Leakage Squeezing using Cellular Automata

Sandip Karmakar and Dipanwita Roy Chowdhury,

Indian Insitute of Technology, Kharagpur, WB, India

Outline

- Introduction
- Background
  - CA
  - Leakage Squeezing
- Leakage Squeezing using CA
  - Non-uniform Nonlinear CA
  - Rules Chosen
  - Experimental Setup
  - Results
- Conclusion

Introduction

- Cellular Automata (CA) are self-evolving systems.
- Each cell updates automatically following a rule embedded into it.
- Leakage Squeezing is a novel scheme for securing sensitive data from unwanted leakages.

Background- CA

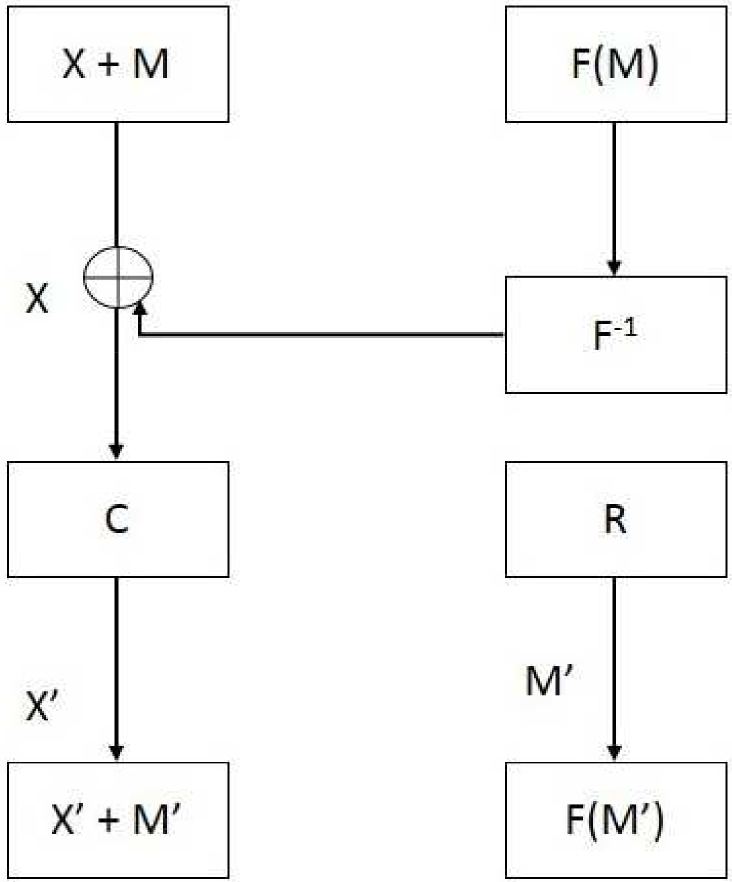
- We consider 1D, 2-value, 2-neighbourhood CA
- It consists of a single dimensional array of cells
- Each cell contains Boolean values
- Each cell also follows a rule, which is a Boolean function of left, right and self cells' values
- The consideration here is on non-uniform CA, -rules vary through cells

