Resilient Functions and Cyclic Codes from CA

ACRI 2016 – Fez

Luca Mariot[1,2], Alberto Leporati[1]

[1] DISCo, Università degli Studi Milano - Bicocca, Italy

[2] I3S, Université Nice Sophia Antipolis, France

luca.mariot@disco.unimib.it

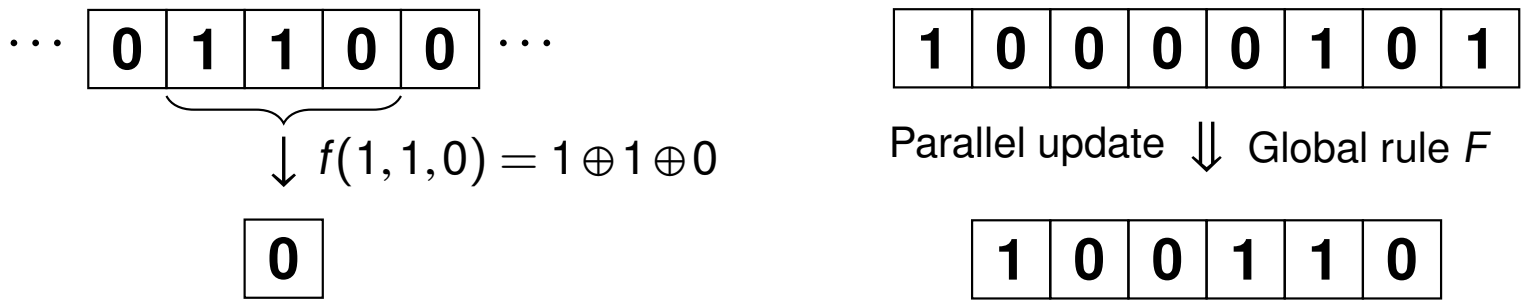
September 5, 2016

One-Dimensional Cellular Automata (CA)

Definition (One-dimensional cellular automaton)

One-dimensional array of $n \in \mathbb{N}$ cells, equipped with a local rule $f : \{0,1\}^{2r+1} \to \{0,1\}$ of radius $r \in \mathbb{N}$.

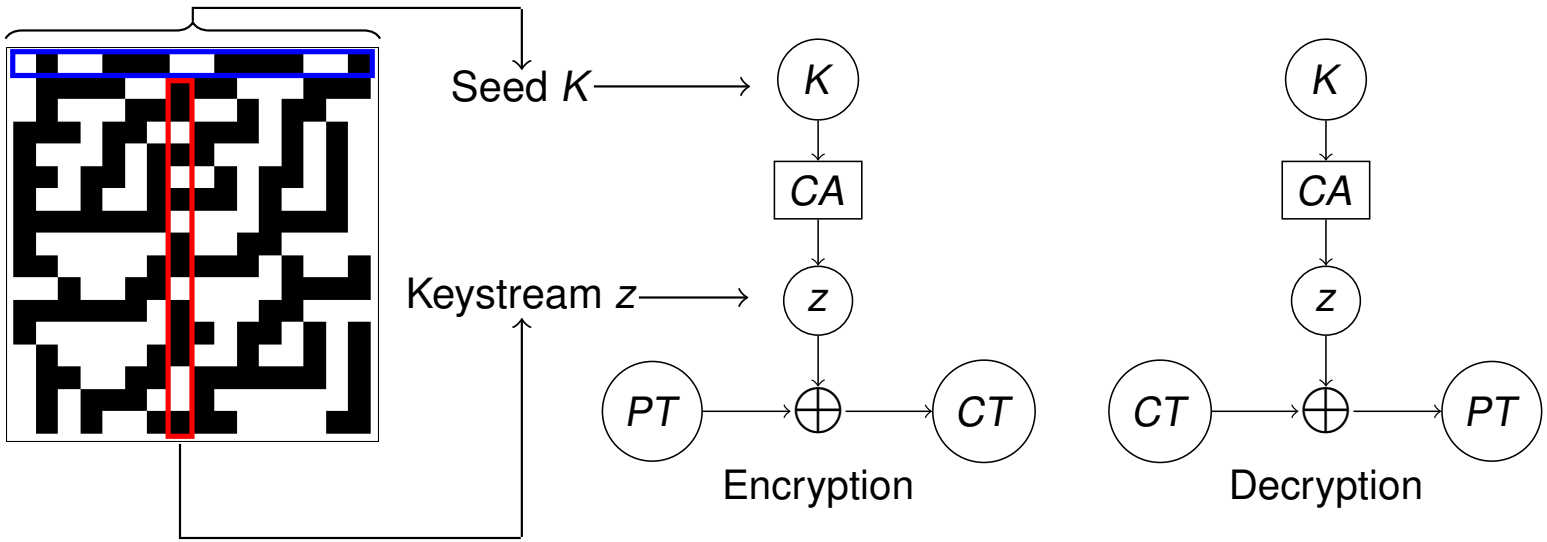
Example: $n = 8$, $r = 1$, $f(s_{i-1}, s_i, s_{i+1}) = s_{i-1} \oplus s_i \oplus s_{i+1}$ (Rule 150)



