Convolutional block codes with cryptographic properties over the semi-direct product $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$

Marion Candau[1,2], Roland Gautier[2] and Johannes Huisman[3]

[1]LMBA, UMR CNRS 6205, Université de Bretagne Occidentale, Brest, France,
marioncandau.mc@gmail.com
[2]Lab-STICC, UMR CNRS 6285, Université de Bretagne Occidentale, Brest, France
[3]LMBA, UMR CNRS 6205, Université de Bretagne Occidentale, Brest, France

Abstract

Classic convolutional codes are defined as the convolution of a message and a transfer function over $\mathbb{Z}$. In this paper, we study time-varying convolutional codes over a finite group G of the form $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$. The goal of this study is to design codes with cryptographic properties. To define a message u of length k over the group G, we choose a subset E of G that changes at each encoding, and we put $u = \sum_i u_i E(i)$. These subsets E are generated chaotically by a dynamical system, walking from a starting point (x, y) on a space where each rectangle represent an element of G. So each iteration of the dynamical system gives an element of the group which is saved on the current E. The encoding is done by a convolution product with a transfer function. We have found a criteria to check if an element in the group algebra can be used as a transfer function. The decoding process is realized by syndrome decoding. We have chosen a particular group $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ to compute the minimum distance. We found it is slightly smaller than those of the best linear block codes. Nevertheless, our codes induce a symmetric cryptosystem whose key is the starting point (x, y) of the dynamical system. Consequently, these codes are a compromise between error correction and security.

1 Introduction

An error correcting code [8, 7] adds redundancy to a message in order to correct it when errors occur during transmission. There are two types of codes : block codes and convolutional codes. The encoding operation of the block codes starts by dividing the message into several different blocks of same length k. Then each block is encoded by a mathematical operation whose result is a block of code word of length $n > k$.

The convolutional codes have been discovered by Elias [2] in 1955. The operation of encoding is the convolution product of the whole message with a transfer function, both defined over the group of integers $\mathbb{Z}$.

These two types of codes do not protect the message if it is intercepted by a third party. To protect the message, we use cryptography [5] before error correcting codes. Without cryptography, in a non-cooperative context, code recognition [6] is hard but possible.

In this paper, we study convolutional block codes over the non-commutative group $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ with a time-varying encoding, in order to design codes with cryptographic properties.

The principle of encoding is the following. The message U is divided into blocks u of length k. Each block u is mapped on a subset $E = \{e_0, \ldots, e_{k-1}\}$ of the finite group G. At each encoding, we use a subset E that is different from the previous. These subsets E are generated chaotically from the key of the encoding. These chaotic subsets are called encoding intervals. Consequently, each block u defines an element in the group algebra $\mathbb{F}_2[G]$ by :

$$u = \sum_{i=0}^{k-1} u_i e_i, \ e_i \in E$$

The transfer function τ defines an element in $\mathbb{F}_2[G]$ too. The code word c is the result of the convolution product of u and τ in $\mathbb{F}_2[G]$. The bits $c_i \in \mathbb{F}_2$ are defined as :

$$c = \sum_{i=0}^{n-1} c_i g_i, \ g_i \in G$$

They constitute the code word that is sent on the channel. In the next section, we will show how to generate some chaotic subsets of length k.

2 Generation of some chaotic subsets of the group

We want to map a message u into the group $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ such that the message's support on the group is different at each encoding. Let $\mathbb{Z}^2$ be the subset of $\mathbb{R}^2$ of all points with integer coordinates and let ρ be the reduction function :

$$\begin{aligned} \rho : \mathbb{Z}^2 &\to \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z} \\ (x, y) &\mapsto (x \mod N, y \mod M) \end{aligned}$$

Given $H = \{(Na, Mb), a, b \in \mathbb{Z}\}$, we have $\rho(x, y) = \rho(x', y')$ if and only if $(x, y) - (x', y') \in H$, then the set $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ is identified with the quotient $\mathbb{Z}^2/H$. Let us recall the definition of a fundamental domain.

