On the Period of GSM's A5/1 Stream Cipher and Its Internal State Transition Structure

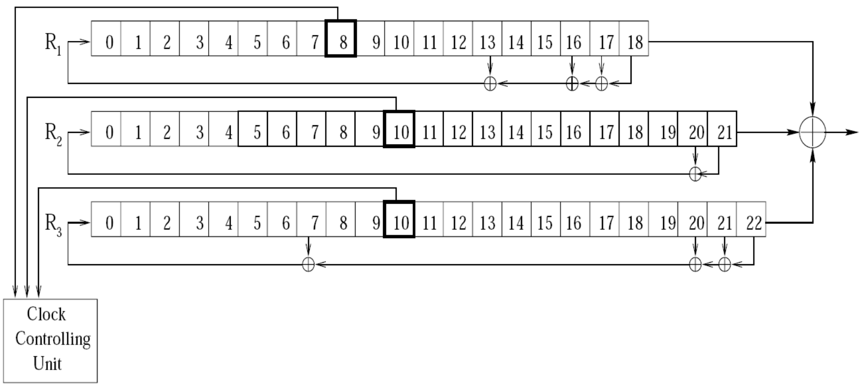
Vahid Amin Ghafari
Information and Communication Technology complex
Malek Ashtar University of Technology
Tehran, Iran
vahidaming@yahoo.com

Ali Vardasbi
Department of Electrical Engineering
Sharif University of Technology
Tehran, Iran
vardasbi@ee.sharif.edu

Outline

- A5/1 Structure
- State Transition In A5/1
- The results of simulations
- Proposition About the Number of Possible Predecessors
- Theoretical View Of The Result
- Conclusion

A5/1 Structure



A5/1 Structure

- Parameters of the A5/1 Registers

Register Number	Length in bits	Primitive Polynomial	Clock-controling bit (LSB is 0)
1	19	$x^{19}+x^5+x^2+x+1$	8
2	22	$x^{22}+x+1$	10
3	23	$x^{23}+x^{15}+x^2+x+1$	10

- Each LFSR is clocked if its clock bit is equal to the majority value.

State Transition In A5/1

- If A5/1's registers were clocked regularly
- Due to the LFSRs' primitive characteristic function and their relatively prime size, the period of the algorithm's generated keystream would be ≈2^64
- The majority function makes it hard to comment about the period of the keystream sequence

State Transition In A5/1

- W. G. Chambers, in Fast Software Encryption 1995 acclaim:
  - the period of an algorithm "like A5/1" was observed to be near 4/3 (2^23-1) .
- This observation was later referenced by Golić in Eurocrypt'97 for A5/1 algorithm.

State Transition In A5/1

- with a high probability, a randomly selected initial state will never be repeated; suggesting the keystream sequence is *ultimately periodic*.
- We tested a set of 10000 randomly selected initial states and in neither of them the first 64 keystream bits were repeated.

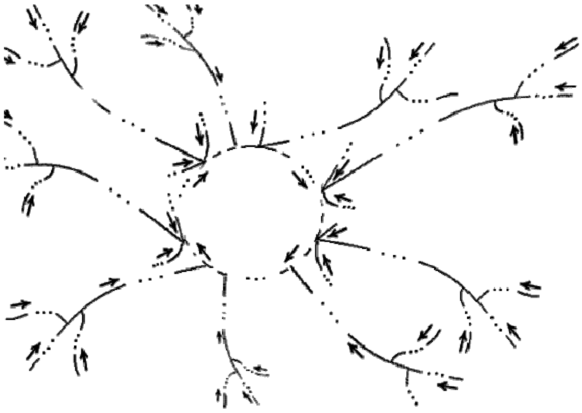
State Transition In A5/1

- The states were observed to enter a loop after an average number of 2^26.17 algorithm clocks.
- Our simulations showed that a big proportion of all the internal states will never be repeated.

٨

State Transition In A5/1

- A scheme of the internal states in a page



The results of simulations

- The space of the algorithm’s internal states could be divided into some independent pages, each page containing one loop, in which there are some branches entering the loop
- Our simulations led us to the conclusion that the average number of each page’s states is approximately 2^51.6 and consequently, there are about 2^12.4 pages.

The results of simulations

- In one of our simulations, 100 initial states were selected randomly and the distance of each state to a loop as well as the period of the loop was measured. The average distance of a randomly selected state to its loop was 2^26.17, while the average period of each loop was 2^25.42.

The results of simulations

- The minimum and maximum of the distance of each state to a loop and the period of the loop

	distance to loop	Loop period
Sample with maximum period of the loop	$2^{26.19}$	$2^{28.41}$
Sample with minimum period of the loop	$2^{27.32}$	$2^{23.41}$
Sample with maximum distance to the loop	$2^{28.08}$	$2^{23.41}$
Sample with minimum distance to the loop	$2^{17.27}$	$2^{24.41}$

The result of simulations

- The ratio of the number of states with one, two, three and four possible predecessors to the total states in a loop
- This ratio remains to be approximately constant for all the loops

One state	Two states	Three states	Four states
0.65	0.125	0.156	0.062

- The theoretical ratio of the number of states with one, two, three and four possible predecessors to the 62.5% states which have at least one possible state.

One state	Two states	Three states	Four states
0.65	0.15	0.15	0.05

Proposition About the Number of Possible Predecessors

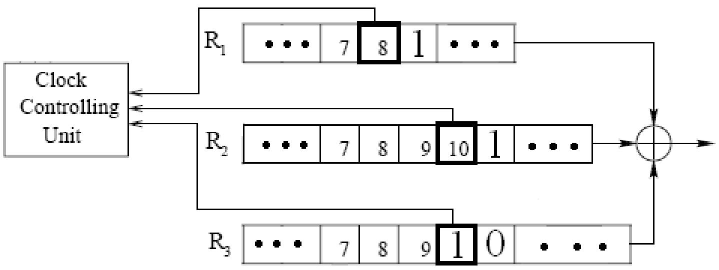
- If an internal state s(t) is randomly chosen according to uniform distribution, then the number of solutions for the predecessor s(t-1) is a nonnegative integer random variable Z with the probability distribution

$$\Pr\{Z=0\}=\frac{3}{8},\ \Pr\{Z=1\}=\frac{13}{32},$$

$$\Pr\{Z=2\}=\Pr\{Z=3\}=\frac{3}{32},\ \Pr=\{Z=4\}=\frac{1}{32}$$

Theoretical View Of The Result

- There are a finite number of internal states
- 37.5% of the states have no possible



Conclusion

- Applications of this discussion
  - time-memory-data tradeoff attacks
  - period of keystream
- with a high probability, a randomly selected state is not periodic
- The average period of states on loop is 2^25.42

Thank you

Any question?