Improving greedy nonrandomness detectors for stream ciphers

Linus Karlsson
Lund University

Joint work with:
Paul Stankovski, Martin Hell

May 9, 2016

Distinguishers and nonrandomness detectors look at the output sequence from a cipher. Their goal is to determine if the output sequence is just random data, or the output of some specific cipher. If the cipher has a good design, it should not be possible to design such a detector, since the cipher's output should appear random.

Stream cipher includes a number of "warm-up" rounds, called initialization rounds. This is a number of rounds in which the cipher is running, but without producing output, thus only mixing the internal state. An important consideration is selecting a sufficiently large number of rounds to avoid a biased initial output sequence, while still avoiding too many which would hurt the performance of the cipher.

We consider the construction of distinguishers and nonrandomness detectors using the maximum degree monomial (MDM) test. We present an iterative algorithm which strives to find a good bit set to use in the MDM test. The algorithm is highly flexible, and can be tweaked by choosing different parameters. It can be seen as a generalization of previous greedy algorithms, where the previous greedy behaviour corresponds to some subset of possible parameters in our new generalized algorithm.

We have analyzed and presented how the different parameters affect the result of the algorithm, such that a correct set of parameters can be selected. Compared to previous greedy algorithms, our algorithm avoids local optima, and thus achieves better results. Running our algorithm on the stream cipher Grain-128a, we achieve record-breaking results when showing nonrandomness in 203 out of 256 initialization rounds.