

Clock Control Sequence Reconstruction in the Generalized Shrinking Generator

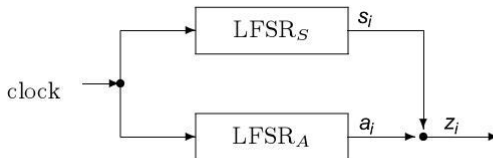
Jan Inge Trontveit

June 7, 2006

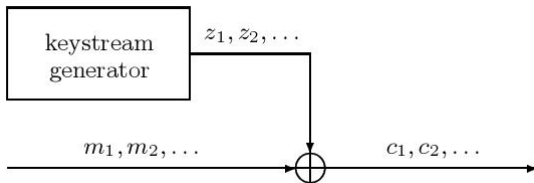
Outline

- 1 Outline
- 2 Introduction
- 3 The attack
- 4 Experiment
- 5 Conclusions
- 6 Future Work

The Shrinking Generator



Applications



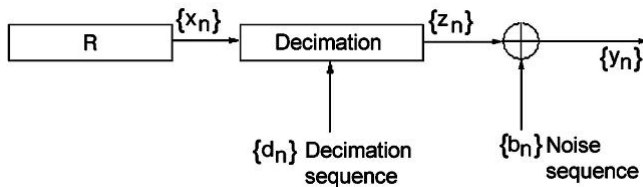
Problem

Reconstruct the generators initial settings.

Methods

- Several approaches
 - A probabilistic coding theory approach (Chambers, Golić)
 - A MAP decoding approach (Johansson)
 - Linear Consistency Test (Molland)
- Known-plaintext

Reduction to step1-stepE



Phase one

- Determine candidate initial states of R
- For every possible initial state of R , the constrained edit distance between its corresponding output sequence of length N and the intercepted sequence of length M is computed. All the initial states that produce the output sequences from R , whose edit distance from the intercepted output sequence is less than a threshold T , are included in the set of candidate initial states.

Phase one

	0	1	2	3	4	5	6	7	8
0	0	0	1	2	2	3	4	5	6
1	X	1	1	1	1	1	2	2	3
2	X	3	3	2	3	2	2	2	3
3	X	3	4	4	4	4	3	3	4
4	X	4	4	5	4	5	4	4	5
5	X	6	5	5	5	6	5	5	5
6	X	7	7	6	6	7	6	7	6
7	X	7	8	7	7	8	8	8	8
8	X	X	9	8	8	8	9	8	8
9	X	X	10	9	10	9	9	10	10
10	X	X	11	11	11	11	11	10	11
11	X	X	11	12	11	11	11	11	12
12	X	X	12	12	13	13	12	12	12
13	X	X	14	14	13	14	13	14	14
14	X	X	14	14	14	15	15	14	14
15	X	X	X	15	15	15	15	16	16
16	X	X	X	16	17	17	17	16	17
17	X	X	X	18	17	17	17	17	17
18	X	X	X	18	19	19	18	19	18
19	X	X	X	20	19	20	20	20	20
20	X	X	X	20	20	20	21	20	20
21	X	X	X	21	22	21	21	22	22
22	X	X	X	X	23	23	23	22	22
23	X	X	X	X	23	23	23	24	24
24	X	X	X	X	25	25	25	24	25
25	X	X	X	X	25	25	25	25	26
26	X	X	X	X	27	27	26	26	27
27	X	X	X	X	27	28	27	27	27
28	X	X	X	X	28	29	28	29	29

Phase two

- Clock control sequence reconstruction
- Search the edit distance matrix for optimal and suboptimal paths
- With zero noise, we only need to reconstruct the optimal paths
- In the presence of noise, we also need to reconstruct suboptimal paths
- The number of paths to be reconstructed is controlled by the value of \mathcal{D}

Phase two

- We increase \mathcal{D} until the correct clock control sequence is found
- Example of a reconstructed clock control sequence:
2,0,3,3,0,1,2,0
- This would correspond to the following binary sequence:
0011000100011010011
- Finally giving us the initial state of the clocking register

Description

- Implementation in C++
- 50 initial states
- Noise level from 0 to 0.45
- 3 different LFSR lengths

Description

- The number of paths to be reconstructed in order to find the true clock control sequence should be as small as possible.
- This number depends on \mathcal{D}
- Given a certain level of noise, the maximum value of \mathcal{D} , denoted by \mathcal{D}_{max} , has been analyzed experimentally.

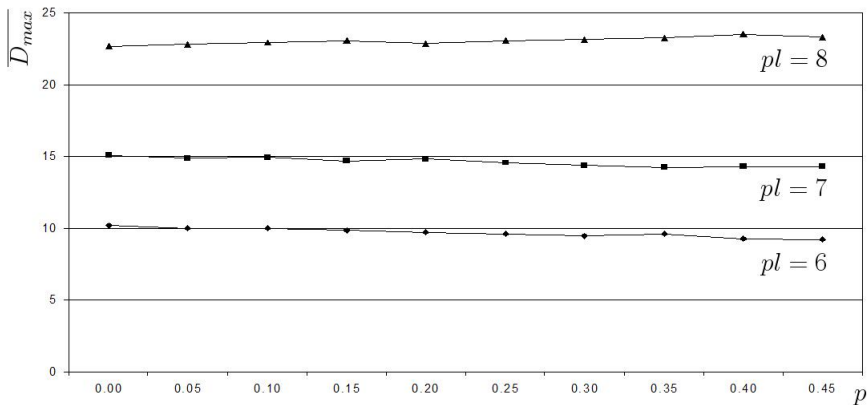
Description

- For a fixed value of \mathcal{D} , the optimal and suboptimal paths are determined.
- We start from $\mathcal{D} = 0$ and we increment \mathcal{D} until the solution is found.
- The value of \mathcal{D}_{max} is stored.

Results

pl	p	diff	n_path	E	largest_step	n_skipped	N
6	0.000000	12	144	5	3	10	21
6	0.000000	12	142	5	2	10	21
6	0.000000	11	423	5	2	11	21
6	0.000000	15	7	5	1	7	21
6	0.000000	12	58	5	1	9	21
6	0.000000	6	1327	5	5	15	21
6	0.000000	16	1	5	0	6	21
6	0.000000	3	1985	5	4	19	21
6	0.000000	10	462	5	2	12	21
6	0.000000	3	3685	5	5	18	21

Results



Conclusions

- The procedure always finds the solution
- Even if the level of noise is relatively high
- $\overline{\mathcal{D}_{max}}$ depends on the length of the necessary clock control sequence
- $\overline{\mathcal{D}_{max}}$ depends on the noise level
- Inexact estimation of N introduces noise

Future Work

- Estimation of N
- Longer LFSRs
- The Alternating Step Generator

Feedback

Opponent and Questions...