and Technology (NIST) at this link:
`http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html`.
(A more detailed presentation is in the documentations of NIST [NIS00]).

A one-round BunnyTN has no security: it fails all NIST tests.
A two-rounds BunnyTN turns out to be weak in the "Approximate Entropy Test".
A three-rounds BunnyTN shows problems with "Cumulative Sums" and with "Longest Run Test".
A four-rounds BunnyTN has apparently no problems with any NIST test.

We would choose 12 rounds, in conservative manners, as three times the minimum of the apparent indistinguishability, but curiously a 12-rounds BunnyTN has some weakness with the "Random Excursion Test". So we move to a 15-rounds BunnyTN. Obtained results are good, except for a tiny discrepancy in the "Non Periodic Template Matchings Test".

Here we present a table with the results of the NIST-tests on BunnyTN with 15 rounds and 60 sequences with 10^6 bits:

P-value	Statistical Test
0.090936	Frequency
0.019188	Block Frequency
0.366918	Cumulative Sums (1/2)
0.181557	Cumulative Sums (2/2)
0.090936	Runs
0.162606	Longest Run
0.595549	Rank
0.304126	FFT
0.224821	Non Overlapping Template (1/148)
0.366918	Overlapping Template
0.595549	Universal
0.224821	Approximate Entropy
0.888137	Random Excursions (1/8)
0.060239	Random Excursions Variant (1/18)
0.002559	Serial (1/2)
0.224821	Serial (2/2)
0.181557	Linear Complexity

7 Evaluation

We have evaluated BunnyTN from many points of view.

Diffusion

Definition 13. Let be $\rho : \mathbb{F}^n \to \mathbb{F}^n$ a typical round. We said that ρ has got *i-th diffusion* k if $\rho^k = \underbrace{\rho \circ \ldots \circ \rho}_{k}$ has got this property:
if $\rho^k(x_1, \ldots, x_i, \ldots, x_n) = (f_1(x_1, \ldots, x_i, \ldots, x_n), \ldots, f_n(x_1, \ldots, x_i, \ldots, x_n))$ then
$f_j(x_1, \ldots, x_i, \ldots, x_n) \notin \mathbb{F}[x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n] \quad \forall j \in \{1, \ldots, n\}$.
We said that ρ has got *diffusion* k if ρ has got i-th diffusion k, $\forall i \in \{1, \ldots, n\}$.

We have proved that BunnyTN has diffusion 2 with only two rounds, i.e. each bit of the ciphertext is edited by each bit of the plaintext after two rounds.

Weakly δ-differential uniform

Definition 14 ([CDS09]). Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $a \in \mathbb{F}_{2^n}^*$, $\hat{F}_a(x) = F(x) + F(x+a)$. We say that F is *weakly δ-differential uniform* if $\forall \in \mathbb{F}_{2^n}^*$ then:

$$\left|\mathrm{Im}(\hat{F}_a)\right| > \frac{2^{n-1}}{\delta}.$$

If F is weakly 2-differential uniform, it is called *weakly APN*.

As it is know [CDS09] the δ differential uniformity implies the weakly δ differential uniformity.
Our functions x^5 and x^{17} are not weakly APN, however they are 4 differential uniform, so they are weakly 4-differential uniform. On the other hand, x^{62} and $x^{62} + e^2$ are weakly APN.

Algebraic Degree

Definition 15. We call *pure monomial* any polynomial in $\mathbb{F}_q[x_1, \ldots, x_n]$ of type $X_S = \prod_{i \in S} x_i$ where $S \subset \{1, \ldots, n\}$ (for example: $x_{\{1,4,5\}} = x_1 x_4 x_5$). $x_\emptyset = 1$.
Given $f : \mathbb{F}^n \to \mathbb{F}$, we can write $f = \sum_{S \subset \{1,\ldots,n\}} a_S X_S$. This writing is called *normal form* of f.