Remark: No boundary conditions ⇒ The array "shrinks"

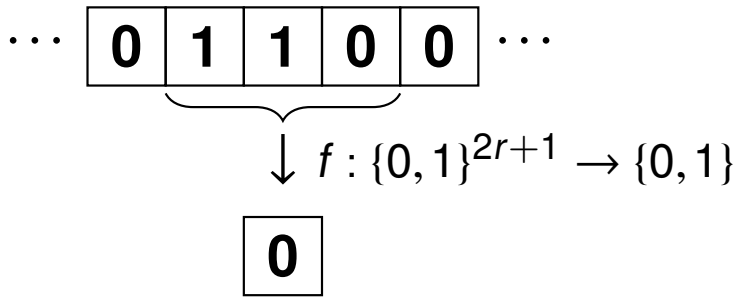
CA-Based Cryptography: Motivations

- General Idea: exploit the emergent complexity of CA to design cryptosystems satisfying confusion and diffusion criteria
- CA-based Pseudorandom Generator (PRG) [Wolfram86]: central cell of rule 30 CA used as a stream cipher keystream



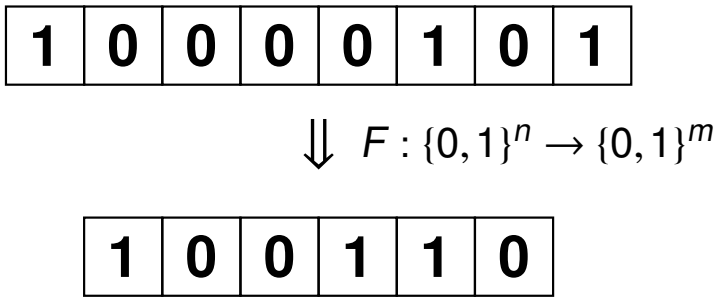
Our Contribution at a Glance

CA-based stream cipher design, up to now:



- Focus on CA local rules, viewed as Boolean functions
- Rationale: choose rule f with best crypto properties

Our approach:



- Some attacks cannot be formalized in a local way
- Idea: Analyse the crypto properties of the CA global rule as a vectorial Boolean function

Resiliency: Basic Definitions

Let $F : \{0,1\}^n \to \{0,1\}^m$ be a n-inputs, m-outputs Boolean function. Then:

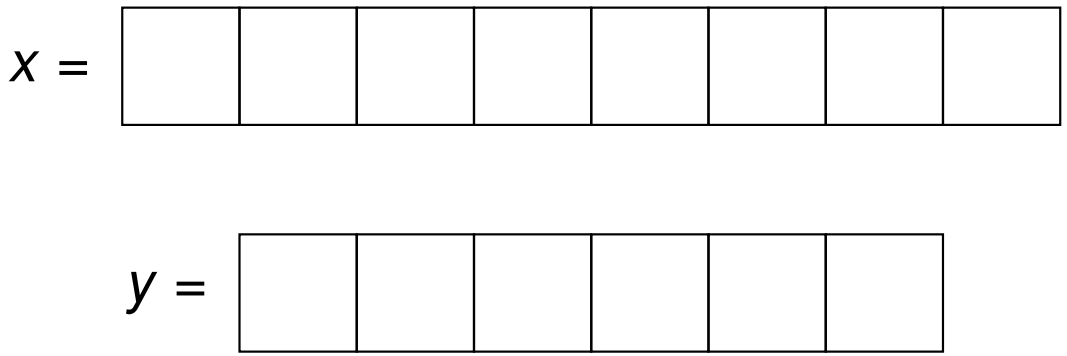
- F is balanced if $|F^{-1}(y)| = 2^m$ for all $y \in \{0,1\}^m$
- F is t-resilient if, fixing any $t < n$ coordinates, the restricted map $F|_t : \{0,1\}^{n-t} \to \{0,1\}$ is balanced

