Four Neighbourhood Cellular Automata as Better Cryptographic Primitives

Jimmy Jose   Dipanwita Roy Chowdhury

Crypto Research Laboratory,
Department of Computer Science and Engineering,
Indian Institute of Technology Kharagpur, India

June 8-10, 2015

Introduction

- 3-neighbourhood CA has good crypto properties.
- Can 4-neighbourhood CA be a better cryptographic primitive?
- increase in neighbourhood radius increase
  - diffusion
  - randomness
  - correlation immunity
- current work analyses cryptographic suitability of 4-neighbourhood CA

Motivation

Advantages of 3-neighbourhood CA

- diffusion
- randomness

Disadvantages of 3-neighbourhood CA

- no 3-neighbourhood nonlinear balanced rule is correlation immune [2]
  - CA using these rules are susceptible to correlation attacks
- Meier-Staffelbach Attack on CA rule 30

Literature

- analysis of 1-resilient 4-neighbourhood CA rules [3]
- analysis of 1-resilient 5-neighbourhood CA rules [5]
- nonlinear and resilient rules from 5-neighbourhood bipermutative CA rules [4]

Our Contribution

- constructed a class of 4-neighbourhood CA
  - rule structure functionally resemble 3-neighbourhood CA rule 30
- studied cryptographic properties of this class
- inapplicability of Meier-Staffelbach attack [1] on 4-neighbourhood CA is shown

4-neighbourhood CA

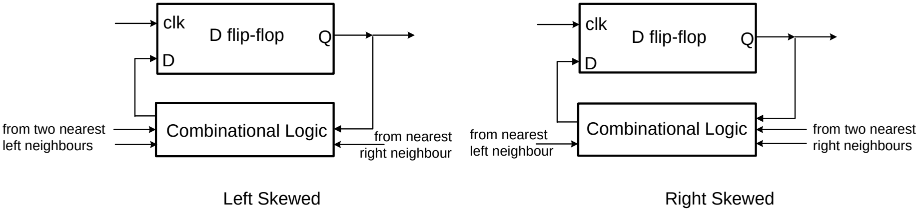
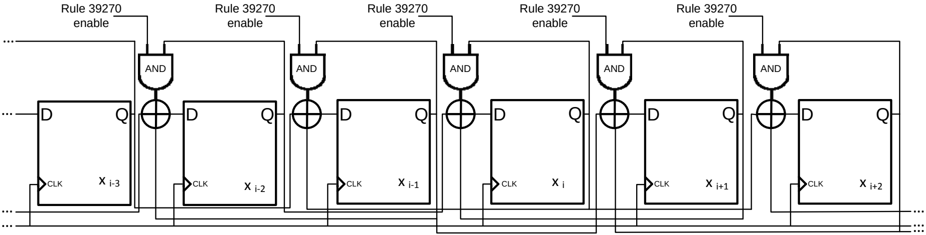


Figure: Single Cell in Left Skewed and Right Skewed 4-neighbourhood CA

- left skewed CA - the cells in the CA depend on two left, itself, and one right cells for their update
- right skewed CA - the cells in the CA depend on one left, itself, and two right cells for their update

4-neighbourhood Linear Hybrid CA



Rule 21930 : $q_i(t+1) = q_{i-2}(t) \oplus q_{i+1}(t)$
Rule 39270 : $q_i(t+1) = q_{i-2}(t) \oplus q_i(t) \oplus q_{i+1}(t)$

Figure: 4-neighbourhood Linear Hybrid CA based on rules 21930, 39270 (left skewed)

Cryptographic Properties

- Nonlinearity
- Balancedness
- Correlation Immunity

Cryptographic Properties

Nonlinearity

the number of bits that must change in the truth table of the Boolean function such that it matches the truth table of the nearest affine function
Nonlinearity of $f(x_1, x_2) = x_1 \oplus x_2 \oplus 1$ is 0 and $f(x_1, x_2) = x_1.x_2 \oplus x_2$ is 1

Balancedness

if the number of 0's and number of 1's in the truth table of a Boolean function are equal, then the function is balanced
$f(x_1, x_2) = x_1 \oplus x_2 \oplus 1$ is balanced but $f(x_1, x_2) = x_1.x_2 \oplus x_2$ is not

Cryptographic Properties

Correlation Immunity

A Boolean function $f(x_1, \ldots, x_n)$ is m-th order Correlation Immune if for every subset of m or fewer variables in $x_1, \ldots, x_n$, the probability of f to take 0 and 1 is not changed given that the values of variables in the subset are fixed in advance while the value of the remaining variables are chosen independently at random

Correlation Imminity of $f(x_1, x_2) = x_1 \oplus x_2 \oplus 1$ is 1 and $f(x_1, x_2) = x_1.x_2 \oplus x_2$ is 0

3-neighbourhood Rules 30 and 246

Rule 30: $q_i(t+1) = q_{i-1}(t) \oplus (q_i(t) + q_{i+1}(t))$
Rule 246: $q_i(t+1) = q_{i-1}(t) + (q_i(t) \oplus q_{i+1}(t))$

