

# Asynchrony Immune Cellular Automata

4th ACA Workshop – ACRI 2016 – Fez

Luca Mariot<sup>1,2</sup>

<sup>1</sup> DISCO, Università degli Studi Milano - Bicocca, Italy

<sup>2</sup> I3S, Université Nice Sophia Antipolis, France

[luca.mariot@disco.unimib.it](mailto:luca.mariot@disco.unimib.it)

September 7, 2016

# Asynchronous CA Model

- ▶ One-dimensional array of  $n$  binary cells  $c = (c_1, \dots, c_n)$
- ▶ Local update rule  $f : \{0, 1\}^{2r+1} \rightarrow \{0, 1\}$
- ▶ *Asynchrony mask*  $s \in \{0, 1\}^{n-2r}$ ,  $s = (s_r, \dots, s_{n-r})$

$$c_i(t+1) = \begin{cases} f(c_{i-r}, \dots, c_i, \dots, c_{i+r}) & , \text{ if } s_i = 0 \\ c_i & , \text{ if } s_i = 1 \end{cases}$$

Example:  $f(c_{i-1}, c_i, c_{i+1}) = c_{i-1} \oplus c_i \oplus c_{i+1}$  (Rule 150)

(a) Synchronous update

$c(t) =$ 

0	1	1	0	0	1	0	1
---	---	---	---	---	---	---	---



$c(t+1) =$ 

0	0	1	1	1	0
---	---	---	---	---	---

$s =$ 

0	0	0	0	0	0
---	---	---	---	---	---

(b) Asynchronous update

$c(t) =$ 

0	1	1	0	0	1	0	1
---	---	---	---	---	---	---	---



$c(t+1) =$ 

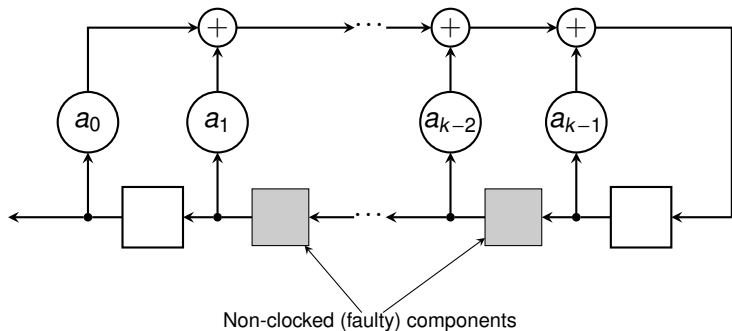
0	1	1	0	1	0
---	---	---	---	---	---

$s =$ 

0	1	0	1	0	0
---	---	---	---	---	---

# Side-Channel Attacks

- ▶ Target the implementation of a cipher
- ▶ **Idea:** Gain information on the internal state of a cipher by injecting faults and tracking them
- ▶ Considered attack: **clock faults**



## Definition (Balancedness)

A CA  $F : \{0, 1\}^n \rightarrow \{0, 1\}^{n-2r}$  is **balanced** if every configuration of  $n - 2r$  cells has exactly  $2^{2r}$  preimages under  $F$

**Remark:** Balancedness is a critical cryptographic property: unbalanced CA have statistical biases exploitable by an attacker

## Problem

*Which CA stay balanced under clock faults?*

# Towards Asynchrony Immunity... (Game Formulation)

1. The *user* chooses a balanced CA  $F : \{0, 1\}^n \rightarrow \{0, 1\}^{n-2r}$

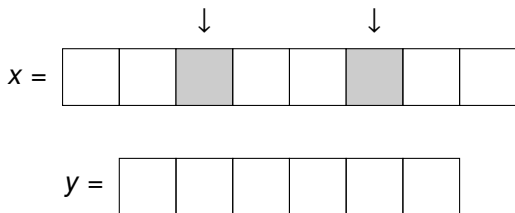
$$x = \begin{array}{|c|c|c|c|c|c|c|c|} \hline & & & & & & & \\ \hline \end{array}$$

$$y = \begin{array}{|c|c|c|c|c|c|} \hline & & & & & \\ \hline \end{array}$$

Example: CA  $F : \{0, 1\}^8 \rightarrow \{0, 1\}^6$  induced by rule 60,  
 $f(x_1, x_2, x_3) = x_2 \oplus x_3$

# Towards Asynchrony Immunity... (Game Formulation)

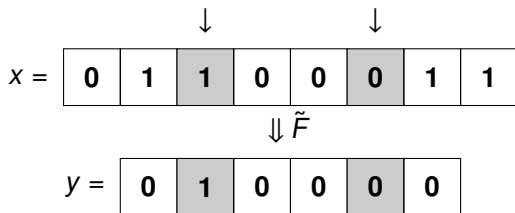
2. The *adversary* blocks the update of  $j < t$  cells