Example: Rule 150, $n = 3$, $m = 1$, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$

(x_1, x_2, x_3)	000	100	010	110	001	101	011	111
$f(x_1, x_2, x_3)$	0	1	1	0	1	0	0	1

The Resiliency Game [Chor85]

1. The *player* chooses a function $F : \{0,1\}^n \to \{0,1\}^m$

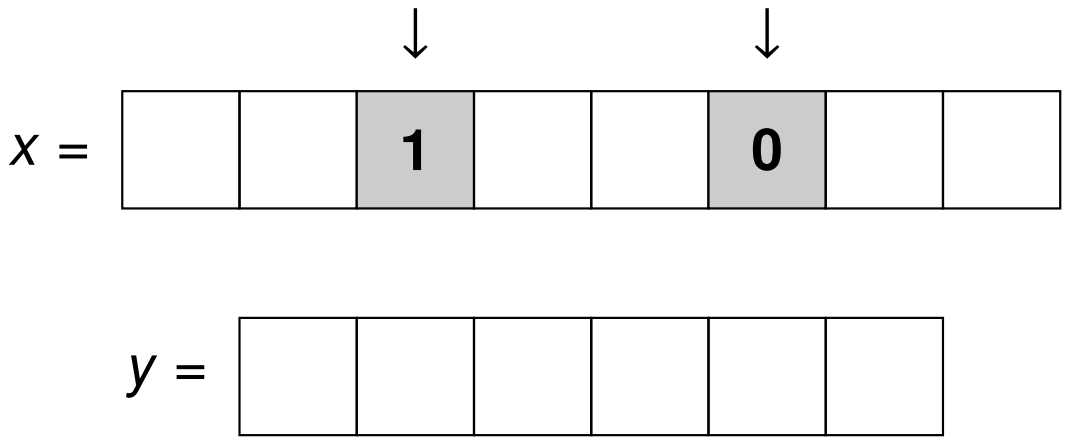


Example: CA $F : \{0,1\}^8 \to \{0,1\}^6$ induced by rule 150,

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$$

The Resiliency Game [Chor85]

2. The *adversary* chooses the values of t input variables

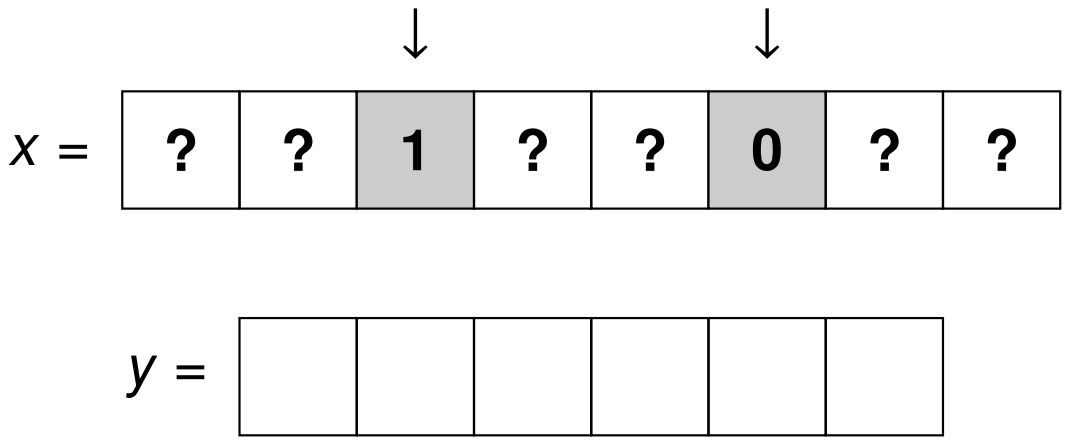


Example: CA $F : \{0,1\}^8 \to \{0,1\}^6$ induced by rule 150,

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$$

The Resiliency Game [Chor85]