Definition 2.1. *Given a set E and a group acting on it, the images of a single point under the group action form an orbit of the action. A fundamental domain*

is a subset of the space which contains exactly one point from each of these orbits. Otherwise, given a set E and a group G acting on it, we denote by $g.x$ the image of the point $x \in E$ under the action of the element $g \in G$. A subset F of E is called a fundamental domain for the group action if:

- $\bigcup_{g \in G} g(F) = E$
- $\forall g, g' \in G$ *such that* $g \neq g', g(F) \cap g'(F) = \emptyset$

We compute a fundamental domain of H in the Euclidean plane. The action of H on the plane sends the point (x, y) to the point $(Na + x, Mb + y)$. The orbit of the point $(0, 0)$ under the action of H is :

$$H.(0,0) = \{(0,0), (N,0), (0,M), (N,M), \ldots\}$$

We extend the action of H on $\mathbb{Z}^2$ to $\mathbb{R}^2$ and consequently, a fundamental domain of H is the rectangle

$$([0,N] \times [0,M]) \setminus ([(0,M),(N,M)] \cup [(N,0),(N,M)])$$

with the segments $[(0,M),(N,M)]$ and $[(N,0),(N,M)]$ that are identified respectively to the segments $[(0,0),(N,0)]$ and $[(0,0),(0,M)]$. This domain is represented on the figure 1. By gluing the identified sides pairwise, we obtain a torus [4].

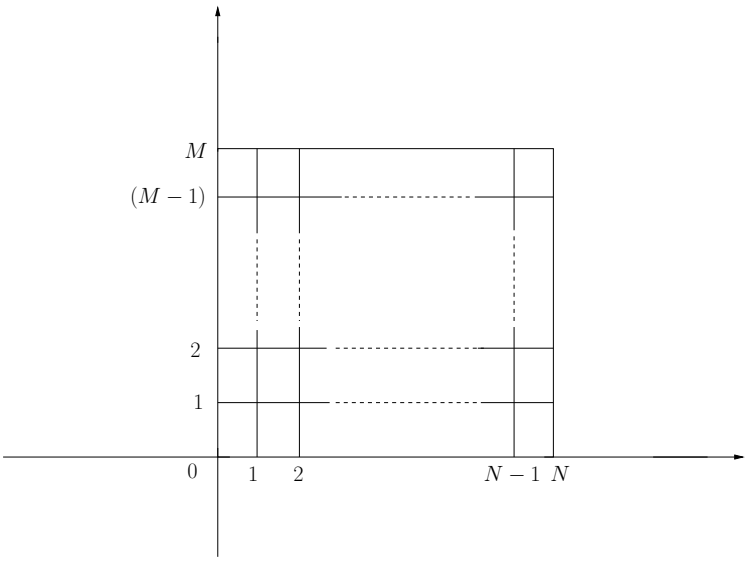

Figure 1: Fundamental domain of H

We represent each element of the group $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ by corresponding each element (i, j) of the group with the little rectangle $[(i,j),(i+1,j),(i+1,j+1),(i,j+1)]$ of the torus $\mathbb{R}^2/H$. This representation is used to generate

sequences of elements of the group in a chaotic order.

To generate these sequences, we use the famous discrete dynamical system called Arnold's cat. This dynamical system is chaotic (Theorem 4.8 of [1]) and usually described on the unit square, so we divide the abscissa by N and the ordinate by M to have a domain defined on the unit square.

Let be $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. This matrix is used to define the following automorphism ϕ on the torus $\mathbb{T}$:

$$\begin{array}{c} \phi : \mathbb{T} \to \mathbb{T} \\ \begin{pmatrix} x \\ y \end{pmatrix} \mapsto A \begin{pmatrix} x \\ y \end{pmatrix} \end{array}$$

The iterations of this automorphism define a discrete dynamical system. To generate the encoding intervals, we use the algorithm 1.

We have then some chaotic subsets of the group $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ that we can used to map the message on the group.

3 Encoding

We first study the problem of transfer functions that should not be right zero divisors in $\mathbb{F}_2[\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}]$.

3.1 Transfer function and injection

To define an error correcting code defined by convolution, each code word must be the result of one and only one message by convolution, otherwise we can not decode. So convoluting by the transfer function must be injective. To put it otherwise, the transfer function must not be a right zero divisor in the algebra $\mathbb{F}_2[G]$. Let us recall the definition of a right zero divisor.

