CARPenter: A Cellular Automata Based Resilient Pentavalent Stream Cipher

Rohit Lakra Anita John Jimmy Jose

Department of Computer Science and Engineering
National Institute of Technology Calicut, India

September 20, 2018
Como, Italy

eSTREAM project

- eSTREAM project [1] - an effort to find out compact efficient stream ciphers
- divided into two categories:
  - software oriented
    - fast encryption in software
  - hardware oriented
    - fast encryption with less hardware

CA in Cryptography

- Accepted as good pseudorandom number generators.
- Some Cellular Automata Based Stream Ciphers -
  - CASTREAM [2]
  - CAvium [4]
  - CAR30 [5]
  - FResCA [3].
- Advantage of higher radii CA -
  - The pseudorandom properties of 3 and 4 neighbourhood CA have been studied and they show that the neighbourhood radii has an impact on pseudorandomness.
  - Pseudorandomness increases with increase in neighbourhood radii if appropriate CA rules are applied.

CARPenter: A Cellular Automata Based Resilient Pentavalent Stream Cipher

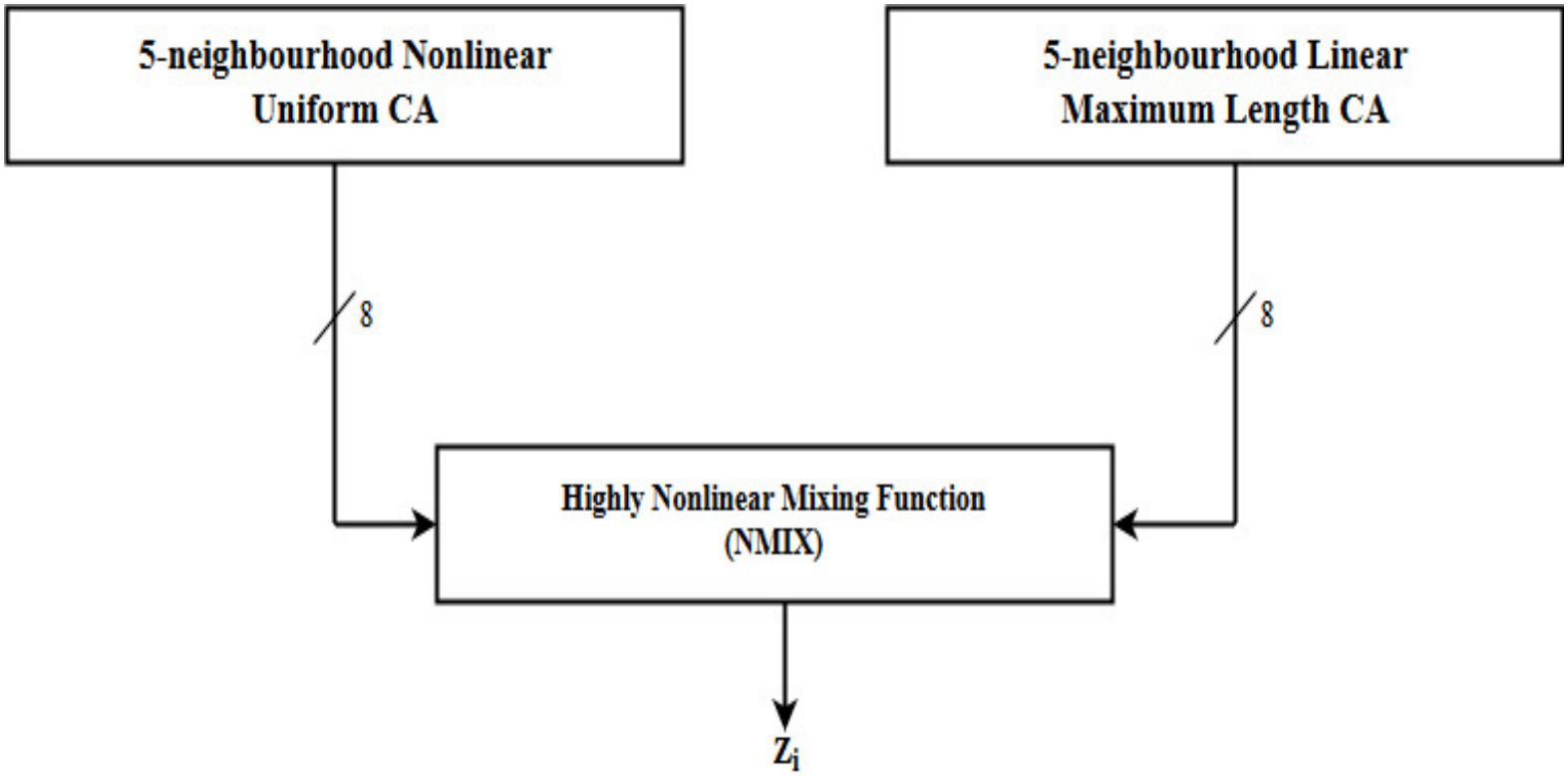

Figure 1: CARPenter Key Generation Phase

CARPenter: Nonlinear Block

1	2	...	128
1452976485 or 1520018790	1452976485 or 1520018790	...	1452976485 or 1520018790

Figure 2: Non linear block

Nonlinear Rule

