Abstract

A fast correlation attack

Andreas Klein

Gent university
Dept. of Pure Mathematics and Computer Algebra
Krijgslaan 281-S22
9000 Ghent, Belgium

Correlation attacks are an important class of attacks against shift register based stream ciphers. Consider for example the following very simple cipher.

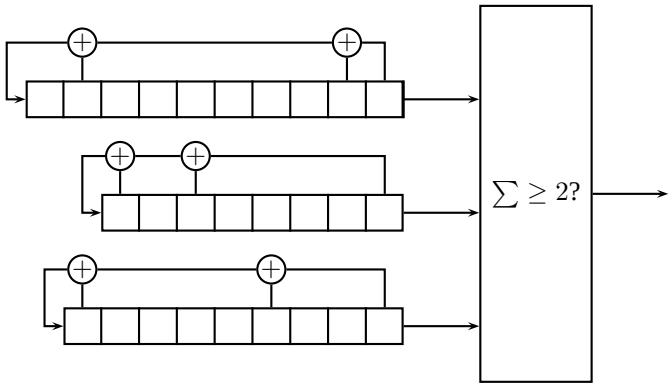

Figure 1: A simple LFSR based cryptosystem.

For each of the three LFSRs we can say that the output of the whole system is equal to the output of the LFSR with probability $\frac{3}{4}$. This is a very strong correlation.

Correlation attacks can be seen as a special decoding problem. The LFSR describe a cyclic code. The remaining part of the stream cipher can be modelled as a Binary Symmetric Channel (BSC), with some error probability $p = \frac{1}{2} - \delta < \frac{1}{2}$. The goal is correct the error (find the seed of the LFSR).

However the problem differs in certain aspects from the problems known from coding theory.

- In contrast to coding theory, the code is not chosen to have a fast decoding algorithm. In fact the designer of the cryptosystem has the opposite goal.
- While in coding theory, we mostly deal with moderate error probabilities, in cryptography we will deal with error probabilities p close to $\frac{1}{2}$.
- In cryptography, the attacker can spend much more computational effort on the decoding algorithm than in coding theory. Everything below 2^{30} operations is very good.

In my talk I will present a new fast correlation attack that extends the attack from Chepyzhov, Johansson and Smeets [1] and Lu and Huang [2].

References

[1] V. Chepyzhov, T. Johansson, and B. Smeets. A simple algorithm for fast correlation attacks on stream ciphers. In *Proceedings of the 7th International Workshop on Fast Software Encryption*, volume 1978 of *LNCS*, pages 181–195, 2001.

[2] P. Lu and L. Huang. A New Correlation Attack of LFSR Sequences. In H. Niederreiter K. Feng and C. Xing, editors, *Coding, Cryptography and Combinatorics*, volume 23 of *Progress in Computer Sience and Applied Logic*, pages 67–84. Birkhäuser, 2004.