Definition 3.1. *Let a be a nonzero element of a ring A. We say that a is a right zero divisor in A if there exists $b \neq 0 \in A$ such that $ba = 0$*

Definition 3.2. *Let G a group and $\tau \in \mathbb{F}_2[G]$. The element τ is a transfer function if τ is not a right zero divisor.*

Here we choose an odd N and an odd M so $G = \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ has an odd cardinal which causes that

$$PGCD(Card(\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}), car(\mathbb{F}_2)) = PGCD(NM, 2) = 1$$

with $car(K)$ the characteristic of the field K. Consequently, we can apply the Maschke theorem [9], and define the Fourier transform $\widehat{f}$ of any function $f \in \mathbb{F}_2[\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}]$.

Algorithm 1 Generation of encoding intervals of length k on the group $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$

Require: N, M, $NbInterval$ the number of intervals, (x, y) the starting point, k the length of the encoding intervals
Ensure: $TabInterval$ the table of intervals
  Build a domain associated with $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z}$
  Initialize a vector $InInterval$ of length $N \times M$.
  $NumberElt = 1$
  while $length(TabInterval) < NbInterval$ **do**
    $\begin{pmatrix} x \\ y \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$
    if $x > 1$ **then**
      $x = x - floor(x)$
    end if
    if $y > 1$ **then**
      $y = y - floor(y)$
    end if
    $ft = square(x, y)$ the number of the square where is (x, y).
    if $InInterval(ft) == 0$ **then**
      $InInterval(ft) = NumberElt$
      $NumberElt++$
      if $NumberElt == k + 1$ **then**
        Initialize a vector $Interval$ of length k.
        for $j = 1$ to $N \times M$ **do**
          if $InInterval(j) \neq 0$ **then**
            $Interval(InInterval(j)) = j$
          end if
        end for
        Add $Interval$ to the table $TabInterval$
        $NumberElt = 1$
        Reset $InInterval$ to a vector of length $N \times M$.
      end if
    end if
  end while
  return $TabInterval$

Let f, τ be in $\mathbb{F}_2[\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}]$, we have the following property :

$$\widehat{f * \tau} = \widehat{f}.\widehat{\tau}$$

This property is used to show the following theorem.

Theorem 1. *Let f, τ be in $\mathbb{F}_2[\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}]$. Let R_i be the i^{th} linear irreducible representation of $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ in $\overline{\mathbb{F}_2}$ (the algebraic closure of $\mathbb{F}_2$). If, for all i, $\widehat{\tau}(R_i)$ is invertible then the application $f \mapsto f * \tau$ is injective.*

Proof. Let τ be in $\mathbb{F}_2[\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}]$.

$$\begin{aligned}
\forall i,\ \widehat{\tau}(R_i) \text{ is invertible} &\Rightarrow \forall f \in \mathbb{F}_2^{\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}} \backslash \{0\},\ \widehat{f}\widehat{\tau} \neq 0 \\
&\Rightarrow \forall f \in \mathbb{F}_2^{\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}} \backslash \{0\},\ \widehat{f * \tau} \neq 0 \\
&\Rightarrow \forall f \in \mathbb{F}_2^{\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}} \backslash \{0\},\ f * \tau \neq 0 \\
&\Rightarrow f \mapsto f * \tau \text{ is injective}
\end{aligned}$$

□

So we have a criteria to determine whether a function $\tau \in \mathbb{F}_2[\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}]$ can be used as a transfer function of a convolutional code.

Remark 3.1. *There is another criteria based on the computation of the determinant of the matrix associated to the linear endomorphism induced by the multiplication-by-τ operation on $\mathbb{F}_2[G]$. This criteria tests if τ is invertible in $\mathbb{F}_2[G]$ by using the Cayley-Hamilton theorem. However, the criteria based on Fourier transform is faster to compute, so we prefer to use it.*

3.2 Example of encoding over $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$

We study encoding over the group $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ because it is the smallest group of the form $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ with non-commutative law. Its group law[1] is :

$$\forall (a,b),(c,d) \in \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z},\ (a,b) \cdot (c,d) = (a + 2^b c \mod 7, b + d \mod 3)$$

To each element $(i,j) \in \mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$, we associate a number such that $(i,j) \mapsto Mi + j = 3i + j$. So we have the following correspondence between numbers and elements :

$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$(4,0)$	$(5,0)$	$(6,0)$
g_0	g_3	g_6	g_9	g_{12}	g_{15}	g_{18}
$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$(4,1)$	$(5,1)$	$(6,1)$
g_1	g_4	g_7	g_{10}	g_{13}	g_{16}	g_{19}
$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$(4,2)$	$(5,2)$	$(6,2)$
g_2	g_5	g_8	g_{11}	g_{14}	g_{17}	g_{20}

[1]It is an additive law therefore it would be logical to note it $+$, but as the $+$ sign is used to represent the elements of the group algebra, we prefer to use $\cdot$ to note the group law.

