Stream Ciphers

[1] M. Afzal and A. Masood, *Algebraic cryptanalysis of a NLFSR based stream cipher*, 3rd International Conference on Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. (2008), 1–6.

[2] Mehreen Afzal and Ashraf Masood, *Resistance of stream ciphers to algebraic recovery of internal secret states*, Third International Conference on Convergence and Hybrid Information Technology, 2008. ICCIT '08 **2** (2008), 625–630.

[3] Mehreen Afzal, Ashraf Masood, and Naveed Shehzad, *Improved results on algebraic cryptanalysis of A5/2*, Communications in Computer and Information Science **12** (2008), no. 4, 182–189.

[4] Sultan Zayid Al-Hinai1, Ed Dawson, Matt Henricksen, and Leonie Simpson, *On the security of the LILI family of stream ciphers against algebraic attacks*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 4586/2007, Springer Berlin / Heidelberg, 2007, pp. 11–28.

[5] Anne Canteaut, *Open problems related to algebraic attacks on stream ciphers*, WCC 2005, Lecture Notes in Comput. Sci., vol. 3969, Springer, Berlin, 2006, pp. 120–134.

[6] Scott Contini and Igor E. Shparlinski, *On Stern's attack against secret truncated linear congruential generators*, Information Security and Privacy, Lecture Notes in Computer Science, vol. 3574, Springer Berlin / Heidelberg, 2005, pp. 52–60.

[7] Tobias Eibach, Enrico Pilz, and Gunnar Völkel, *Attacking Bivium using SAT solvers*, Theory and Applications of Satisfiability Testing, SAT 2008, Lecture Notes in Computer Science, vol. 4996, Springer, Berlin, 2008, pp. 63–76.

[8] Aline Gouget, Hervé Sibert, Come Berbain, Nicolas Courtois, Blandine Debraize, and Chris Mitchell, *Analysis of the bit-search generator and sequence compression techniques*, Fast Software Encryption (Berlin), Lecture Notes in Computer Science, vol. 3557, Springer-Verlag, 2005, pp. 196–214.

[9] Antoine Joux and Frédéric Muller, *A chosen IV attack against Turing*, Selected Areas in Cryptography, Lecture Notes in Comput. Sci., vol. 3006, Springer, Berlin, 2004, pp. 194–207. MR MR2094730 (2005f:94106)

[10] P. Loidreau and V. Shorin, *Application of Gröbner bases techniques for searching new sequences with good periodic correlation properties*, IEEE International Symposium on Information Theory (ISIT), Adelaide, 2005.

[11] Cameron McDonald, Chris Charnes, and Josef Pieprzyk, *An algebraic analysis of Trivium ciphers based on the boolean satisfiability problem*, 2007.

[12] Deike Priemuth-Schmid and Alex Biryukov, *Slid pairs in Salsa*20 *and Trivium.*

[13] Werner Schindler and Le Van Ly, *How to embed short cycles into large nonlinear feedback-shift registers*, Security in Communications Networks: 4th International Conference, SCN 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers, Lecture Notes in Comput. Sci., vol. 3352, Springer, Berlin, 2005, p. 367.

[14] Kenneth Koon-Ho Wong, *Applications of finite field computation to cryptology: Extension field arithmetic in public key systems and algebraic attacks on stream ciphers*, Phd, Queensland University of Technology, 2008.

[15] Haina Zhang and Xiaoyun Wang, *Cryptanalysis of stream cipher grain family*, 2009.