1-Resiliency of Bipermutive CA Rules

AUTOMATA 2013 - September 17-19 - Giessen

Alberto Leporati, Luca Mariot

Dipartimento di Informatica, Sistemistica e Comunicazione,
Università degli Studi Milano - Bicocca,
Viale Sarca 336/14, 20124 Milano, Italy
alberto.leporati@unimib.it, l.mariot@campus.unimib.it

September 17, 2013

Outline

Cellular Automata: Basic Definitions

Definition

A finite one-dimensional cellular automaton (CA) is a 4-tuple $\langle n, A, r, f \rangle$ where $n \in \mathbb{N}$ is the number of cells, A is the set of local states, $r \in \mathbb{N}$ is the radius and $f : A^{2r+1} \to A$ is the local rule.

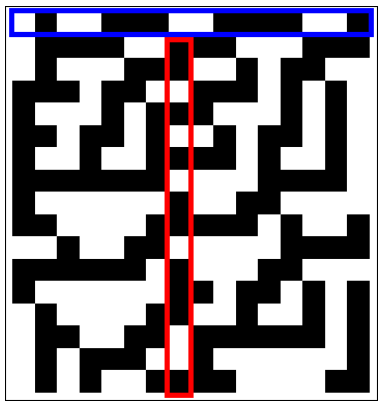
- Each cell i updates its state c_i in parallel by computing $f(c_{i-r}, \cdots, c_i, \cdots, c_{i+r})$
- Periodic CA: the array of n cells is seen as a ring, thus the first cell follows the last one
- When $|A| = 2$, the local rule can be considered as a boolean function, that is a mapping $f : \mathbb{F}_2^m \to \mathbb{F}_2$, where $m = 2r + 1$

Pseudorandom Numbers and Sequences

- In cryptography and computer simulations pseudorandom numbers and sequences are most commonly used, since Truly random numbers are impractical to produce
- A binary sequence $s \in \{0,1\}^*$ is called pseudorandom if it cannot be distinguished from a truly random sequence in polynomial time
- A pseudorandom number generator (PRNG) is a function g which takes as input a short truly random sequence (the seed) and expands it in an arbitrarily long pseudorandom sequence

Wolfram's PRNG

- Main idea: sample the trace of a particular cell in a CA equipped with the elementary rule 30 (radius $r = 1$) as a pseudorandom sequence, using a random initial configuration as seed



Example with 16 cells CA, 8^{th} cell sampled. Wolfram suggested to use a CA having at least $n = 127$ cells

- Pseudorandom quality of the generated sequences assessed only by means of statistical tests in [Wolfram, 1986]

Walsh Transform

- There are several properties that a boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ used in a cryptographic PRNG should satisfy, in order to resist to specific attacks
- Some of these properties can be characterized through the Walsh transform of f, defined for all $\omega \in \mathbb{F}_2^m$ as:

$$\hat{F}(\omega) = \sum_{x \in \mathbb{F}_2^m} \hat{f}(x) \cdot (-1)^{\omega \cdot x}$$

where $\hat{f}(x) = (-1)^{f(x)}$ and $\omega \cdot x$ denotes the usual dot product on $\mathbb{F}_2^m$ between ω and x

Cryptographic Properties of Boolean Functions

Some important cryptographic properties for a boolean function f:

- Balancedness: The counterimages $f^{-1}(0)$ and $f^{-1}(1)$ have the same cardinality, 2^{m-1}. This is verified if and only if $\hat{F}(0) = 0$
- Nonlinearity: The Hamming distance of f from the set of affine functions. It is computed as $NI(f) = 2^{-1}(2^m - W_{\max}(f))$, where $W_{\max}(f)$ is the maximum absolute value of $\hat{F}(\omega)$ for all $\omega \in \mathbb{F}_2^m$
- Correlation-immunity: f is k-th order correlation immune if and only if $\hat{F}(\omega) = 0$ for all $\omega \in \mathbb{F}_2^m$ which have at most k nonzero coordinates

Cryptographic Properties of Elementary CA Rules

- The elementary rule 30 used by Wolfram is both balanced and nonlinear, but it is not first order correlation-immune
- More generally, [Martin, 2008] showed that there are no elementary rules which are both nonlinear and 1-resilient (that is, balanced and first order correlation immune)
- CA-based PRNGs using nonlinear elementary rules are thus vulnerable to correlation attacks
- Consequence: necessity to explore the sets of rules having radii $r > 1$ to find good trade-offs between cryptographic properties and pseudorandom quality of the generated sequences