2. The values for the remaining variables are randomly chosen

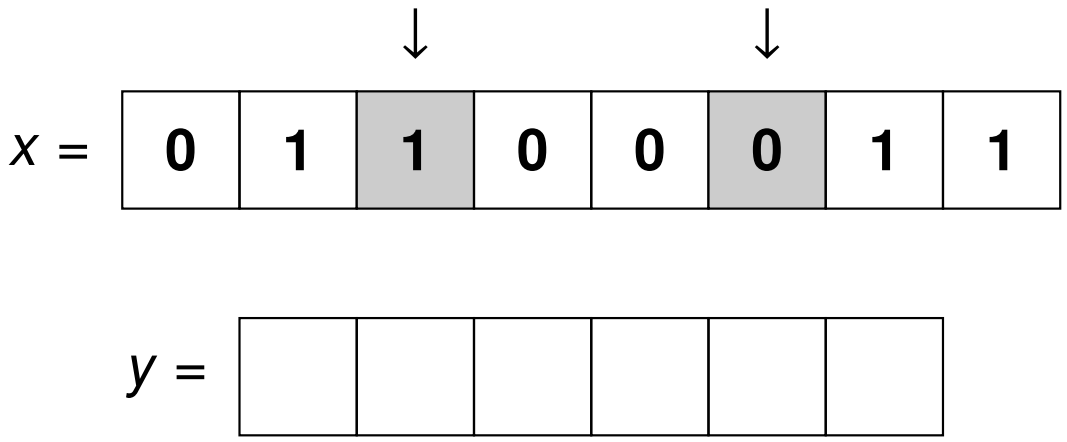


Example: CA $F : \{0,1\}^8 \to \{0,1\}^6$ induced by rule 150,

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$$

The Resiliency Game [Chor85]

2. The values for the remaining variables are randomly chosen

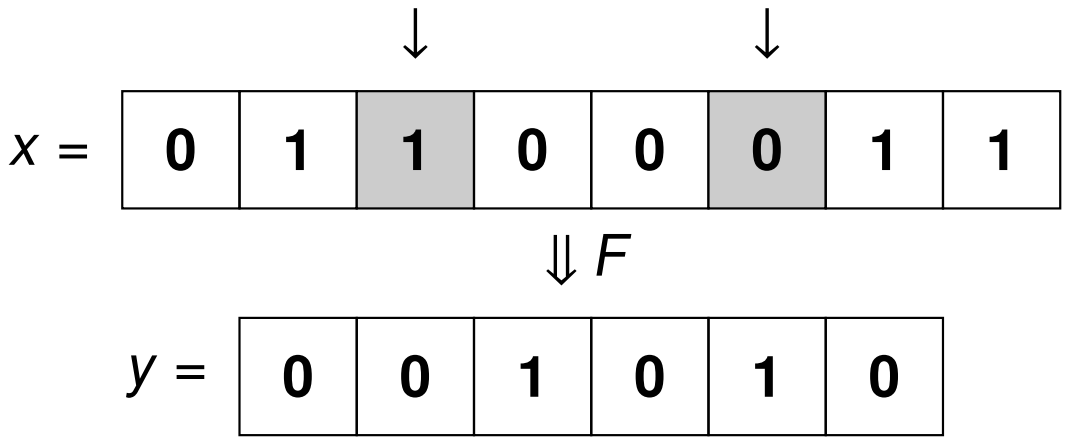


Example: CA $F : \{0,1\}^8 \to \{0,1\}^6$ induced by rule 150,

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$$

The Resiliency Game [Chor85]

3. The player applies function F

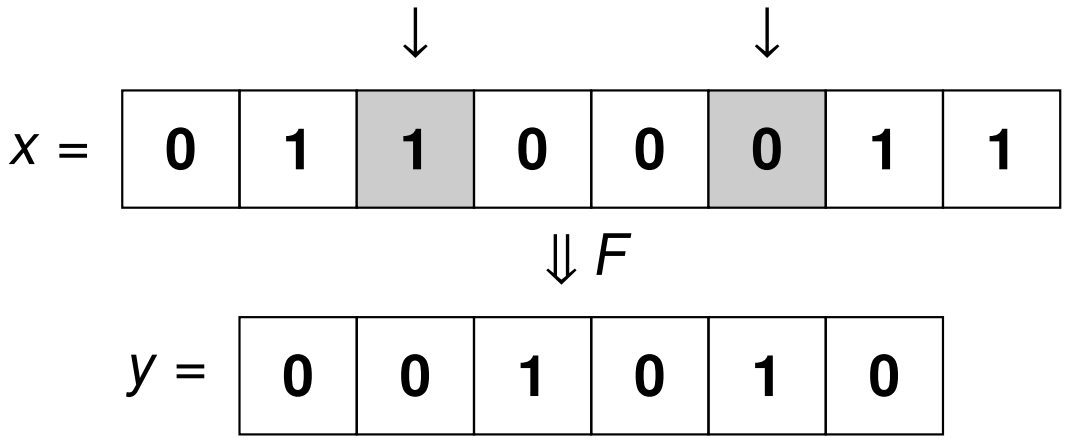


Example: CA $F : \{0,1\}^8 \to \{0,1\}^6$ induced by rule 150,

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$$

The Resiliency Game [Chor85]