Let

$$u = [1, 0, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1]$$

be a message. Its length is $k = 14$. Let $(x, y) = \left(\frac{\sqrt{2}}{2}, \frac{16\sqrt{2}}{113}\right)$ be an irrational point of the domain of $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. We generate the encoding interval of length k from (x, y) with the dynamical system. The starting point (x, y) has the property that $\frac{4}{7} < x < \frac{5}{7}$ and $0 < y < \frac{1}{3}$. Consequently, the first element of E is $(4, 0)$ i.e. g_{12}. The first iteration of the dynamical system gives the second point $(x, y) = \left(\frac{145\sqrt{2}}{226}, \frac{177\sqrt{2}}{226} - 1\right)$. We have $\frac{6}{7} < x < 1$ and $0 < y < \frac{1}{3}$, so the second element of E is $(6, 0)$, i.e. g_{18}. After some iterations, we obtain :

$$\begin{aligned} E &= [(4,0),(6,0),(0,0),(2,1),(0,2),(5,1),(1,2),(6,2),(4,1),(0,1),\\ &\quad (3,2),(2,0),(5,0),(5,2)]\\ &= [g_{12}, g_{18}, g_0, g_7, g_2, g_{16}, g_5, g_{20}, g_{13}, g_1, g_{11}, g_6, g_{15}, g_{17}] \end{aligned}$$

The message on the group is then :

$$u = \sum_i u_i E(i) = (4,0) + (0,0) + (1,2) + (6,2) + (0,1) + (3,2) + (2,0) + (5,2)$$

Let τ be a transfer function such that :

$$\begin{aligned} \tau &= [0,0,0,0,0,0,0,0,1,0,1,1,1,0,1,1,1,0,0,0,0]\\ &= \sum_{i=0}^{n-1} \tau_i g_i = g_8 + g_{10} + g_{11} + g_{12} + g_{14} + g_{15} + g_{16}\\ &= (2,2) + (3,1) + (3,2) + (4,0) + (4,2) + (5,0) + (5,1) \end{aligned}$$

Consequently, the convolution product between u and τ is :

$$\begin{aligned} u * \tau &= ((4,0) + (0,0) + (1,2) + (6,2) + (0,1) + (3,2) + (2,0) + (5,2))\\ &\quad \times ((2,2) + (3,1) + (3,2) + (4,0) + (4,2) + (5,0) + (5,1))\\ &= (4,0)\cdot(2,2) + (4,0)\cdot(3,1) + (4,0)\cdot(3,2) + (4,0)\cdot(4,0) + (4,0)\cdot(4,2)\\ &\quad + (4,0)\cdot(5,0) + (4,0)\cdot(5,1) + ((0,0) + (1,2) + (6,2) + (0,1) + (3,2)\\ &\quad + (2,0) + (5,2))\cdot((2,2) + (3,1) + (3,2) + (4,0) + (4,2) + (5,0) + (5,1))\\ &= (4 + 2^0 \times 2 \mod 7, 0 + 2 \mod 3) + (4 + 2^0 \times 3 \mod 7, 0 + 1 \mod 3)\\ &\quad + (4 + 2^0 \times 3 \mod 7, 0 + 2 \mod 3) + (4,0)\cdot(4,0) + (4,0)\cdot(4,2)\\ &\quad + (4,0)\cdot(5,0) + (4,0)\cdot(5,1) + ((0,0) + (1,2) + (6,2) + (0,1) + (3,2)\\ &\quad + (2,0) + (5,2))\cdot((2,2) + (3,1) + (3,2) + (4,0) + (4,2) + (5,0) + (5,1))\\ &= (6,2) + (0,1) + (0,2) + (4,0)\cdot(4,0) + (4,0)\cdot(4,2) + (4,0)\cdot(5,0)\\ &\quad + (4,0)\cdot(5,1) + ((0,0) + (1,2) + (6,2) + (0,1) + (3,2) + (2,0) + (5,2))\\ &\quad \cdot((2,2) + (3,1) + (3,2) + (4,0) + (4,2) + (5,0) + (5,1))\\ &= (0,2) + (1,0) + (1,1) + (3,0) + (3,2) + (4,2) + (5,1) + (5,2) + (6,0) + (6,2)\\ &= g_2 + g_3 + g_4 + g_9 + g_{11} + g_{14} + g_{16} + g_{17} + g_{18} + g_{20}\\ &= (0,0,1,1,1,0,0,0,0,1,0,1,0,0,1,0,1,1,1,0,1) \end{aligned}$$

So the code word is $c = (0,0,1,1,1,0,0,0,0,1,0,1,0,0,1,0,1,1,1,0,1)$.