Permutive and Bipermutive Functions

Notation: by $(x, \tilde{x}_{\{i\}})$ we denote the vector

$$(x, \tilde{x}_{\{i\}}) = (x_1, \ldots, x_{i-1}, \tilde{x}, x_i, \ldots, x_{m-1}) \in \mathbb{F}_2^m \ ,$$

where $x \in \mathbb{F}_2^{m-1}$ and $\tilde{x} \in \mathbb{F}_2$.

Definition

A boolean function $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is called i-permutive if, for all $x \in \mathbb{F}_2^{m-1}$, it results that

$$f(x, 0_{\{i\}}) \neq f(x, 1_{\{i\}}) \ .$$

Function f is called bipermutive if it is both 1-permutive and m-permutive.

Chaotic CAs Induced by Bipermutive Rules

- Bipermutive rules are known to induce strongly chaotic CAs, when the latter are considered as discrete time dynamical systems on the set of biinfinite configurations $A^{\mathbb{Z}}$
- In particular, the two following results hold:
  - A CA based on a rule f which is bipermutive is expansively chaotic [Cattaneo et al., 2000]
  - A CA based on a rule f which is either 1-permutive or m-permutive is mixing chaotic [Cattaneo et al., 2002]
- Hence, bipermutive rules seem to be good candidates to design a CA-based PRNG

Main Theoretical Findings on Bipermutive Rules

Lemma

If $f : \mathbb{F}_2^m \to \mathbb{F}_2$ is i-permutive for any $i \in \{1, \cdots, m\}$, then f is balanced.

Lemma

Let $f : \mathbb{F}_2^m \to \mathbb{F}_2$ be bipermutive.
Then f is first order correlation- immune.

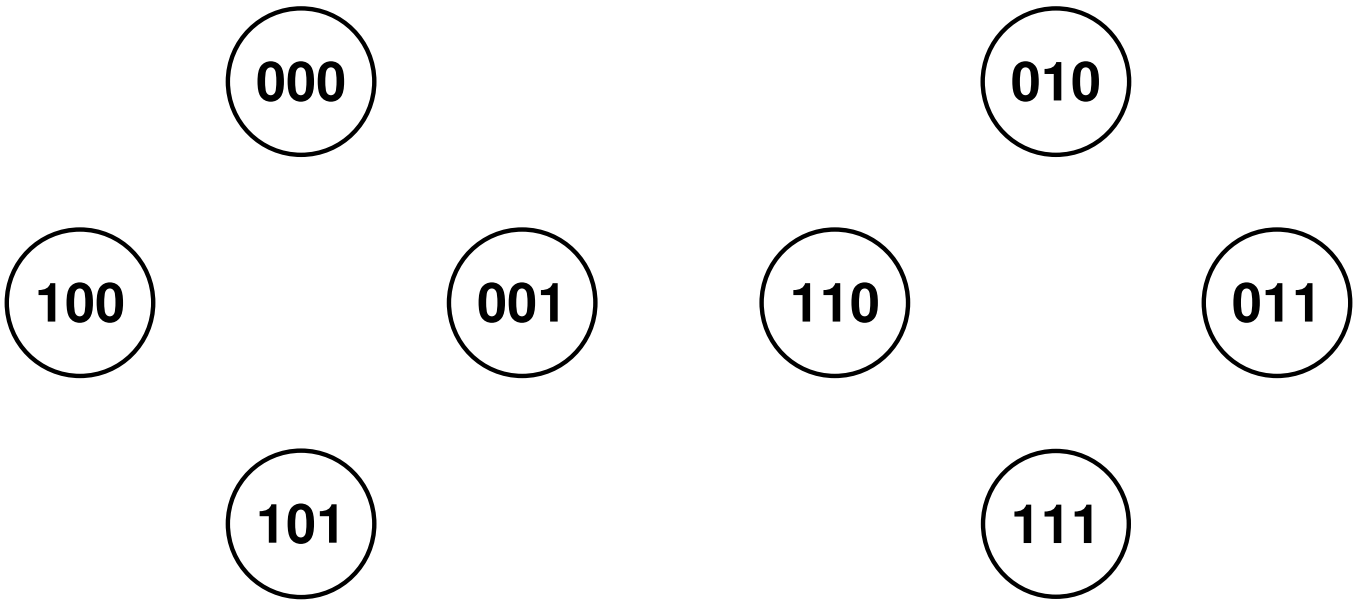
By combining the two lemmas, the following result holds:

Theorem

Let $f : \mathbb{F}_2^m \to \mathbb{F}_2$ be a bipermutive boolean function.
Then, f is 1-resilient.