- Outcome: if $F(x)$ is uniformly distributed over $\mathbb{F}_2^m$, then the player wins. Otherwise, the adversary wins



Example: CA $F : \{0,1\}^8 \to \{0,1\}^6$ induced by rule 150,

$$f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$$

Winning Strategy for the Player: choose a t-resilient function

Bipermutive Cellular Automata

Definition (Bipermutivity)

A single-output Boolean function $f : \{0,1\}^n \to \{0,1\}$ is bipermutive if, fixing either the leftmost or the rightmost $n-1$ variables, the resulting restriction $f|_{n-1} : \{0,1\} \to \{0,1\}$ is a permutation

Equivalently, f is bipermutive if

$$f(x_1, x_2, \cdots, x_{n-1}, x_n) = x_1 \oplus g(x_2, \cdots, x_{n-1}) \oplus x_n$$

where $g : \{0,1\}^n \to \{0,1\}$

Example: Rule 150, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$, with $g(x_2) = x_2$

Main Result

In [Leporati13], the following result was proved:

Theorem

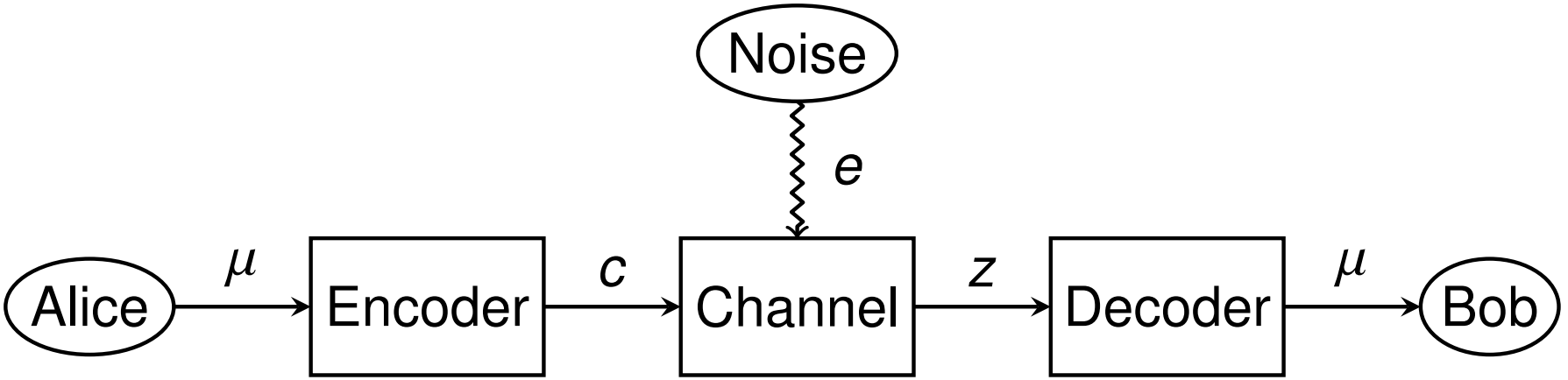
Let $f : \{0,1\}^n \to \{0,1\}$ be bipermutive. Then, f is 1-resilient

We generalized this result to CA global rules:

Theorem

Given a CA with n cells and bipermutive local rule $f : \{0,1\}^{2r+1} \to \{0,1\}$, the global rule $F : \{0,1\}^n \to \{0,1\}^{n-2r}$ induced by f is 1-resilient

Error-Correcting Codes – Communication Model



- $\mu \in \{0,1\}^m$: message
- $c \in \{0,1\}^n$: codeword ($n > m$)
- $e \in \{0,1\}^n$: error pattern
- $z = c \oplus e$ (received word)

Linear Codes

Definition

A (n, m, d) binary linear code C of minimum distance d is an m-dimensional subspace of $\mathbb{F}_2^n = \{0,1\}^n$, such that for all $c_1, c_2 \in C$

$$d_H(c_1, c_2) \geq d$$

where d_H denotes the Hamming distance

$$g_1, \cdots, g_m \in \mathbb{F}_2^n \text{ basis of } C \Leftrightarrow G = \begin{pmatrix} g_1 \\ \vdots \\ g_m \end{pmatrix} m \times n \text{ generator matrix of } C$$