Background – Leakage Squeezing

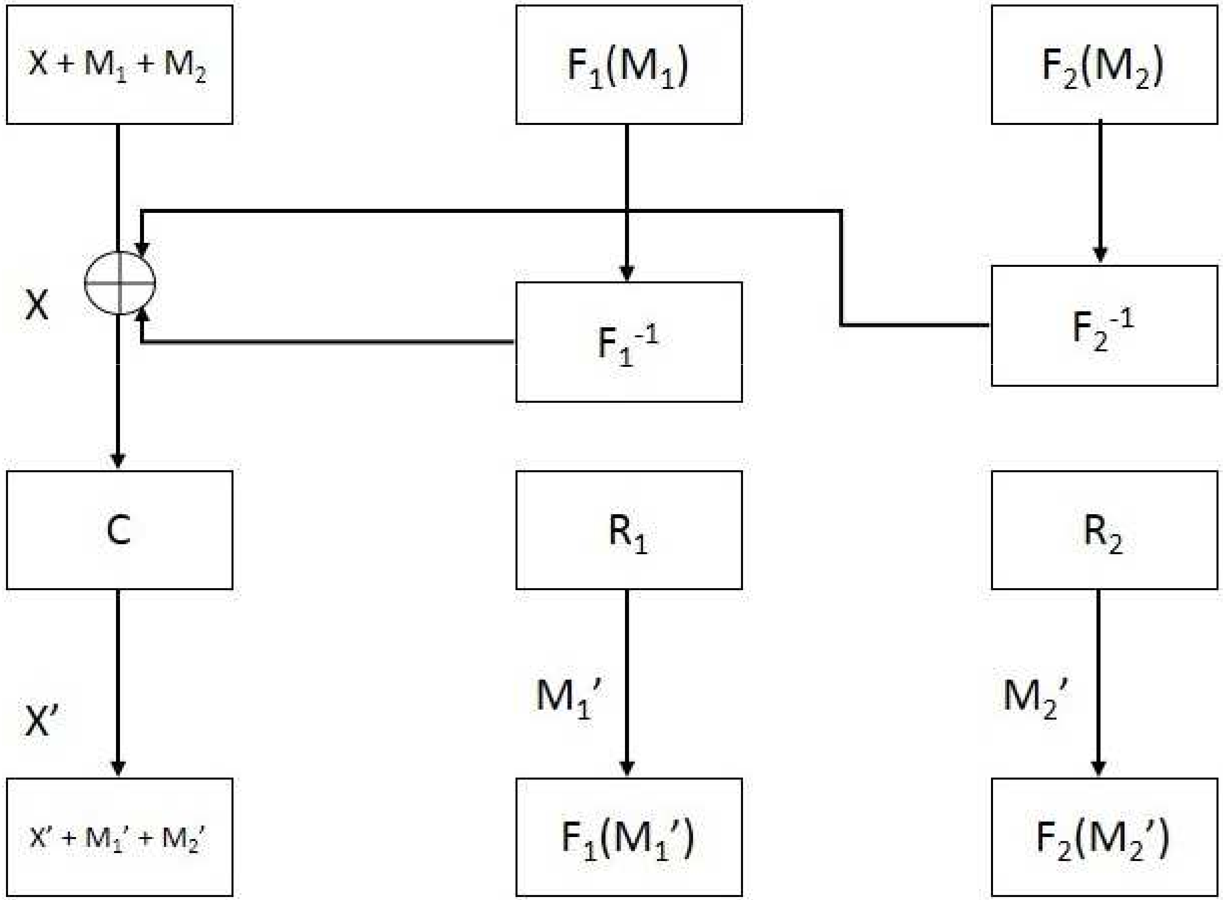
- Idea is not to store sensitive values in registers
- This avoids unwanted leakages (side channel leakages)
- Instead the value is masked, S+M.
- A bijection of the mask is also stored, F(M)
- When needed we can get back the value by,

  S = S+M+(1/F)F(M), since, (1/F) is known.

Leakage Squeezing of Order One



Leakage Squeezing of Order Two



Leakage Squeezing

- Leakage squeezing of order d is satisfied by a (2n, n, d+1) code.
- An extensive study of such code generation and their properties using linear CA is done [9].

d-monomial Test

- It states that a good pseudorandom generator in its ANF Boolean form with n variables should contain, $(1/2)({}^{n}C_{d})$, d-degree monomials.

Leakage Squeezing using CA

- The problem with the design for Leakage Squeezing using Linear Bijections is that, it is much easily invertible.
- To make it stronger the design bijection should have other cryptographic properties, like, balancedness, algebraic dgeree, resiliency, nonlinearity and should be good in d-monomial tests.

Leakage Squeezing using CA

- We consider a number of non-uniform nonlinear CA introduced in [5].
- These are,
- 1. Ruleset 1 : Rules 30 and 60 spaced alternately over a 3-neighbourhood CA.
- 2. Ruleset 2 : Rules 30, 60 and 90 spaced alternately over a 3-neighbourhoodCA.
- 3. Ruleset 3 : Rules 30, 60, 90 and 120 spaced alternatively over a 3-neighbourhood CA.