4 Decoding

The convolution product is a linear operation because the convolution product of two functions in $\mathbb{F}_2^G$ correspond to the product of two elements in the group algebra $\mathbb{F}_2[G]$. Consequently, the convolution product over a finite group G defines linear block codes. Syndrome decoding is usually used to decode linear codes. We will see the decoding of the previous example by syndrome decoding.

Suppose that the receiver receives the word

$$r = (0,0,1,1,1,1,0,0,0,1,0,1,0,0,1,0,1,1,1,0,1)$$

He knows the encoding interval E and the transfer function used in encoding. He can compute the generator matrix whose lines are the result of the convolution of $e_i * \tau$, where e_i is the function with a 1 on the bit $e_i \in E$ and 0 otherwise. He can then compute the parity check matrix H from the systematic generator matrix. Here he has :

$$H = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0
\end{pmatrix}$$

He performs $r^t H$ and he obtains the vector $(0,1,1,0,0,0,0)$ corresponding to the syndrome of an error on the 6th bit. The receiver corrects the value of the 6th bit and obtain $c = (0,0,1,1,1,0,0,0,0,1,0,1,0,0,1,0,1,1,1,0,1)$, which is the code word that has been sent. Then, in order to get the message that has been sent, the receiver performs the convolution product of c and τ^{-1} [2]:

$$\begin{aligned}
u &= c * \tau^{-1} \\
&= ((0,2) + (1,0) + (1,1) + (3,0) + (3,2) + (4,2) + (5,1) + (5,2) + (6,0) + (6,2)) \\
&\cdot ((0,2) + (1,1) + (1,2) + (2,0) + (2,2) + (3,0) + (3,1) \\
&+ (3,2) + (4,1) + (5,1) + (6,1)) \\
&= (0,0) + (0,1) + (1,2) + (2,0) + (3,2) + (4,0) + (5,2) + (6,2) \\
&= g_0 + g_1 + g_5 + g_6 + g_{11} + g_{12} + g_{17} + g_{20}
\end{aligned}$$

Then, he identifies the bits u_i with the encoding interval E.

$$\begin{array}{lcl}
\text{E} & = & [g_{12}, g_{18}, \ g_0, \ \ g_7, \ \ g_2, \ \ g_{16}, \ g_5, \ \ g_{20}, \ g_{13}, \ g_1, \ \ g_{11}, \ g_6, \ \ g_{15}, \ g_{17}] \\
\text{u} & = & [\,1, \ \ 0, \ \ 1, \ \ 0, \ \ 0, \ \ 0, \ \ 1, \ \ 1, \ \ 0, \ \ 1, \ \ 1, \ \ 1, \ \ 0, \ \ 1\,]
\end{array}$$

[2] To compute τ^{-1}, we compute the inverse Fourier transform of the vector composed by all the $(\widehat{\tau}(R_i))^{-1}$.

5 Properties

5.1 Encoding properties

We test the criteria of theorem 1 to the $2^{21} = 2,097,152$ functions of $\mathbb{F}_2^G$ and $84,672$ functions pass the test (around 4%) and can be considered as transfer functions. Moreover, we have 2^{21} encoding intervals so we can define $84,672 \times 2^{21}$ codes over $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$. We want to compute the minimum distance of all these codes but their number is too large. However, we can reduce their number thanks to the following theorems.