Encoding: vector-matrix multiplication

$$\mu \mapsto c = \mu G$$

Error Correction – Syndrome Decoding

- Parity Check Matrix: a $(n-m)\times n$ matrix H such that

$$s = Hz^\top = 0 \Leftrightarrow z \in C$$

s: Syndrome of z

- Suppose $z = c \oplus e$, $c \in C$ and $e \in \mathbb{F}_2^n$. Then

$$Hz^\top = H(c \oplus e)^\top = \cancel{Hc^\top} \oplus He^\top = He^\top$$

Syndrome Decoding: find $e \in \mathbb{F}_2^n$ and return $c = z \oplus e$

Cyclic Codes

Definition

A (n, m, d) linear code is cyclic if for all $c = (c_0, c_1, \cdots, c_{n-1}) \in C$

$$\sigma(c) = (c_1, \cdots, c_{n-1}, c_0) \in C$$

- Generator Matrix:

$$G = \begin{pmatrix} g_0 & \cdots & g_{n-m} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-m} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & g_0 & \cdots & g_{n-m} \end{pmatrix}$$

- Parity-check Matrix:

$$H = \begin{pmatrix} h_m & \cdots & h_0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & h_m & \cdots & h_0 & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & h_m & \cdots & h_0 \end{pmatrix}$$

Linear CA

- Local rule: linear combination of the neighborhood cells

$$f(x_0, \cdots, x_{2r}) = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \ , \ a_i \in \mathbb{F}_2$$

- Global rule: $m \times (m + 2r)$ $2r+1$-diagonal transition matrix

$$M_F = \begin{pmatrix} a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{2r} \end{pmatrix}$$

$$x = (x_0, \cdots, x_{n-1}) \mapsto M_F x^\top$$

Linear CA are Cyclic Codes

$$M_F = \begin{pmatrix} a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & a_0 & \cdots & a_{2r} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & a_0 & \cdots & a_{2r} \end{pmatrix}$$

$$G = \begin{pmatrix} g_0 & \cdots & g_{n-m} & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & g_0 & \cdots & g_{n-m} & 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & g_0 & \cdots & g_{n-m} \end{pmatrix}$$

Linear CA $\Leftrightarrow$ Cyclic codes

Question: How is encoding/decoding performed?

Encoding in Linear CA

Remark: if a_0, $a_{2r} \neq 0$ (f is bipermutive) then

$$y_i = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \;\Rightarrow\; x_{2r} = a_0 x_0 \oplus \cdots \oplus y_i$$

1. Initialize the leftmost $2r$ cells $(x_0, \cdots, x_{2r})$

$x =$	**0**	**1**	**?**	**?**	**?**	**?**	**?**	**?**
$y =$	**1**	**0**	**0**	**1**	**1**	**0**		

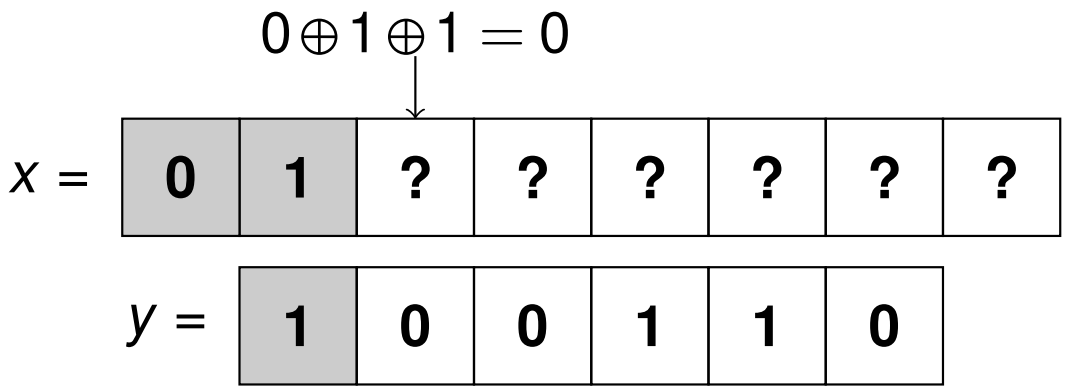
Example: rule 150, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$

Encoding in Linear CA

Remark: if a_0, $a_{2r} \neq 0$ (f is bipermutive) then

$$y_i = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \;\Rightarrow\; x_{2r} = a_0 x_0 \oplus \cdots \oplus y_i$$