Table: Cryptographic Properties of 3-neighbourhood Rules 30 and 246

sl. no.	Rule No	Nonlinearity			Balancedness			Correlation Immunity		
		1	2	3	1	2	3	1	2	3
1	30	2	4	36	True	True	True	0	0	0
2	246	2	6	22	False	False	False	0	0	0

Nonlinear Rules Resembling Rule 30

Table: Four-neighbourhood Nonlinear Rules

sl. no.	Rule No	Left Skewed Rule	sl. no.	Rule No	Left Skewed Rule
1	510	$q_{i-2} \oplus (q_{i-1} + q_i + q_{i+1})$	14	50070	$q_{i-1} \oplus q_i \oplus (q_{i-2} + q_{i+1})$
2	854	$(q_{i-2} + q_{i+1}) \oplus (q_{i-1} + q_i)$	15	51510	$q_{i-2} \oplus q_i \oplus (q_{i-1} + q_{i+1})$
3	1334	$(q_{i-2} + q_i) \oplus (q_{i-1} + q_{i+1})$	16	57630	$q_{i-2} \oplus q_{i-1} \oplus (q_i + q_{i+1})$
4	3870	$(q_{i-1} \oplus (q_{i-2} + q_i + q_{i+1})$	17	60350	$(q_{i-2} \oplus q_{i-1} \oplus q_i) + q_{i+1}$
5	4382	$(q_{i-2} + q_{i-1}) \oplus (q_i + q_{i+1})$	18	60894	$(q_{i-2} \oplus q_{i-1} \oplus q_{i+1}) + q_i$
6	13110	$q_i \oplus (q_{i-2} + q_{i-1} + q_{i+1})$	19	61438	$(q_i + q_{i+1}) + (q_{i-2} \oplus q_{i-1})$
7	21846	$q_{i+1} \oplus (q_{i-2} + q_{i-1} + q_i)$	20	63990	$(q_{i-2} \oplus q_i \oplus q_{i+1}) + q_{i-1}$
8	28662	$(q_{i-2} \oplus q_{i-1}) + (q_i \oplus q_{i+1})$	21	64510	$(q_{i-1} + q_{i+1}) + (q_{i-2} \oplus q_i)$
9	31710	$(q_{i-2} \oplus q_i) + (q_{i-1} \oplus q_{i+1})$	22	65022	$(q_{i-1} + q_i) + (q_{i-2} \oplus q_{i+1})$
10	32190	$(q_{i-2} \oplus q_{i+1}) + (q_{i-1} \oplus q_i)$	23	65430	$(q_{i-1} \oplus q_i \oplus q_{i+1}) + q_{i-2}$
11	39318	$q_i \oplus q_{i+1} \oplus (q_{i-2} + q_{i-1})$	24	65470	$(q_{i-2} + q_{i+1}) + (q_{i-1} \oplus q_i)$
12	42390	$q_{i-1} \oplus q_{i+1} \oplus (q_{i-2} + q_i)$	25	65502	$(q_{i-2} + q_i) + (q_{i-1} \oplus q_{i+1})$
13	43350	$q_{i-2} \oplus q_{i+1} \oplus (q_{i-1} + q_i)$	26	65526	$(q_{i-2} + q_{i-1}) + (q_i \oplus q_{i+1})$

Cryptographic Properties of the Selected Rules

sl. no.	Rule No	Nonlinearity			Balancedness			Correlation Immunity		
		1	2	3	1	2	3	1	2	3
1	510	2	28	224	True	True	True	0	0	0
2	854	6	38	366	False	False	False	0	0	0
3	1334	6	30	412	False	False	False	0	0	0
4	3870	2	32	272	True	True	False	0	0	0
5	4382	6	42	412	False	False	False	0	0	0
6	13110	2	32	272	True	True	False	0	0	0
7	21846	2	28	224	True	True	True	0	0	0
8	28662	4	40	304	False	False	False	0	0	0
9	31710	4	40	392	False	False	True	0	0	1
10	32190	4	48	400	False	False	False	0	0	0
11	39318	4	32	368	True	True	True	1	1	1
12	42390	4	40	408	True	True	True	1	0	1
13	43350	4	48	384	True	True	True	1	2	1

Cryptographic Properties of the Selected Rules (continued)

sl. no.	Rule No	Nonlinearity			Balancedness			Correlation Immunity		
		1	2	3	1	2	3	1	2	3
14	50070	4	52	428	True	False	False	1	0	0
15	51510	4	40	408	True	True	True	1	0	1
16	57630	4	32	368	True	True	True	1	1	1
17	60350	4	16	60	False	False	False	0	0	0
18	60894	4	16	92	False	False	False	0	0	0
19	61438	2	2	2	False	False	False	0	0	0
20	63990	4	16	92	False	False	False	0	0	0
21	64510	2	3	5	False	False	False	0	0	0
22	65022	2	2	2	False	False	False	0	0	0
23	65430	4	16	60	False	False	False	0	0	0
24	65470	2	4	8	False	False	False	0	0	0
25	65502	2	3	5	False	False	False	0	0	0
26	65526	2	2	2	False	False	False	0	0	0