- Rule 1452976485 [11]: $S_i^{t+1} = (\neg S_{i-2}^t \cdot \neg S_i^t \cdot \neg S_{i+1}^t \cdot \neg S_{i+2}^t) + (\neg S_{i-2}^t \cdot \neg S_{i-1}^t \cdot S_{i+1}^t \cdot \neg S_{i+2}^t) + (\neg S_{i-2}^t \cdot S_i^t \cdot \neg S_{i+1}^t \cdot S_{i+2}^t) + (S_{i-2}^t \cdot \neg S_i^t \cdot \neg S_{i+1}^t \cdot S_{i+2}^t) + (S_{i-2}^t \cdot S_i^t \cdot \neg S_{i+1}^t \cdot \neg S_{i+2}^t) + (\neg S_{i-2}^t \cdot S_{i-1}^t \cdot S_{i+1}^t \cdot S_{i+2}^t) + (S_{i-2}^t \cdot \neg S_{i-1}^t \cdot S_{i+1}^t \cdot S_{i+2}^t) + (S_{i-2}^t \cdot S_{i-1}^t \cdot S_{i+1}^t \cdot \neg S_{i+2}^t)$
- Rule 1520018790 [11]: $S_i^{t+1} = (\neg S_{i-2}^t \cdot \neg S_{i-1}^t \cdot \neg S_{i+1}^t \cdot \neg S_{i+2}^t) + (\neg S_{i-2}^t \cdot \neg S_{i-1}^t \cdot S_{i+1}^t \cdot \neg S_{i+2}^t) + (\neg S_{i-2}^t \cdot S_{i-1}^t \cdot \neg S_i^t \cdot \neg S_{i+2}^t) + (S_{i-2}^t \cdot \neg S_{i-1}^t \cdot \neg S_{i+1}^t \cdot \neg S_{i+2}^t) + (\neg S_{i-2}^t \cdot S_{i-1}^t \cdot S_i^t \cdot S_{i+2}^t) + (S_{i-2}^t \cdot \neg S_{i-1}^t \cdot S_{i+1}^t \cdot S_{i+2}^t) + (S_{i-2}^t \cdot S_{i-1}^t \cdot \neg S_i^t \cdot S_{i+2}^t) + (S_{i-2}^t \cdot S_{i-1}^t \cdot S_i^t \cdot \neg S_{i+2}^t)$

where '+' and '.' and $\neg$ represents OR, AND and NOT Boolean operations respectively.