Definition 16 ([CM03]). If $f : \mathbb{F}^n \to \mathbb{F}$, $f = \sum_{S \subset \{1,\ldots,n\}} a_S X_S$ then the *algebraic degree* of f is

$$\Delta(f) = \max\{deg(X_S) | a_S \neq 0\}$$

If $F : \mathbb{F}^n \to \mathbb{F}^m$, $F(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$ then the *algebraic degree* of F is

$$\Delta(F) = \min_{(\lambda_1,\ldots,\lambda_m) \in (\mathbb{F}^m)^*} \Delta(\sum_{i=1}^{m} \lambda_i f_i)$$

The algebraic degree of x^5 and x^{17} is 2, the algebraic degree of x^{62} is 5. The algebraic degree for x^5 and x^{17} is very low, but it is the minimum to have a nonlinearity. The algebraic degree for the inverse is very good (it is the maximum).

Algebraic Density

Definition 17. If $f : \mathbb{F}^n \to \mathbb{F}$, $f = \sum_{S \subset \{1,\ldots,n\}} a_S X_S$ then the *algebraic density* of f is

$$\eta(f) = |\{a_S | a_S \neq 0\}|$$

If $F : \mathbb{F}^n \to \mathbb{F}^m$, $f(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n))$ then the *algebraic density* of F is

$$\eta(F) = \min_{(\lambda_1,\ldots,\lambda_m) \in \mathbb{F}^m} \eta(\sum_{i=1}^{m} \lambda_i f_i)$$

The density of x^5, x^{17} is 7, the one of x^{62} is 23. This is not very good because a random function over $\mathbb{F}^6$ has density 32. However this is not so terrible, because the use of many rounds give us a good density.

Anti-invariance

Definition 18. Let $F : \mathbb{F}^n \to \mathbb{F}^n$, it is *strongly l-anti-invariant* if $\forall V, W \subset \mathbb{F}^n$ r-dimensional subspace such that $f(V) = W$, then $r < n - l$.
Let $F : \mathbb{F}^n \to \mathbb{F}^n$, is is *$l$-anti-invariant* if $\forall V \in \mathbb{F}^n$ r-dimensional subspace such that $F(V) = V$, then $r < n - l$.

In BunnyTN x^5, x^{17} and x^{62} are 3-anti-invariant and strongly-3-anti-invariant.

Affine equivalence

Definition 19 ([BCP06]). Let be $\mathbb{K}$ a field and $F, G : \mathbb{K}^n \to \mathbb{K}^n$ two functions. They are *affine equivalent* if exist two $n \times n$ invertible matrix A and B and two vectors c and d of length n such that:

$$B(F(Ax + c)) + d = G(x) \quad \forall x \in \mathbb{K}^n.$$

x^5 and x^{17} are affine equivalent.
x^{62} is in a different affine equivalent class.

Proper and strongly proper

Definition 20 ([CDS09]). Let be $V = \oplus_{i=1}^{s} V_i$ vectorial space and $V_i \subset V$ subspaces of V. We call V_i *bricks*.
Let be $I \subset \{1, \ldots, s\}$ $I \neq \emptyset$, $W = \oplus_{i \in I} V_i$ is called *wall*.

Definition 21. Let be $\lambda \in \mathrm{GL}(V)$, λ is *proper* if a sum of V_i does not exist which is invariant per λ; i.e. $\forall W$ wall, $\lambda(W) \neq W$.

Definition 22. Let be $\lambda \in GL(V)$, λ is *strongly proper* if $\forall W$ wall, $\lambda(W)$ is not a wall.

Mixing Layer of BunnyTN is proper and strongly proper.

Effective non linearity

Definition 23 ([DK07]). $F : \mathbb{F}^n \to \mathbb{F}^n$, $f \in \mathrm{Sym}_{\mathbb{F}^n}$. Its *effective non linearity* is:

$$\mathrm{E}(F) = \frac{2^n}{(2^n-1)^2} \sum_{\alpha,k\neq 0} \mathbb{P}(\alpha \overset{F_k}{\to} \alpha)$$

where F_k is the *Even-Mansovr's Cipher*, i.e. $F_k(x) = F^{-1}(F(x)+k)$.

