Greedy Distinguishers and Nonrandomness Detectors

Paul Stankovski
Dept. of Electrical and Information Technology, Lund University,
P.O. Box 118, 221 00 Lund, Sweden

Abstract. We present the concept of greedy distinguishers and show how some simple observations and the well known greedy heuristic can be combined into a very powerful strategy (the Greedy Bit Set Algorithm) for efficient and systematic construction of distinguishers and nonrandomness detectors. We show how this strategy can be applied to a large array of stream and block ciphers, and we show that our method outperforms every other method we have seen so far by presenting new and record-breaking results for Trivium, Grain-128 and Grain v1.

We show that the greedy strategy reveals weaknesses in Trivium reduced to 1026 (out of 1152) initialization rounds using $2^{45}$ complexity – a result that significantly improves all previous efforts. This result was further improved using a cluster; 1078 rounds at $2^{54}$ complexity. We also present an 806-round distinguisher for Trivium with $2^{44}$ complexity.

Distinguisher and nonrandomness records are also set for Grain-128. We show nonrandomness for the full Grain-128 with its 256 (out of 256) initialization rounds, and present a 246-round distinguisher with complexity $2^{42}$.

For Grain v1 we show nonrandomness for 96 (out of 256) initialization rounds at the very modest complexity of $2^7$, and a 90-round distinguisher with complexity $2^{39}$.

On the theoretical side we define the Nonrandomness Threshold, which explicitly expresses the nature of the randomness limit that is being explored.

Keywords: algebraic cryptanalysis, distinguisher, nonrandomness detector, maximum degree monomial, Trivium, Grain, Rabbit, Edon80, AES, DES, TEA, XTEA, SEED, PRESENT, SMS4, Camellia, RC5, RC6, HIGHT, CLEFIA, HC, MICKEY, Salsa, Sosemanuk.

1 Introduction

The output of a sensibly designed cipher should appear random to an external observer. Given a random-looking bit sequence, that observer should not be able to tell if the sequence is genuinely produced by the cipher in question or not. This simple idea is the core of cryptographic distinguishers and nonrandomness detectors.
Recently we have seen several attempts at finding distinguishers and nonrandomness detectors and the best ones seem to be built using the maximum degree monomial test (see [27,11]) or some derivative of it. This test is superb for detecting nonrandomness, but it also provides a window into the internals of the cryptographic algorithm we are examining. The maximum degree monomial test can provide statements such as “The IV bits are not mixed properly”, which can be invaluable to the algorithm designer.

The core of this test is a bit set, and the efficiency of the test is largely determined by how this bit set is selected. For this selection process, it seems that guesswork has been the most prominent ingredient. The reason for this may be that systematic methods have seemed too complicated to find or use, or simply that the importance of bit set selection has been underestimated. By far, the best systematic approach we have seen so far was due to Aumasson et al. [2]. They used a genetic algorithm to select a bit set, and this is a very reasonable approach for unknown and complex searchspaces. The complexity of the searchspace depends on the algorithm we are examining, but are they really so complex that we need to resort to such methods? In this paper we present a very simple deterministic and systematic approach that outperforms all other methods we have seen so far. We call it the Greedy Bit Set Algorithm.

Stream ciphers have an initialization phase, during which they “warm up” for a number of rounds before they are deemed operational. Block ciphers are not explicitly initialized in this way, but they do operate in rounds. For our purposes, this can be translated into an initialization phase.

How many rounds are needed to warm up properly? This is a question that every algorithm designer has been faced with, but we have not yet seen any satisfactory answer to this question. We make some observations that lead us to a definition of the Nonrandomness Threshold, which helps us to better understand the nature of the problem. The Greedy Bit Set Algorithm is a tool that can and should be used by designers to determine realistic lower bounds on the initialization period for their algorithm.

We go on to show how the Greedy Bit Set Algorithm performs against a wide variety of new and old stream and block ciphers, and we find new record-breaking results for Trivium, Grain-128 and Grain v1. We reveal weaknesses in Trivium reduced to 1026 out of 1152 initialization rounds in $2^{45}$ complexity, thereby significantly improving all previous efforts. By using a cluster we are able to improve this result even further to 1078 rounds at $2^{54}$ complexity. For Trivium we also present a new 806-round distinguisher of complexity $2^{44}$. Both distinguishing and nonrandomness records are also set for Grain-128. We show nonrandomness in 256 (out of 256) initialization rounds, and present a 246-round distinguisher with complexity $2^{42}$. For Grain v1 we show nonrandomness for 96 (out of 256) initialization rounds for a cost of only $2^7$.

The paper is organized as follows. In Section 2 we give an overview of the black box model attack scenario and explain the maximum degree monomial test. We also briefly describe the software tools developed for this paper. In Section 3 we present our Greedy Bit Set Algorithm, comment on the importance of key