CARPenter: Linear Block

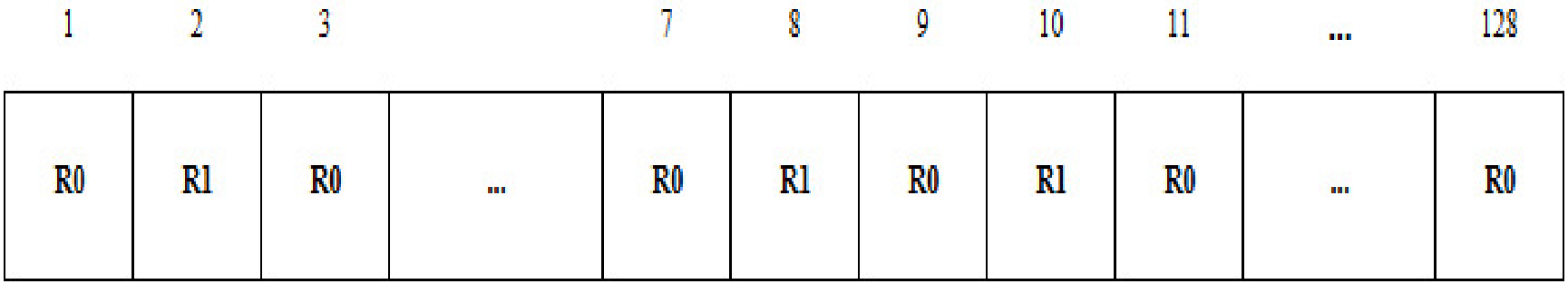

Figure 3: Linear block

- R0 : $S_i^{t+1} = S_{i-2}^t \oplus S_{i-1}^t \oplus S_{i+1}^t \oplus S_{i+2}^t$
- R1 : $S_i^{t+1} = S_{i-2}^t \oplus S_{i-1}^t \oplus S_i^t \oplus S_{i+1}^t \oplus S_{i+2}^t$

Nonlinear Mixing Block

Non-linear mixing block uses a nonlinear, balanced and reversible Boolean function NMix [8].

NMix Function

The NMix function is defined for two n-bit inputs. If inputs are $X = x_1, x_2, \ldots, x_{n-1}, x_n$ and $Y = y_1, y_2, \ldots, y_{n-1}, y_n$ and output is $Z = z_1, z_2, \ldots, z_{n-1}, z_n$, then the i^{th} bit of NMix is defined as follows.

$z_i = x_i \oplus y_i \oplus c_{i-1}$

$c_i = x_0.y_0 \oplus \cdots \oplus x_i.y_i \oplus x_{i-1}.x_i \oplus y_{i-1}.y_i$

and $x_{-1} = y_{-1} = c_{-1} = 0, 0 \leq i \leq n-1$

Working of CARPenter

- CARPenter is a Grain-like **C**ellular **A**utomata Based **R**esilient **Pent**avalent Stream Ciph**er**.
- The 128-bit key is loaded into the nonlinear block and the 128-bit IV is loaded into the linear block of the cipher.
- The cipher has two phases, namely initialization phase and keystream generation phase.

Initialization Phase

- The initialization phase consists of 16 iterations and the output is suppressed in this phase.
- During this phase, the output is fed back to the linear and nonlinear blocks.