Theorem 2. *Let $f, \tau \in \mathbb{F}_2^G$, $g \in G$ and let w be the weight function, i.e. $\forall f \in \mathbb{F}_2^G$, $w(f) = Card\left(\{x \in G \mid f(x) \neq 0\}\right)$. We use the natural left action of G on itself. Then :*

$$w(f * \tau) = w(f * (g.\tau))$$

Proof. Firstly, we have :

$$\begin{aligned} w(g.f) &= Card\left(\{x \in G \mid (g.f)(x) \neq 0\}\right) \\ &= Card\left(\{x \in G \mid f(x.g) \neq 0\}\right) \end{aligned}$$

The action on the group is only a permutation of the elements so

$$w(g.f) = w(f)$$

We have then $w(f * \tau) = w(g.(f * \tau))$. Secondly, we have :

$$\begin{aligned} (g.(f * \tau))(x) &= (f * \tau)(x.g) \\ &= \sum_{t \in G} f(t)\tau(t^{-1}xg) \\ &= \sum_{t \in G} f(t)(g.\tau)(t^{-1}x) \\ &= (f * (g.\tau))(x) \end{aligned}$$

Finally, we have $w(f * \tau) = w(g.(f * \tau)) = w(f * (g.\tau))$. □

Similarly, we can proof the following theorem.

Theorem 3. *Let $f, \tau \in \mathbb{F}_2^G$, $g \in G$ and let w be the weight function, i.e. $\forall f \in \mathbb{F}_2^G$, $w(f) = Card\left(\{x \in G \mid f(x) \neq 0\}\right)$. We use the natural right action of G on itself.*

$$w(f * \tau) = w((f.g) * \tau)$$

We can reduce the number of codes to be tested by taking only the representatives of the orbits under the left action of G on the sets E and the representatives of orbits under the left action of G on the transfer function τ. So we have now $4,032$ functions τ and $99,950$ sets E, then $4,032 \times 99,950 = 402,998,400$ codes to be tested. We have computed the maximum minimum distance for

k	d_{min} linear block codes	d_{min} codes over $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$
2	14	13
3	12	11
4	10	10
5	10	9
6	8	8
7	8	7
8	8	7
9	8	6
10	7	5
11	6	5
12	5	4
13	4	4
14	4	4
15	4	3
16	3	3
17	2	2
18	2	2
19	2	2
20	2	1

Table 1: Comparison of minimum distances of the known linear block codes with those of the convolutional codes over $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$

each length k, that we have compared with the minimum distance of the best linear block codes that we find in [3]. The results are in table 1. We have also computed the number of sets E which achieve a distance d in table 2.

From these tables, we can see that the maximum minimum distance of codes over $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ is smaller for certain k, than the minimum distance of linear block codes and, is identical for the lengths k equals to $4, 6, 13, 14, 16, 17, 18, 19$. Then, we can see that all the sets E don't achieve this maximum minimum distance. To encode, these subsets E will be generated chaotically, so we will not able to choose "good" sets. Only the choice of the transfer function will be important to have a large minimum distance. Consequently, we have computed, for each transfer function, the average distance for all the sets E of length k. We obtain some average-optimal transfer functions for each k. The table 3 presents which average distances these transfer functions achieve.

It can be seen that the optimal average distance is smaller than the minimum distance of the linear block codes. Nevertheless, we have in addition, some cryptographic properties we present in the following.

5.2 Cryptographic properties

The protocol of exchange a message with these codes will be the following.

Alice and Bob agree on a secret key, i.e. a point (x, y) on the unit square.

k	number of E achieving a certain distance
2	10 $E \to d = 13$
3	68 $E \to d = 11$
4	217 $E \to d = 10$ and 68 $E \to d = 9$
5	863 $E \to d = 9$ and 106 $E \to d = 8$
6	2596 $E \to d = 8$ and 2 $E \to d = 7$
7	5535 $E \to d = 7$ and 3 $E \to d = 6$
8	106 $E \to d = 7$ and 9584 $E \to d = 6$
9	12261 $E \to d = 6$ and 1759 $E \to d = 5$
10	16796 $E \to d = 5$
11	6204 $E \to d = 5$ and 10592 $E \to d = 4$
12	14020 $E \to d = 4$
13	9097 $E \to d = 4$ and 593 $E \to d = 3$
14	27 $E \to d = 4$ and 5511 $E \to d = 3$
15	2598 $E \to d = 3$
16	710 $E \to d = 3$ and 259 $E \to d = 2$
17	285 $E \to d = 2$
18	68 $E \to d = 2$
19	10 $E \to d = 2$
20	1 $E \to d = 1$

Table 2: Number of E achieving a certain distance over $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$

They also agree on the other parameters of the codes N, M, k and the transfer function τ.

Alice computes encoding intervals E as much as necessary to map all the blocks of k bits that make up her message, with the point (x, y) and the discrete dynamical system. She computes all the $u = \sum_i u_i E(i)$ messages on the chosen group. She encodes her messages by convoluting them on the group with the function τ. She deduces the bits of the code words to send to Bob. Then, she sends all her code words to Bob.