Non-uniform Nonlinear CA

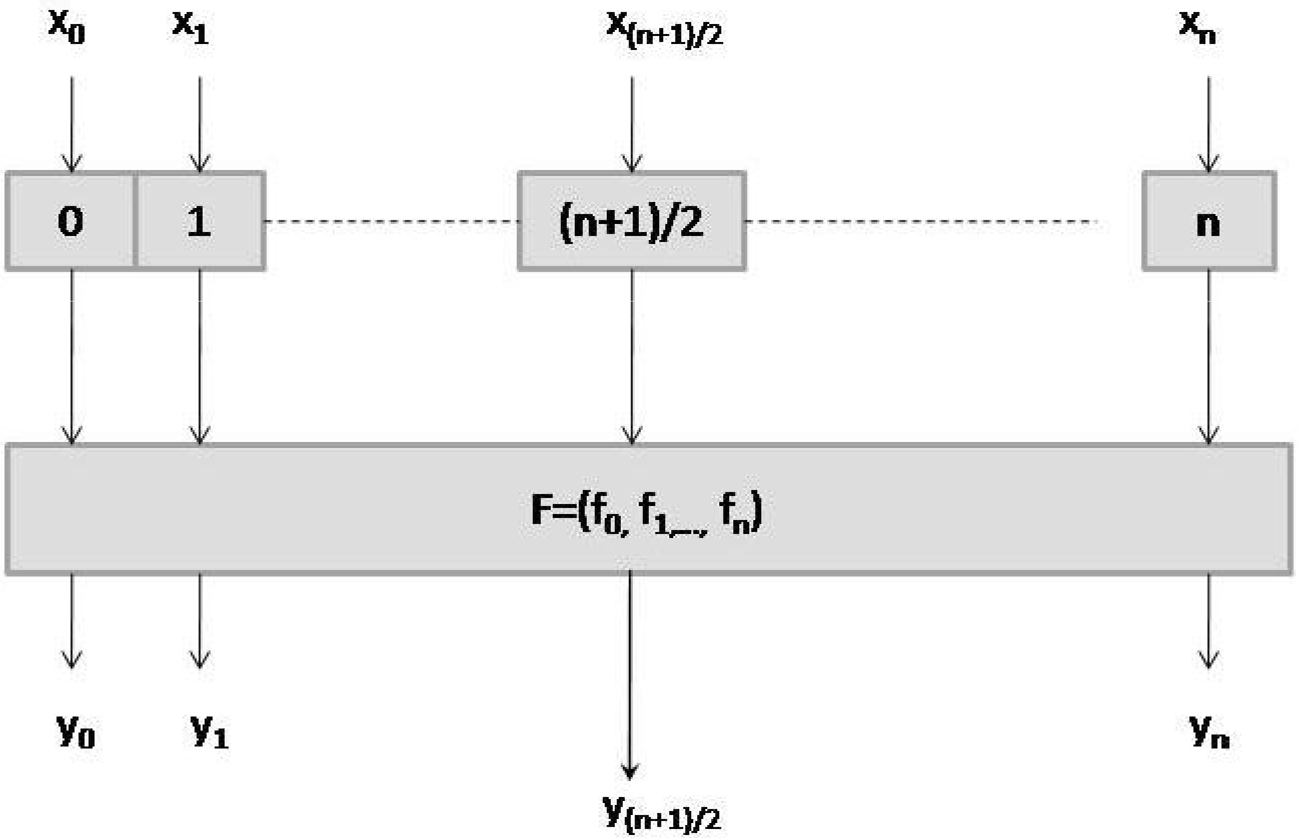
- 4. Ruleset 4 : Rules 30, 60, 90, 120 and 150 spaced alternatively over a 3-neighbourhood CA.
- 5. Ruleset 5 : Rules 30, 60, 90, 120, 150, 180, 210, 240 spaced alternatively over a 3-neighbourhood CA.
- 6. Ruleset 6 : Rules 30, 60, 90, 120, 150, 180, 210, 240, 15, 45 spaced alternatively over a 3-neighbourhood CA.
- Note that none of the CA is max-length, so, we need to devise some way to reach max-length.

Functional Model of Analysis

- Each cell is considered to have a Boolean unknown literal xi.
- At the (t+1)th iteration, the output of the each cell, c, is updated as,

  $c(t+1)=f_c(t)[(c-1)(t), c(t), (c+1)(t)]$
- This is iterated for multiple cycles.
- The generated ANF is analyzed for cryptographic properties.

Functional Model of Analysis



Experiment

- Experiment is done using Mathematica.
- Experiment could only be carried out till 3rd iteration, since, beyond the process takes huge time/memory.
- These three iterations are indicative to the design.