2. Compute $x_{2r} = x_{2r} = a_0 x_0 \oplus \cdots \oplus y_0$



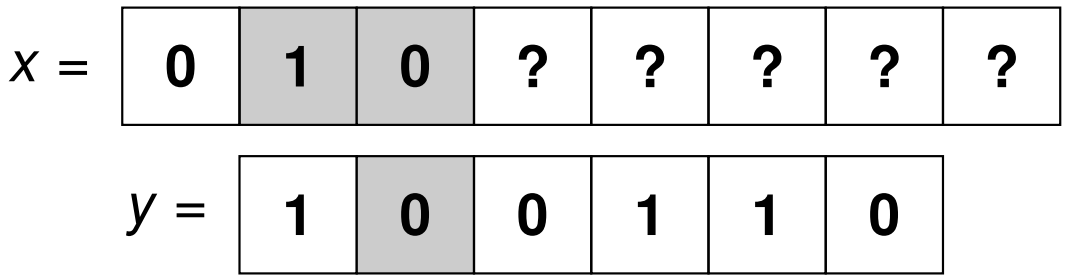
Example: rule 150, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$

Encoding in Linear CA

Remark: if a_0, $a_{2r} \neq 0$ (f is bipermutive) then

$$y_i = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \;\Rightarrow\; x_{2r} = a_0 x_0 \oplus \cdots \oplus y_i$$

3. Shift the $(2r)$-cell window one place to the right



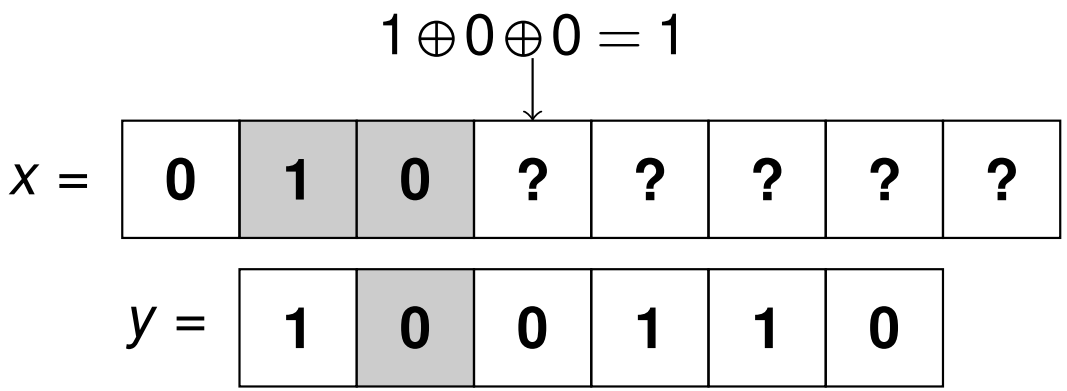
Example: rule 150, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$

Encoding in Linear CA

Remark: if a_0, $a_{2r} \neq 0$ (f is bipermutive) then

$$y_i = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \;\Rightarrow\; x_{2r} = a_0 x_0 \oplus \cdots \oplus y_i$$

4. Compute $x_\delta = a_0 x_1 \oplus \cdots \oplus y_1$



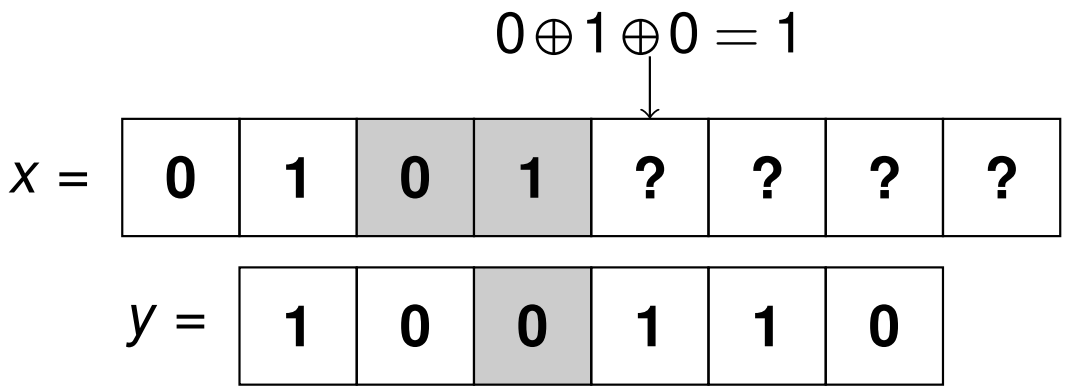
Example: rule 150, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$