Theorem 24.

$$\mathrm{E}(F) \approx -1 + 2^{-2n} \sum_{\alpha\neq 0,\beta\neq 0} (\mathrm{DDT}^F(\alpha,\beta))^2$$

where DDT is the *Distribution Differential Table*, which is a square matrix so defined:

$$\mathrm{DDT}^F(\alpha,\beta) = \{x : F(x) + F(x+\alpha) = \beta\}.$$

Effective non linearity of one round of BunnyTN is about 232.

A Appendix

To decipher we need to know the inverse of S-Box and of Mixing Layer.
The inverse of Mixing Layer is given by:

$$A^{-1} = \begin{bmatrix} e^{46} & e^{56} & e^{53} & e^{31} \\ e^{35} & e^{48} & e^{38} & e^{29} \\ e^{20} & e^{18} & e^{11} & e^{58} \\ e^{50} & e^{47} & e^{25} & e^{12} \end{bmatrix}$$

References

[ABK98] R.J. Anderson, E. Biham, and L. Knudsen, *Serpent: A proposal for the Advanced Encryption Standard*, NIST AES Proposal, 1998.

[AKL+07] A. Andrey Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, *PRESENT: An ultra-lightweight block cipher*, Proc. of CHES 2007, LNCS, vol. 4727, Springer, 2007, pp. 450–466.

[BCP06] L. Budaghyan, C. Carlet, and A. Pott, *New classes of almost bent and almost perfect nonlinear polynomials*, Information Theory, IEEE Transactions on **52** (2006), no. 3, 1141–1152.

[BR00] P. Barreto and V. Rijmen, *The whirlpool hashing function*, First open NESSIE Workshop, Leuven, Belgium, vol. 13, 2000, p. 14.

[CDN98] G. Carter, E. Dawson, and L. Nielsen, *Key schedules of iterative block ciphers*, Information Security and Privacy, Springer, 1998, pp. 80–89.

[CDS09] A. Caranti, F. Dalla Volta, and M. Sala, *On some block ciphers and imprimitive groups*, AAECC **20** (2009), no. 5-6, 229–350.

[CM03] N. Courtois and W. Meier, *Algebraic attacks on stream ciphers with linear feedback.*, Proc. of EUROCRYPT 2003, LNCS, vol. 2656, Springer, 2003, pp. 345–359.

[CMR05] C. Cid, S. Murphy, and M. J. B. Robshaw, *Small scale variants of the AES*, Proc. of FSE 2005, LNCS, vol. 3557, Springer, 2005, pp. 145–162.

[Cou07] N.T. Courtois, *Ctc2 and fast algebraic attacks on block ciphers revisited*, IACR ePrint report **152** (2007), 2007.

[CW09] C. Cid and R. P. Weinmann, *Block ciphers: algebraic cryptanalysis and Gröbner bases*, Gröbner Bases, Coding, and Cryptography (M. Sala, T. Mora, L. Perret, S. Sakata, and C. Traverso, eds.), RISC Book Series, Springer, Heidelberg, 2009, pp. 307–327.

[DK07] O. Dunkelman and N. Keller, *A new criterion for nonlinearity of block ciphers*, Information Theory, IEEE Transactions on **53** (2007), no. 11, 3944–3957.

[DR02] J. Daemen and V. Rijmen, *The Design of Rijndael*, Springer, 2002.

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[MS77] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. II*, North-Holland Publishing Co., Amsterdam, 1977, North-Holland Mathematical Library, Vol. 16.

[NIS00] *A statistical test suite for random and pseudorandom number generators for cryptographic applications*, Special Publication SP 800-22, NIST, 2000.

[Nyb94] K. Nyberg, *Differentially uniform mappings for cryptography*, Proc. of EUROCRYPT 1993, LNCS, vol. 765, Springer, 1994, pp. 55–64.

[PJ99] Enes Pasalic and Thomas Johansson, *Further results on the relation between nonlinearity and resiliency for boolean functions*, Cryptography and Coding (Michael Walker, ed.), Lecture Notes in Computer Science, vol. 1746, Springer Berlin / Heidelberg, 1999, 10.1007/3-540-46665-7_3, pp. 796–796.