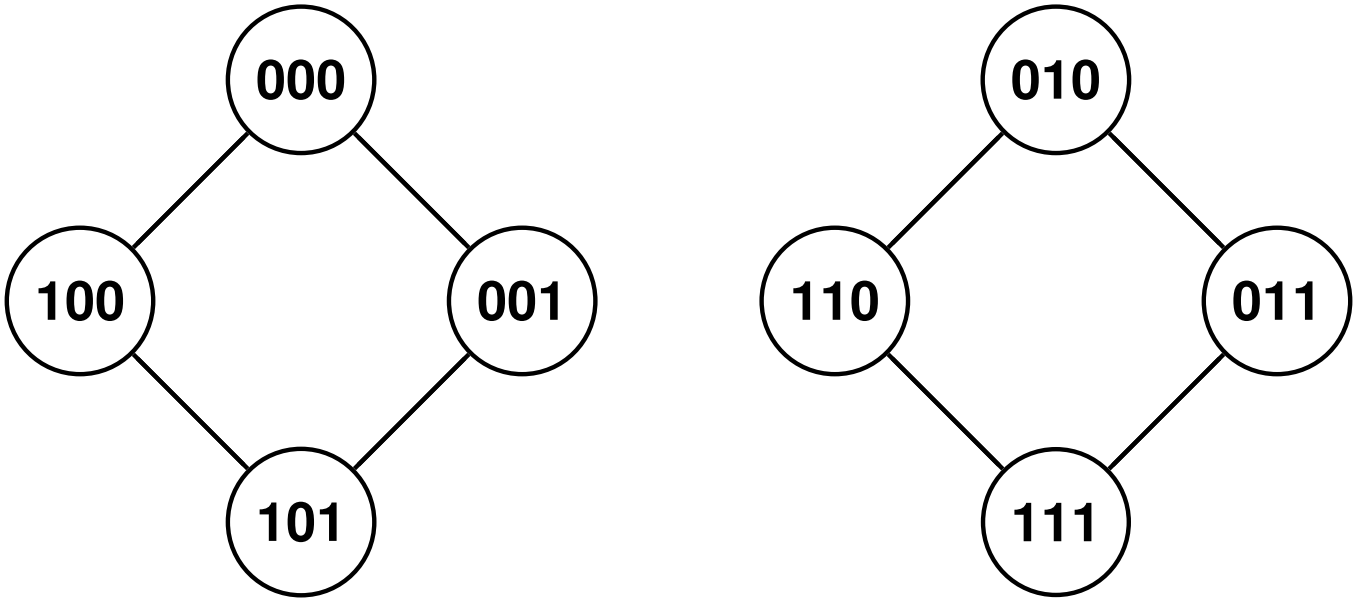
Graph-Based Enumerative Encoding for Bipermutive Rules (1/4)

- Idea: represent the input vectors $x \in \mathbb{F}_2^m$ as vertices of an undirected graph $G = (V, E)$



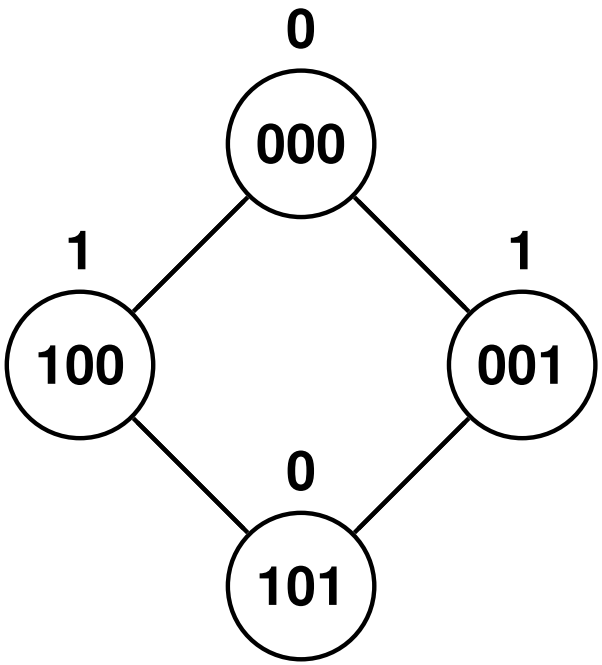
Graph-Based Enumerative Encoding for Bipermutive Rules (2/4)