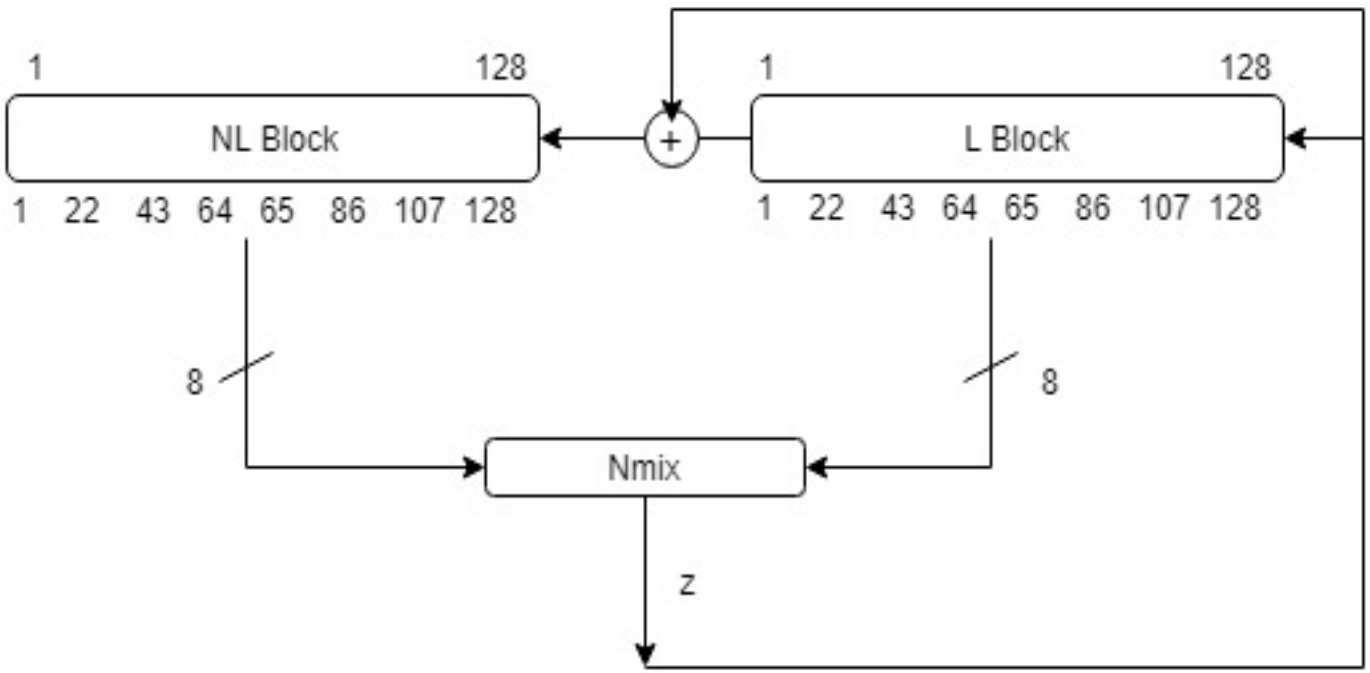

Figure 4: Cipher Initialization

Initialization Phase

- The output of the NMix function is XORed with the first bit in the linear block and this XORed value has dual role in nonlinear block.
- It acts as the second-right-neighbour of the 127^{th} bit and as both first and second right neighbour of the 128^{th} bit in the nonlinear block.