Example: CA  $F : \{0, 1\}^8 \rightarrow \{0, 1\}^6$  induced by rule 60,  
 $f(x_1, x_2, x_3) = x_2 \oplus x_3$

# Towards Asynchrony Immunity... (Game Formulation)

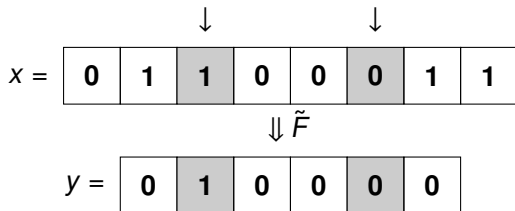
3. The user evaluates the global rule of the asynchronous CA  $\tilde{F}$



Example: CA  $F : \{0, 1\}^8 \rightarrow \{0, 1\}^6$  induced by rule 60,  
 $f(x_1, x_2, x_3) = x_2 \oplus x_3$

# Towards Asynchrony Immunity... (Game Formulation)

- ▶ **Outcome:** if  $\tilde{F}$  is still balanced, then the user wins. Otherwise, the adversary wins



Example: CA  $F : \{0, 1\}^8 \rightarrow \{0, 1\}^6$  induced by rule 60,  
 $f(x_1, x_2, x_3) = x_2 \oplus x_3$

**Asynchrony Immune CA  $\Leftrightarrow$  winning strategies for the player**



# Asynchrony Immunity: Definition

**Difference with Resiliency Game** [Chor85]: choice of the *values* of the cells by the adversary  $\Rightarrow$  **stronger attack hypothesis**

## Definition

A local rule  $f : \{0, 1\}^{2r+1} \rightarrow \{0, 1\}$  is  $(t, n)$ -asynchrony immune (( $t, n$ )-AI) if, for all  $0 < k \leq n - 2r$  and for all asynchrony masks  $s$  of weight at most  $t$ , the synchronous CA  $F : \{0, 1\}^{k+2r} \rightarrow \{0, 1\}^k$  and the asynchronous CA  $\tilde{F} : \{0, 1\}^{k+2r} \rightarrow \{0, 1\}^k$  are balanced

# Asynchrony Immunity: Basic Properties

- ▶ Idea: search for AI rules with additional crypto properties (high nonlinearity), pruning the search space through symmetries
- ▶ **Reflection:**  $f^R(x_1, \dots, x_{2r+1}) = f(x_{2r+1}, \dots, x_1)$
- ▶ **Complement:**  $f^C(x_1, \dots, x_{2r+1}) = 1 \oplus f(x_1, \dots, x_{2r+1})$

## Lemma

*Let  $f : \{0, 1\}^{2r+1} \rightarrow \{0, 1\}$  be a  $(t, n)$ -AI local rule. Then,  $f^R$  and  $f^C$  are  $(t, n)$ -AI as well*

# Search for AI Rules

- ▶ **Goal:** find nonlinear (3, 10)-AI rules
- ▶ In elementary CA, only rule 60 is (3, 10)-AI, but it is linear
- ▶ Extended the search to the  $2^{2^4}$  4-neighborhood local rules
- ▶ 18 (3, 10)-AI rules, 12 of which nonlinear
- ▶ All the rules found are *center-permutive*, i.e.

$$f(x_{i-r}, \dots, x_i, \dots, x_{i+r}) = x_i \oplus g(x_{i-r}, \dots, x_{i+r})$$

## Conjecture




Let  $f$  be a  $(t, n)$ -asynchrony immune local rule. Then,  $f$  is center-permutive

## Summary:

- ▶ Introduction of a new cryptographic property modelled using asynchronous CA
- ▶ Possible applications in side-channel countermeasures for CA-based ciphers
- ▶ Performed a computer search of  $(3, 10)$ -AI nonlinear 4-neighborhood rules

## Perspectives:

- ▶ Prove (or disprove) the center-permutivity conjecture
- ▶ Restrict the search to surjective CA [Amoroso72]
- ▶ Design a family of bent (maximally nonlinear) AI rules
- ▶ Cryptanalyze existing ciphers (e.g., KECCAK [Keccak11])

-  [Amoroso72] Amoroso, S., Patt, Y.N.: Decision Procedures for Surjectivity and Injectivity of Parallel Maps for Tessellation Structures. J. Comput. Syst. Sci. 6(5): 448-464 (1972)
-  [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)
-  [Keccak11] Bertoni, G., Daemen, J., Peeters, M., Assche, G.V.: The KECCAK reference. <http://keccak.noekeon.org/> (2011)