

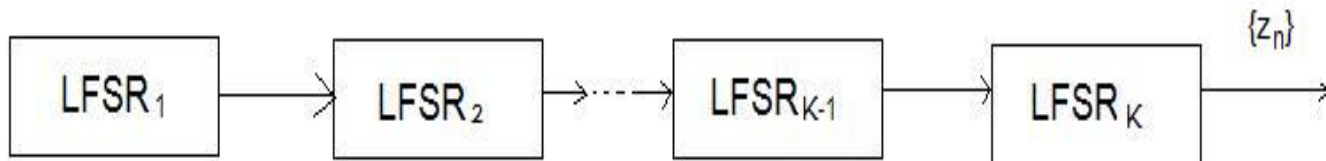
Cryptanalysis of a cascade of non-uniformly clocked linear feedback shift register

Lelai Shi

1. Introduction

- Two most important cryptographic quality criteria for stream ciphers: length of the period of the output sequence and linear complexity of the output sequence.
- To achieve these criteria, non-linear filters, non-linear combiners and irregular clocking are applied.
- Non-linear filters and non-linear combiners were shown to be vulnerable to various kinds of attacks.(e.g. correlation attack by Siegenthaler)

- Besides, with irregular clocking it is possible to achieve longer periods and higher linear complexities than with non-linear filters and combiners .
- Because of that, it is of particular interest to investigate the ciphertext-only cryptanalysis of a cascade of pseudorandom sequence generators employing linear feedback shift registers (LFSRs) with the irregular clocking.

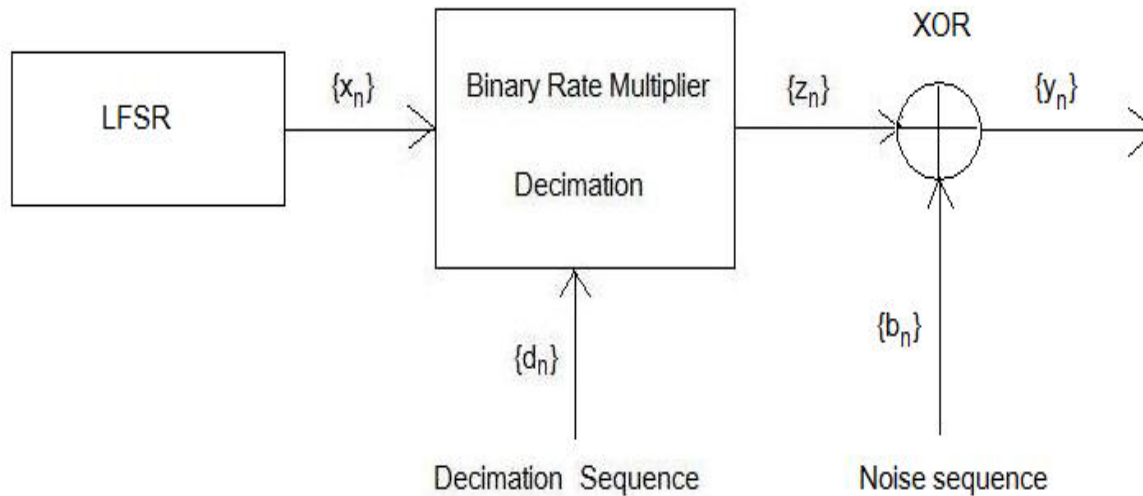


2. Problem description

- Given the prefix of the intercepted output sequence of length M , determine the initial states of all the LFSRs in the cascade.
- Generalize the correlation attack against a scheme with 2 LFSRs, of which one irregularly clocks another, to a cascade of irregularly clocked LFSRs.

3. Statistical model

- This is statistical model of a stage of the cascade.

