Siegenthaler's correlation attack

1. Background

In 1985, Siegenthaler proposed an attack against a special class of stream ciphers, so-called non-linear combiners. The attack is successful if there is correlation between the output sequence of the generator and the output sequence of some of the Linear Feedback Shift Registers (LFSRs) that generate inputs for the combining non-linear function. In this project, we concentrate on Geffe's non-linear combiner (see the slide 32, Topic 2.2), which, in its original form, was broken by Siegenthaler using this correlation attack.

2. The task for the student

1. Implement the Geffe's generator in your favorite programming language (any language can be used – c/c++, Java, Python, c#, Pascal, Matlab, etc.) Use feedback polynomials of a low degree, between 10 and 20 (both limits included). To generate feedback polynomials, use the software that we demonstrated during the exercises (23_PrimPolGen.zip, available in Blackboard).
2. Write a short (up to 5 A4 pages) report about the Siegenthaler's correlation attack. From this report, it should be clear that you have understood the attack – provide examples, especially related to Geffe's generator cryptanalysis (see Section IV of the original Siegenthaler's paper, available in Blackboard).
3. Implement the Siegenthaler's attack against Geffe's generator with the feedback polynomials used in Task 1. Write a short report (up to 5 A4 pages) about your implementation of the attack and the results obtained – what was the noise level that you used, how many false positives were obtained (i.e. how many elements of the candidate initial state set), what was the probability of false alarm that you set and consequently the length of the intercepted noised output sequence. Vary the noise level and the length of the intercepted noised output sequence and discuss the results.
4. Propose a different Boolean combiner for Geffe's generator that has better correlation properties. Apply the Siegenthaler's attack on your proposed generator. Compare the results obtained with those discussed in Task 3. Write a short report (up to 5 A4 pages) about this. Remarks: Do not use a sum as a combiner, it is a linear combiner! Remember, with 3 variables, we cannot have a balanced Boolean function with no correlation with any input variable. So, try to find a Boolean combiner that is balanced and has relatively small correlation with the input variables. If we drop the balancedness criterion, propose a combiner with no correlation with any input variables. What is the consequence of such a choice for the security of the cipher?

3. Handing in

This is individual work. Put everything you produce in a single ZIP file Siegenthaler.zip. The handing in technology will be Inspera, and the submission will be anonymous. The deadline is June 2nd 2020 at 12.00 Oslo time.

4. References

[1] T. Siegenthaler, Decrypting a class of stream ciphers using ciphertext only, IEEE Transactions on Computers, Vol. c-34, No. 1, January 1985.