Bob receives the word r, the code word that Alice has sent, with errors dues to perturbations on the channel. He computes, like Alice, encoding intervals E as much as necessary. He deduces the parity check matrix of each code. He uses syndrome decoding to correct errors and finds the code words c sent by Alice. He computes $c * \tau^{-1}$ for each code word and finds the message u on the group. Finally, he uses the encoding intervals to find the bits u_i of the message.

Imagine now that a third party, Eve, listens to the communication and intercepts the bit stream. Each code word is the result of the convolution of a message and a transfer function on $G = \mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$, with each message mapping on a different subset E of G. Each code word have some dependent bits but the dependence relations are different for each received word. So, if she uses the rank criteria [6], she sees that all the matrices have full rank, and she can not deduce the parameters of the code with this method.

k	optimal average distance
2	10,4
3	8,9
4	7,7895
5	7,0268
6	6,0517
7	5,3374
8	4,8088
9	4,3097
10	3.9243
11	3,6456
12	3,1897
13	2,8278
14	2,5845
15	2,1840
16	2
17	2
18	1,9365
19	1,44
20	1

Table 3: Average distance achieving by the average-optimal transfer function τ for all the sets E of length k

To decode, Eve needs to have the encoding intervals E to compute the parity check matrix like Bob. These encoding intervals are computed from the point (x, y) on the unit square. If Eve tries to guess this point and choose a point (x', y') close to the point (x, y), then she obtains some completely different encoding intervals E, thanks to the chaotic nature of the dynamic system involved. Moreover, these chaotic property requires Alice and Bob to have their software in the same precision.

So Eve needs to know exactly the point (x, y) but it is secret. Without this point, she can neither correct errors nor get the messages u in binary form.

These properties shows that the point (x, y) is the secret key of a symmetric cryptosystem.

6 Conclusion

In this paper, we have proposed convolutional blocks over a group of the form $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ with odd N, M. We have used a time-varying encoding by computing some chaotic subset E from a dynamical system on a quotient of $\mathbb{Z}^2$. These subsets have been used to map the message u of length k into the group. We have found a criteria to check if a element of the group algebra can be used to a transfer function of the code. We have computed the minimum distance of

the code defined over the group $\mathbb{Z}/7\mathbb{Z} \rtimes \mathbb{Z}/3\mathbb{Z}$ to compare it with those of the best linear block codes. We have found that this distance is identical or slightly smaller than the distance of the linear block codes. Nevertheless, our codes can also defined a symmetric cryptosystem whose key is the starting point (x, y) of the dynamical system. Consequently, these convolutional block codes over the group $\mathbb{Z}/N\mathbb{Z} \rtimes \mathbb{Z}/M\mathbb{Z}$ are a compromise between error correction and security.

References

[1] Devaney, R.L.: An Introduction to Chaotic Dynamical Systems, 2nd edn. Addison-Wesley (1989)

[2] Elias, P.: Coding for Two Noisy Channels. In: Information Theory, The 3rd London Symposium, pp. 61–76. Buttersworth's Scientific Publications (1955)

[3] Grassl, M.: Bounds on the minimum distance of linear codes and quantum codes. Online available at http://www.codetables.de (2007). Accessed on 2014-07-21

[4] Hatcher, A.: Algebraic Topology. Cambridge University Press (2002)

[5] Katz, J., Lindell, Y.: Introduction to modern cryptography. Chapman & Hall/CRC cryptography and network security. Chapman & Hall/CRC, Boca Raton (2008)

[6] Marazin, M., Gautier, R., Burel, G.: Blind recovery of k/n rate convolutional encoders in a noisy environment. EURASIP J. Wireless Comm. and Networking **2011**, 168 (2011)

[7] Moon, T.K.: Convolutional codes. In: Error Correction Coding: Mathematical Methods and Algorithms, chap. 12, pp. 452–580. Wiley-Interscience (2005)

[8] Neubauer, A.: Convolutional codes. In: Coding Theory: Algorithms, Architectures and Applications, chap. 3, pp. 112–177. Wiley-Interscience (2007)

[9] Serre, J.P.: Linear representations of finite groups. Graduate texts in mathematics 42. Springer-Verlag, New York Heidelberg (1977)