Automated algebraic cryptanalysis

Stankovski, Paul

Published in:
Proceedings of the ECRYPT Workshop on Tools for Cryptanalysis 2010

2010

Automated Algebraic Cryptanalysis

Paul Stankovski

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

Abstract. We describe a simple tool for automatic algebraic cryptanalysis of a large array of stream- and block ciphers. Three tests have been implemented and the best results have led to continued work on a computational cluster. Our best results show nonrandomness in Trivium up to 1070 rounds (out of 1152), and in the full Grain-128 with 256 rounds.

Keywords: algebraic cryptanalysis, maximum degree monomial test, automated testing

The core of this work is the Maximum Degree Monomial (MDM) test [1, 2], which we use for algebraic cryptanalysis of a large array of stream and block ciphers. To facilitate time-efficient and automatic testing, we created a tool for running algebraic cryptanalysis tests. We assembled several specialized implementations that output initialization data, which is necessary for the algebraic tests. A generic interface then provides uniform access to all primitives. Algebraic tests can be implemented generically and run for each of the supported algorithms. This has been done for Trivium, Grain-128, Grain v1, Rabbit, Edon80, AES-128/256, DES, TEA, XTEA, SEED, PRESENT, SMS4, Camellia, RC5, RC6, HIGHT, CLEFIA, HC-128/256, MICKEY v2, Salsa20/12 and Sosemanuk.

We have implemented three particularly interesting tests. A greedy incarnation of the MDM test reveals inadequacies in bit mixing, and does so beautifully. This test can also point out unexpected key weight anomalies. A bit-flip test was devised to catch simple symmetry errors. Also, exhaustive search for small but optimal bit sets for the MDM test was also implemented.

The greedy approach to finding promising bit sets for the MDM test works exceptionally well for Trivium and Grain-128 (compare to [3, 4]). Using a computational cluster, we then pushed our computational limits to show weaknesses in Trivium reduced to 1070 (out of 1152) initialization rounds. The greedy strategy also works well for Grain-128, revealing nonrandomness through all 256 initialization rounds.

Our vision is that every algorithm designer should use our or other similar testing tools during algorithm development to catch algebraic weaknesses earlier than what has been possible before.

References

1. M.-J. O. Saarinen. Chosen-IV statistical attacks on eSTREAM stream ciphers. eSTREAM, ECRYPT Stream Cipher Project, Report 2006/013, 2006. http://www.ecrypt.eu.org/stream.
2. H. Englund, T. Johansson, and M. S. Turan. A framework for chosen IV statistical analysis of stream ciphers. In K. Srinathan, C. Pandu Rangan, and M. Yung, editors, *Progress in Cryptology - INDOCRYPT 2007*, volume 4859/2007 of *Lecture Notes in Computer Science*, pages 268–281. Springer-Verlag, 2007.
3. J.-P. Aumasson, I. Dinur, L. Henzen, W. Meier, and A. Shamir. Efficient FPGA Implementations of High-Dimensional Cube Testers on the Stream Cipher Grain-128. Available at http://eprint.iacr.org/2009/218/, Accessed June 17, 2009, 2009.
4. J.-P. Aumasson, I. Dinur, W. Meier, and A. Shamir. Cube Testers and Key Recovery Attacks on Reduced-Round MD6 and Trivium. In O. Dunkelman, editor, *Fast Software Encryption 2009*, volume 5665 of *Lecture Notes in Computer Science*, pages 1–22. Springer-Verlag, 2009.