Meier-Staffelbach Attack

From the state values of the i-th cell - temporal sequence - for $n+1$ time steps from t to $t+n$, the attack tries to find the state value of cells at the t-th time step

Exploits the many-to-one mapping from the right-hand initial states to the temporal sequence or its adjacent sequence

Meier-Staffelbach Attack (Continued)

Triangle for 3-neighbourhood Rules

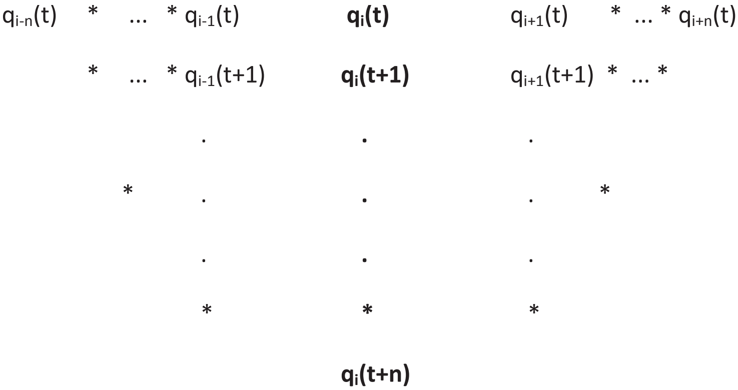


Figure: Triangle determined by initial site vector $q_{i-n}(t), \ldots, q_{i+n}(t)$ for

Attack Principle

- A random set of values for right-hand initial states may give correct right adjacent sequence even if the values were wrong
- Knowledge of right adjacent sequence is equivalent to knowledge of seed

Triangle for 4-neighbourhood Rules

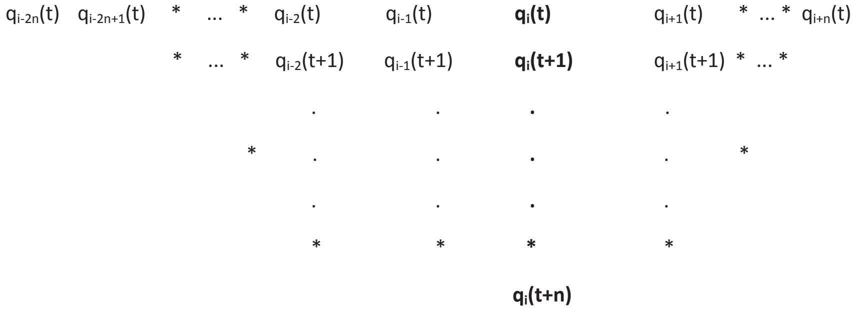


Figure: Triangle determined by initial site vector $q_{i-2n}(t), \ldots, q_{i+n}(t)$ for 4-neighbourhood rules

Meier-Staffelbach Attack on 4-neighbourhood CA (continued)

- Right-hand initial states not sufficient to compute right adjacent sequence
- Knowledge of right adjacent sequence is not sufficient to compute the seed

Example with a 4-neighbourhood CA rule

LHS of the triangle

Rule 57630: $q_i(t+1) = q_{i-2}(t) \oplus q_{i-1}(t) \oplus (q_i(t) + q_{i+1}(t))$
calculation of right adjacent sequence needs left adjacent sequence too (not known) unlike 3-neighbourhood CA

RHS of the triangle

Rewriting :$q_{i+1}(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus (q_{i+1}(t) + q_{i+2}(t))$
Rearranging:$q_{i-1}(t) = q_{i+1}(t+1) \oplus q_i(t) \oplus (q_{i+1}(t) + q_{i+2}(t))$
to find the values in cells at column $i-1$, we require the values in column $i+2$ also (unlike 3-neighbourhood CA) in addition to the values in columns i and $i+1$

Comparison

If K_s – the seed
K_{r1} – the right adjacent sequence
K_{r2} – the sequence to the right of right-adjacent sequence
In 3-neighbourhood CA, $F : \{K_s\} \rightarrow \{K_{r1}\}$
In 4-neighbourhood CA, $F : \{K_s\} \rightarrow \{K_{r1}, K_{r2}\}$

Conclusion

- studied the cryptographic suitability of a class of 4-neighbourhood nonlinear CA rules
- shown the inapplicability of Meier-Staffelbach attack against 4-neighbourhood CA

References

- Meier, W., Staffelbach, O.:Analysis of pseudo random sequences generated by cellular automata. In: EUROCRYPT '91. pp. 186–199 (1991)
- Siegenthaler, T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Transactions on Information Theory 30(5), 776–780 (1984)
- Lacharme, P., Martin, B., Solé, P., et al.: Pseudo-random sequences, boolean functions and cellular automata. Proceedings of BFCA pp. 80–95 (2008)
- Leporati, A., Mariot, L.: 1-resiliency of bipermutive cellular automata rules. In: AUTOMATA 2013. pp. 110-123 (2013)
- Formenti, E., Imai, K., Martin, B., Yunés, J-B.: Advances on random sequence generation by uniform cellular automata. In: Computing with New Resources, pp. 56-70 (2014)

Thank You