Results-Balancedness

	Iterations		
Rules	1	2	3
Ruleset 1	Y	Y	Y
Ruleset 2	Y	Y	Y
Ruleset 3	Y	Y	Y
Ruleset 4	Y	Y	Y
Ruleset 5	Y	Y	Y
Ruleset 6	Y	Y	Y

Results-Nonlinearity

	Nonlinearity		
	Iterations		
Rules	1	2	3
Ruleset 1	2	8	32
Ruleset 2	2	8	48
Ruleset 3	2	8	48
Ruleset 4	2	8	48
Ruleset 5	2	8	32
Ruleset 6	2	2	48

Results-Resiliency

	Resiliency		
	Iterations		
Rules	1	2	3
Ruleset 1	1	0	0
Ruleset 2	2	2	1
Ruleset 3	2	2	1
Ruleset 4	2	2	1
Ruleset 5	2	2	2
Ruleset 6	2	2	1

Results-Algebraic Degree

	Algebraic Degree		
	Iterations		
Rules	1	2	3
Ruleset 1	2	2	3
Ruleset 2	2	2	3
Ruleset 3	2	3	3
Ruleset 4	2	3	4
Ruleset 5	2	3	4
Ruleset 6	2	3	4

Results-d-monomial Test

	Number of n-th degree terms			
Rules	1	2	3	4
Ruleset 1	3,3,5	1,3,3	0,0,2	0,0,0
Ruleset 2	3,3,2	1,3,3	0,0,1	0,0,0
Ruleset 3	3,2,4	1,3,5	0,1,3	0,0,0
Ruleset 4	3,2,4	1,3,7	0,1,7	0,0,2
Ruleset 5	3,2,4	1,3,5	0,2,6	0,0,3
Ruleset 6	3,2,4	1,3,5	0,2,6	0,0,3

Results-Distance

- All the rulesets show distance 2 throughout the three cycles.
- Thus order 1 leakage squeezing is guaranteed.

Conclusion

- We have shown that rulesets introduced earlier are good in cryptographic properties and are usable in cryptographic applications especially Leakage Squeezing.
- Considering all properties rulesets 5 and 6 are best candidates for the designs of bijection.

References

1. Claude Carlet, Jean-Luc Danger, Sylvain Guilley, and Houssem Maghrebi. Leakage squeezing of order two. Cryptology ePrint Archive, Report 2012/567, 2012. http://eprint.iacr.org/.
2. Eric Filiol. A new statistical testing for symmetric ciphers and hash functions. *Proc. Information and Communications Security 2002, Volume 2513 of LNCS*, 2002.
3. Howard Gutowitz. Cellular automata: Theory and experiment., 1991.
4. Markku juhani O. Saarinen. Chosen-iv statistical attacks on e-stream stream ciphers. *eSTREAM, ECRYPT Stream Cipher Project, Report 2006/013*, pages 5–19, 2006.
5. Sandip Karmakar, Debdeep Mukhopadhyay, and Dipanwita Roy Chowdhury. d-monomial Tests on Cellular Automata for Cryptographic Design. *ACRI 2010*, 2010.
6. Houssem Maghrebi, Sylvain Guilley, and Jean-Luc Danger. Leakage squeezing countermeasure against high-order attacks. In ClaudioA. Ardagna and Jianying Zhou, editors, *Information Security Theory and Practice. Security and Privacy of Mobile Devices in Wireless Communication*, volume 6633 of *Lecture Notes in Computer Science*, pages 208–223. Springer Berlin Heidelberg, 2011.
7. Bruno Martin Patrick Sole. Pseudo-random sequences generated by cellular automata. *International Conference on Relations, Orders and Graphs: Interactions with Computer Science*, 2008.
8. Bruno Martin. Patrick Sole Patrik Lacharme. Pseudo-random sequences, boolean functions and cellular automata. *Boolean Functions: Cryptography and Applications*, 2007.
9. D Roy Chowdhury S Nandi S Chattopadhyay P Pal Chaudhuri. Additive cellular automata - theory and applications., 1997.
0. S. Wolfram. Random sequence generation by cellular automata. In *Advances in Applied Mathematics, Volume-7*, pages 123–169, 1986.