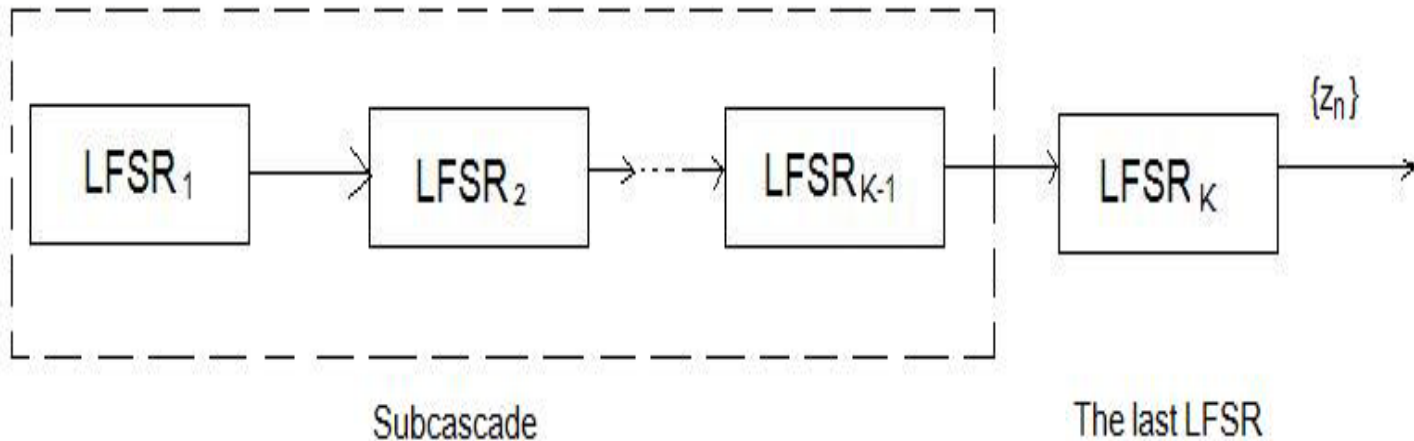


4. Constrained edit distance

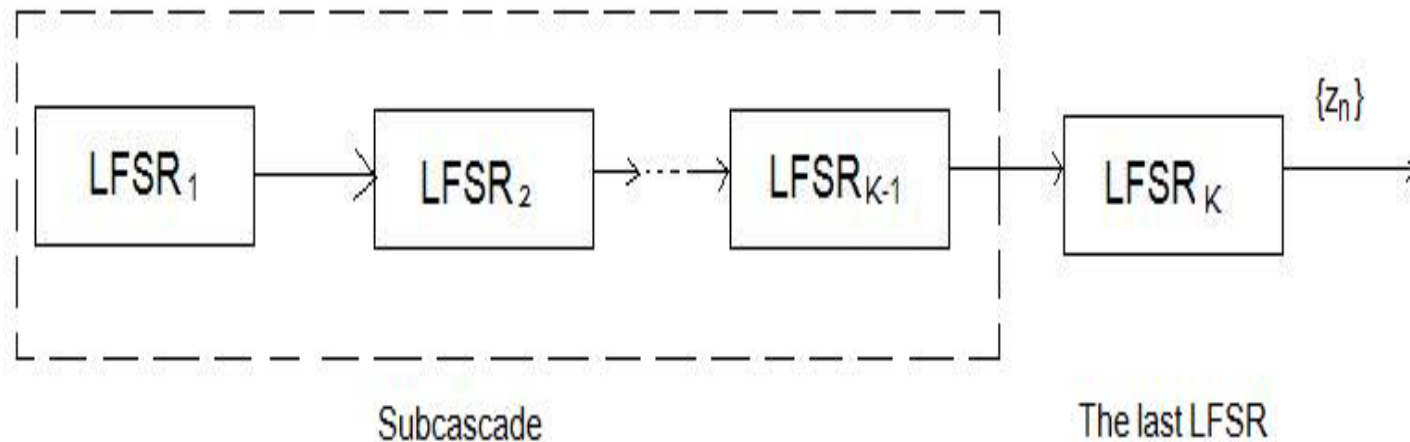
- What is constrained edit distance in general?
- The constrained edit distance used in this thesis:
 1. The maximum length of runs of deletions is E .
 2. The elementary edit operations are ordered in the sense that first the deletions are performed and then the substitutions.

5. Phases of cryptanalysis

- Phase 1: Splitting the Cascade into subcascades.



- Phase 2: Reconstruction of Candidate Initial State
- Phase 3: Clock Control Sequence Reconstruction.



6. Experimental work

- We use three LFSRs with the same feedback polynomials:

$$f(x) = 1 + x^2 + x^7 + x^6 + x^{10}$$



- The result shows that, after searching 7612 paths, the correct clock sequence is found equal to clock 2.
- After searching only 20 paths, the correct clocked sequence was found equal to clock 1.

7. Conclusion

- It is feasible to generalize the correlation attack against a scheme with 2 LFSRs, of which one irregularly clocks another, to a cascade of irregularly clocked LFSRs.