Encoding in Linear CA

Remark: if a_0, $a_{2r} \neq 0$ (f is bipermutive) then

$$y_i = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \;\Rightarrow\; x_{2r} = a_0 x_0 \oplus \cdots \oplus y_i$$

5. Repeat until preimage is complete



Example: rule 150, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$

Encoding in Linear CA

Remark: if a_0, $a_{2r} \neq 0$ (f is bipermutive) then

$$y_i = a_0 x_0 \oplus \cdots \oplus a_{2r} x_{2r} \;\Rightarrow\; x_{2r} = a_0 x_0 \oplus \cdots \oplus y_i$$

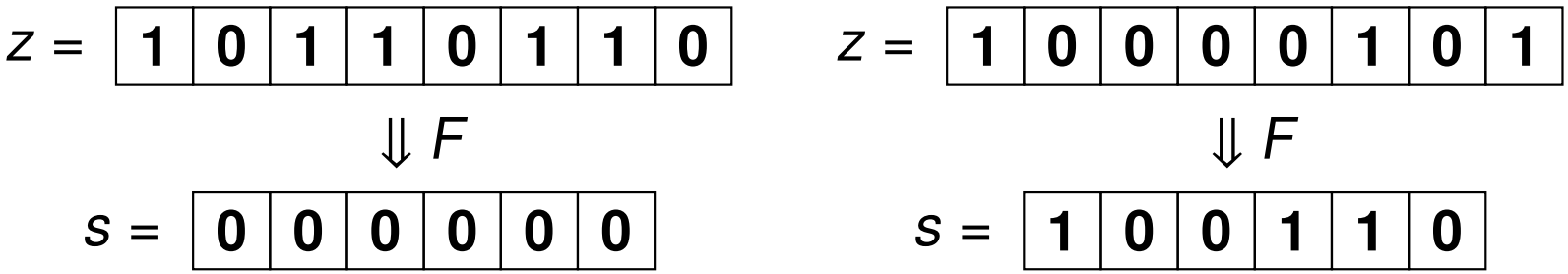
5. Repeat until preimage is complete

$x =$	**0**	**1**	**0**	**1**	**1**	**1**	**1**	**0**
$y =$		**1**	**0**	**0**	**1**	**1**	**0**	

Example: rule 150, $f(x_1, x_2, x_3) = x_1 \oplus x_2 \oplus x_3$

Decoding in Linear CA

- CA Transition Matrix $\Leftrightarrow$ Parity Check Matrix
- Syndrome computation is performed by CA global rule



(a) $s = \underline{0} \Rightarrow$ No errors

(b) $s \neq \underline{0} \Rightarrow$ Errors occurred

Last Missing Piece: minimum distance d

Putting the Pieces Together

Theorem ([Stin04])

A linear function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ defined by a matrix M_F is $(d-1)$–resilient iff M_F is the generator matrix of a (n, m, d) linear code.

- Our theorem shows that every bipermutive linear CA induces a cyclic code with minimum distance $d \geq 2$, since the global rule is 1-resilient
- One can view the design of linear cyclic codes as the search of high resilient CA global rules.

Summary

- Study of the cryptographic properties of CA global rules, focusing on resiliency
- Main result: all bipermutive CA global rules are 1-resilient
- Linear CA are equivalent to linear cyclic codes
- Minimum distance $\Leftrightarrow$ Resiliency of CA global rule

Future directions

Cyclic codes form a broad category of linear codes:

- Reed-Solomon Codes
- BCH Codes
- Reed-Muller Codes
- ...

Applications to cryptography:

- MDS matrices for diffusion layer in block ciphers
- Secret sharing schemes
- Analysis of other properties of CA global rules (nonlinearity,...)

References

- [Chor85] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich, R. Smolensky: The bit extraction problem or t-resilient functions. In: Proceedings of FOCS '85, pp. 396–407. IEEE Computer Society (1985)
- [Leporati13] Leporati, A., Mariot, L.: 1-Resiliency of Bipermutive Cellular Automata Rules. In: AUTOMATA 2013, LNCS 8155, pp. 110-123 (2013)
- [Stins04] Stinson, D.R.: Combinatorial Designs: Constructions and Analysis. Springer, Heidelberg (2004)
- [Wolfram86] Wolfram, S.: Random Sequence Generation by Cellular Automata. Adv. Appl. Math. 7(2), 123–169 (1986)