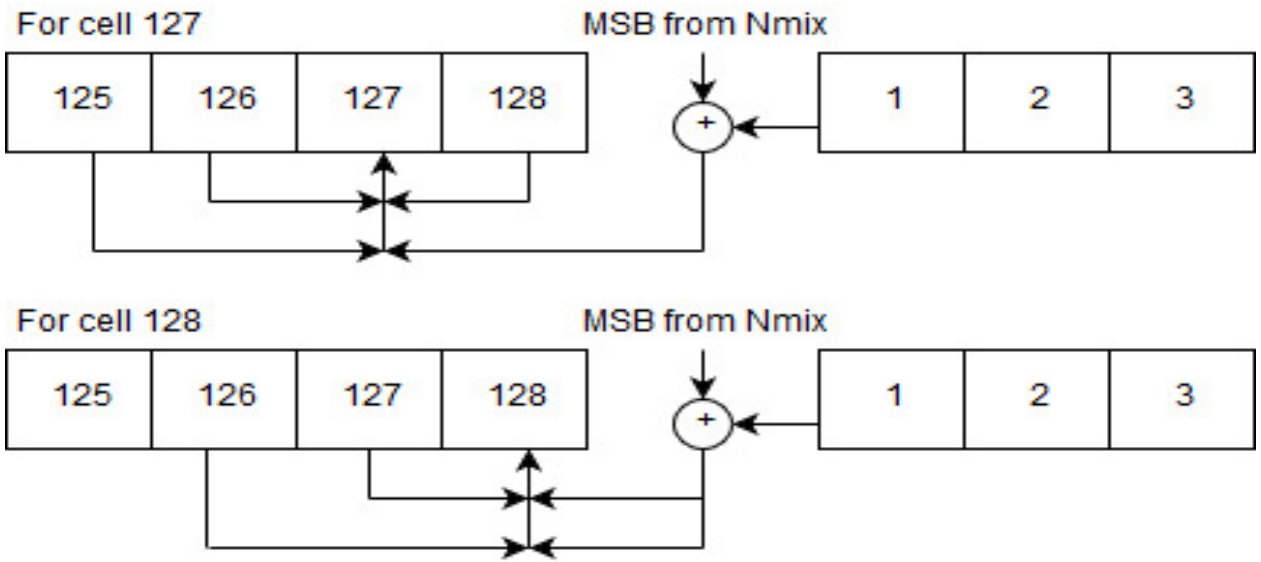

Figure 5: Updation of cell 127 and cell 128 of nonlinear block

Initialization Phase

- The output of NMix also acts as the second-right-neighbour of the 127^{th} bit and as both first and second right neighbours of the 128^{th} bit in the linear block.
- In each iteration, each bit in the nonlinear block changes its state according to any one of the 5-neighbourhood nonlinear rule 1452976485 or rule 1520018790.
- In the linear block, the state transition takes place according to the rules R0 and R1.

Initialization Phase

- Eight taps each are selected from both linear and nonlinear blocks so that the number of inputs to the NMix block are 16.
- The eight taps correspond to the bit positions 1, 22, 43, 64, 65, 86, 107 and 128 in both the blocks.
- In order to have influence of all the state bits in output in lesser number of iterations, the taps are positioned equally except the two middle ones.

Key Generation Phase

- After initialization phase, the feed back lines are removed and the keystream bits are generated.

Security Analysis

NIST Statistical Test Suite

- National Institute of Standards and Technology (NIST) has developed a statistical test suite known as NIST statistical test suite [10].
- NIST test suite is a package of 15 tests to test the randomness of pseudo-random binary sequence of arbitrary length.

Security Analysis

Randomness test of CARPenter

- To test the randomness of CARPenter, a bit stream of length 0.1 billion bits has been generated and fed to the NIST test suite.
- Input bit stream is divided into 100 keystreams of 1 million bits each by the NIST test suite.
- All the tests passed with appropriate P-values as shown in Table 1.

Security Analysis

Table 1: NIST test result

		Rule 1452976485		Rule 1520018790	
SI.No	Test Name	P-value	Status	P-value	Status
1	Frequency test	0.955835	Pass	0.657933	Pass
2	Block Frequency test	0.494392	Pass	0.289667	Pass
3	Cumulative Sums test	0.595549	Pass	0.108791	Pass
4	Runs test	0.616305	Pass	0.955835	Pass
5	Longest Runs test	0.171867	Pass	0.534146	Pass
6	Rank test	0.739918	Pass	0.191687	Pass
7	FFT test	0.153763	Pass	0.616305	Pass
8	Non overlapping template test	0.595549	Pass	0.289667	Pass
9	Overlapping template test	0.834308	Pass	0.595549	Pass
10	Universal	0.419021	Pass	0.334538	Pass
11	Approximate Entropy	0.115387	Pass	0.419021	Pass
12	Random Excursions	0.178278	Pass	0.026648	Pass
13	Random Excursions Variant	0.706149	Pass	0.723129	Pass
14	Serial	0.759756	Pass	0.319084	Pass
15	Linear Complexity	0.994250	Pass	0.202268	Pass

Security Analysis

Resiliency

- The two bipermutive nonlinear rules used in the NL block of CARPenter are 2-resilient [11]. That means, they are both balanced and 2^{nd} order correlation immune.

Security Analysis

Algebraic Attack

- If the number of different input variables available in the output Boolean function is high, then the immunity against the algebraic attack will be high.
- The output function of CARPenter contains 16 and 68 different input variables in first and second iteration respectively and will increase with each iteration.
- After 16 iterations, at the time of keystream generation the output Boolean function will be affected by all the 256 bits of the cipher.
- So output Boolean function of the cipher will have high algebraic degree at the time of key generation and will prevent the algebraic attack on CARPenter.

Security Analysis

Linear attack

- Nonlinearity of output Boolean function in the first iteration is 32256 and will increase with each iteration. At the time of key generation phase, nonlinearity will be much higher.