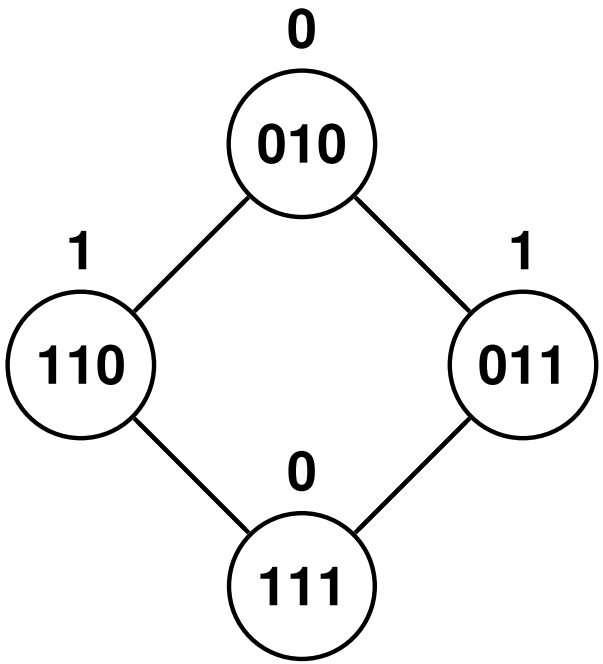
- Only those inputs which differ either in the leftmost or rightmost variable and agree on the remaining coordinates are connected



Graph-Based Enumerative Encoding for Bipermutive Rules (3/4)

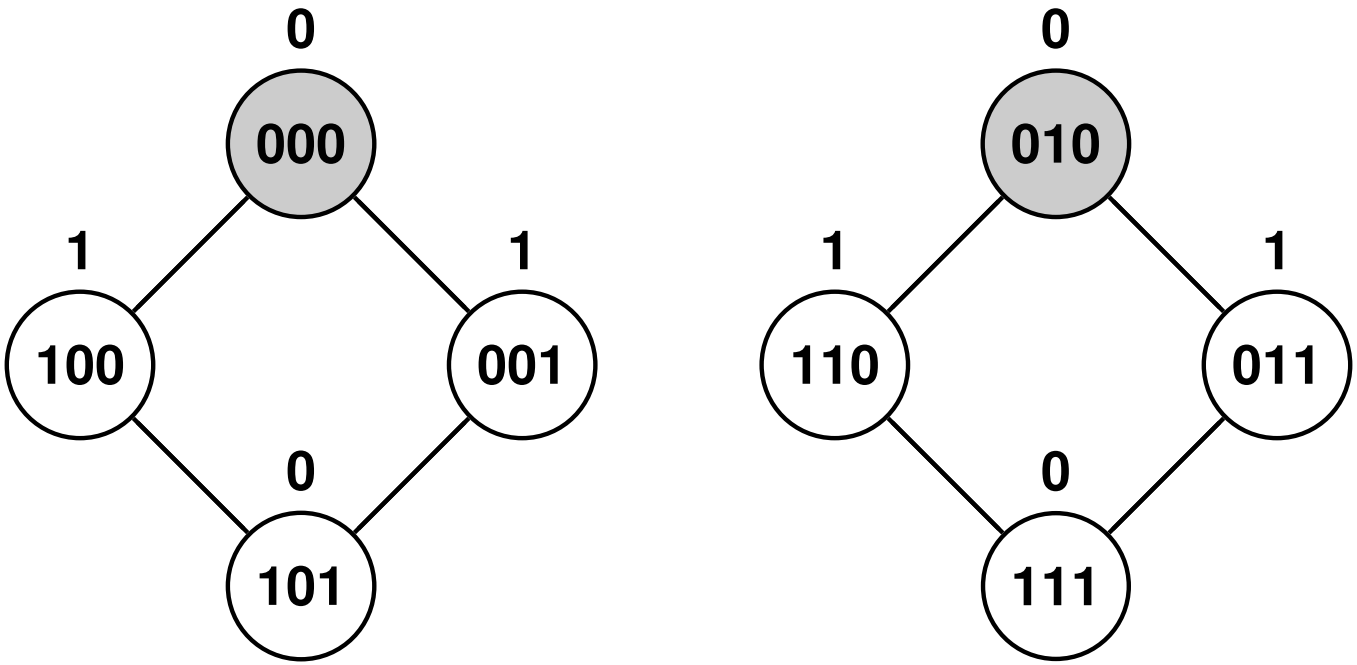
- A bipermutive rule is represented as a label function $f : V \to \mathbb{F}_2$, where the values of adjacent labels differ





Graph-Based Enumerative Encoding for Bipermutive Rules (4/4)

- f is indexed by a binary string of length 2^{m-2}, which specifies the configuration of its representatives (shaded in gray)



Representation of rule 90, corresponding to configuration string $c = 00$

Application to the Case $r = 2$

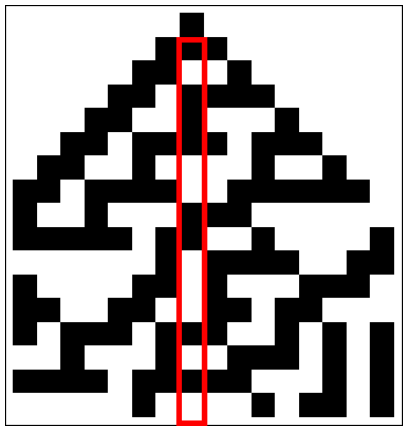
- The enumerative encoding has been applied to explore the space of $2^{2^{5-2}} = 256$ bipermutive rules of radius $r = 2$
- Algorithm: for all 256 configuration strings do:
  - Instantiate the corresponding bipermutive rule on the graph G
  - Compute the Walsh Transform
  - Check the cryptographic properties
  - If the rule is nonlinear and 2-resilient, select it
- The selected rules were 56, all of which had nonlinearity $NI(f) = 8$

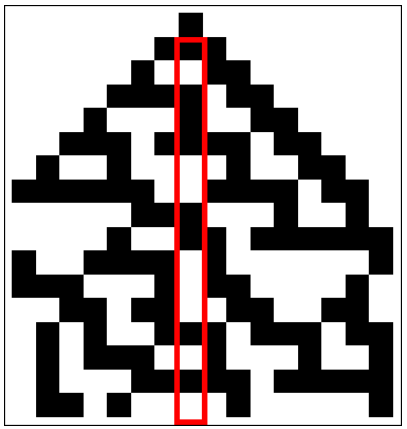
ENT Tests

- The selected 56 rules have been investigated with the ENT randomness tests suite [Walker, 2008], using a periodic CA of $n = 64$ cells and sampling the trace of the 32^{nd} cell
- For each rule, a single sequence of $2^{16} = 65536$ bits has been generated using the initial configuration containing only a 1 in the 32^{nd} cell
- The results obtained by rule 30 have been used as a selection benchmark: Chi-Square p-value in the interval $[0.1, 0.9]$, error in the approximation of $\pi < 1\%$
- The resulting rules meeting these selection criteria were 28

Reflexive pairs

- 24 rules out of 28 presented the same ENT results in pairs
- The rules in the pairs are related by the reflexive transformation: given $f : \mathbb{F}_2^m \to \mathbb{F}_2$, its reflection is defined as $f_R(x) = f(x_R)$, where x_R is vector x considered in reverse order
- The sequences produced for the ENT tests are thus the same





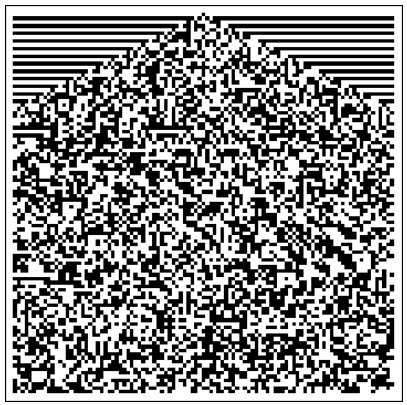
Example: Symmetric trace generation between rule 30 (left) and its reflection, rule 86 (right).