Security Analysis

Meier-Staffelbach Attack

- Meier and Staffelbach attacked the Rule-30 based stream cipher designed by Wolfram in [9]. The state of the i^{th} cell from time t to $t + n$ (temporal sequence) is known to the attacker.
- This attack tries to guess the right half of initial state and then tries to generate the right adjacent neighbour of temporal sequence.
- Since there is a many-to-one mapping from the right side to the temporal sequence, a guessed right side value may give correct right adjacent sequence.
- Since there is a linear relation between the temporal sequence and the left half, the attack calculates the left half, by moving backward from $t + n$ to t.
- Then the calculated seed is used to generate the temporal sequence. Attack is successful if the generated temporal sequence matches with original temporal sequence.

Security Analysis

Inapplicability of Meier-Staffelbach Attack on CARPenter

- This attack is not applicable to CARPenter.
- In order to compute the right adjacent neighbour of temporal sequence, knowledge of the state of left neighbour is required because of the use of 5-neighbourhood CA.
- Since there is a many-to-one mapping from the right side to the temporal sequence, a guessed right side value may give correct right adjacent sequence.
- Random value cannot be assigned to the left hand side of the temporal sequence because there is no many-to-one mapping from left hand side to the temporal sequence.

Security Analysis

Time/Memory/Data tradeoff attack

- If inner state of a stream cipher consists of n bits, then $O(2^{n/2})$ is the complexity of this attack on stream cipher.
- Inner state of the CARPenter consists of 256 bits which makes it difficult to perform Time/ Memory/Data/ tradeoff attack.

Security Analysis

Fault Attack

- In this attack, a fault can be introduced at any bit position. The attacker has partial control on the timings and the position of the fault and can observe the behaviour of the cipher by resetting the cipher and reintroducing the fault at different positions.
- Because of the use of CA in CARPenter, the fault tracking becomes impossible.
- In NL block, the fault will dissipate nonlinearly and any fault introduced in linear block will reach the nonlinear block in initialization phase itself making it difficult to track the fault.

Summary

- We have proposed a Grain-like, 5-neighbourhood CA based stream cipher called CARPenter.
- The cipher exhibits very good cryptographic properties.
- Initialization phase of CARPenter is faster than Grain and FResCA.
- Generated keystream has good pseudorandomness and is strong against different attacks.

References I

- The estream project. http://www.ecrypt.eu.org/stream/project.html. Accessed: 2018-06-12.
- Sourav Das and Dipanwita Roy Chowdhury. CASTREAM: A new stream cipher suitable for both hardware and software. In Cellular Automata, pages 601-610, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.
- Jimmy Jose and Dipanwita Roy Chowdhury. FResCA: A fault-resistant cellular automata based stream cipher. In Cellular Automata, pages 24-33, Cham, 2016. Springer International Publishing.
- Sandip Karmakar, Debdeep Mukhopadhyay, and Dipanwita Roy Chowdhury. CAvium - strengthening trivium stream cipher using cellular automata.J. Cellular Automata, 7:179-197, 2012

References II


Sourav Das and Dipanwita RoyChowdhury. CAR30: A new scalable stream cipher with rule 30. Cryptography and Communications, 5(2):137–162, Jun 2013.


Swapan Maiti and Dipanwita Roy Chowdhury. Study of five-neighborhood linear hybrid cellular automata and their synthesis. In Mathematics and Computing, pages 68-83, Singapore, 2017. Springer Singapore.


A primitive polynomial search program. notabs.org/primitivepolynomials/primitivepolynomials.htm. Accessed: 2018-06-12.

References III


Jaydeb Bhaumik and Dipanwita Roy Chowdhury. Nmix: An ideal candidate for key mixing. In SECRYPT 2009, Proceedings of the International Conference on Security and Cryptography, Milan, Italy, July 7-10, 2009, SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications, pages 285-288. INSTICC Press, 2009.


Willi Meier and Othmar Staffelbach. Analysis of pseudo random sequences generated by cellular automata. In Advances in Cryptology — EUROCRYPT '91 , pages 186-199, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.


NIST statistical test suite. https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software. Accessed: 2018-06-12.

References IV


Alberto Leporati and Luca Mariot. Cryptographic properties of bipermutive cellular automata rules. J. Cellular Automata, 9:437-475, 2014.

Thank You