NIST Tests

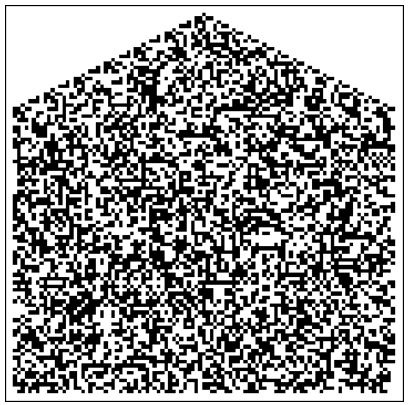
- 16 rules passing the ENT tests have been successively studied by means of the more stringent NIST suite [NIST, 2010]
- Tested rules:
  - for each of the 12 reflexive pairs, only the rule having the smallest Wolfram code
  - 4 self-reflexive rules (i.e., those rules such that $f = f_R$)
- Test Parameters for each rule:
  - Sample of $N = 1000$ pseudorandom sequences
  - Periodic CA of 64 cells with the trace of the 32^{nd} cell sampled
  - Length of each sequence: 10^6 bits
- Thus, for each rule 125MB of pseudorandom data have been analysed

Final Rules

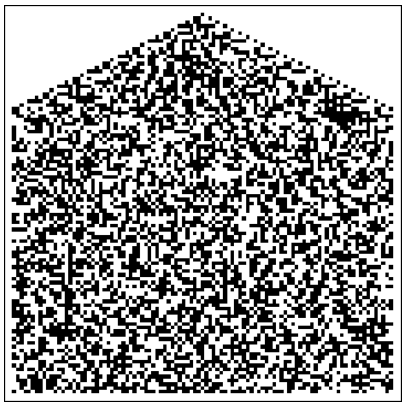
- Among the 16 rules tested with the NIST suite, three of them passed all the 187 tests, like the elementary rule 30



(a) Rule 1452976485



(b) Rule 1520018790



(c) Rule 2778290790

Conclusions

- Bipermutive rules are interesting for cryptographic CA-based PRNGs design, since they are both strongly chaotic and 1-resilient
- A graph-based enumerative encoding has been used to explore the set of 256 bipermutive rules of radius 2. The rules resulting nonlinear and 2-resilient have been subjected to the ENT and NIST statistical tests
- Three rules passed all the tests, like rule 30. However, they cannot be used alone in the design of a CA-based PRNG
- As a matter of fact, there are other cryptographic properties which were not considered, such as the Strict Avalanche Criterion and the algebraic degree

Future Developments

Some possible future directions of research on the subject include:

- Study the class of bipermutive rules with respect to other cryptographic properties
- Use combinatorial techniques to explore the spaces of bipermutive rules of higher radii which result sufficiently limited for an exhaustive search
- Use heuristic methods to search the spaces of bipermutive rules which are too large for an exhaustive search

Some Additional Results...

The presented results have been extended in the master thesis of the second author. Key findings:

- It is possible to deduce the cryptographic properties of a bipermutive rule r by checking the properties of its configuration string c, the latter considered itself as a boolean function
- The set of bipermutive rules of radius $r = 3$ has been explored by spanning the space of balanced boolean functions in 5 variables
- The sets of bipermutive rules of radius $r = 4$, 5 and 6 have been explored by means of Genetic Algorithms, Particle Swarm Optimization and Ant Colony Optimization

References


Cattaneo, G., Finelli, M., Margara, L.: Investigating Topological Chaos by Elementary Cellular Automata Dynamics. Theor. Comput. Sci. 244(1-2), 219-244 (2000)


Cattaneo, G., Dennunzio, A., Margara, L.: Chaotic Subshifts and Related Languages Applications to One-Dimensional Cellular Automata. Fundam. Inform. 52(1-3), 39-80 (2002)


Martin, B.: A Walsh Exploration of Elementary CA Rules. J. Cell. Aut. 3(2), 145-156 (2008)


National Institute of Standards and Technology: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. Special Publication 800-22, Revision 1a (2010)


Walker, J.: ENT Randomness Test Suite, `http://www.fourmilab.ch/random/`


Wolfram, S.: Random Sequence Generation by Cellular Automata. Adv. Appl. Math. 7(2), 123-169 (1986)