SENS 2008
Fourth Scientific Conference with International Participation
SPACE, ECOLOGY, NANOTECHNOLOGY, SAFETY
4–7 June 2008, Varna, Bulgaria

RECENT ATTACKS AGAINST SUMMATION, SHRINKING AND SELF-SHRINKING STREAM CIPHERS - SHORT SURVEY

Borislav Stoyanov

University of Shoumen
Faculty of Computer Informatics
e-mail: bpstoyanov@yahoo.com

Keywords: *Cryptography, Stream Ciphers, Cryptography Attacks*

Abstract: *This paper discusses recent attacks against summation, shrinking and self-shrinking stream ciphers. Some attacks against shrinking stream cipher are applicable also against self-shrinking stream cipher.*

Introduction

Research of resistance against cryptography attacks is one of the most important requirements to the stream ciphers. The attacks and statistical researches form complete picture of stream ciphers properties.

This paper shortly notates the most recent attacks against summation [27], shrinking [6] and self-shrinking [24] stream ciphers.

Basics of the summation, shrinking and self-shrinking stream ciphers

The summation combiner is a stream cipher in which two maximal periods' binary Linear Feedback Shift Register (LFSR) [25] sequences of periods 2^r and 2^s-1, are combined using addition-with-carry, but the carry is saved and added in at the next stage.

In the shrinking generator, a control LFSR R_0 is used to select a portion of the output sequence of a second LFSR R1. The produced keystream is a shrunken, irregularly decimated subsequence of the output sequence of R_1, as depicted in Fig. 1.

The algorithm of shrinking stream cipher consists of the following steps:

1. Registers R_0 and R_1 are clocked.
2. If the output of R_0 is 1, the output bit of R_1 forms a part of the keystream.
3. If the output of R_0 is 0, the output bit of R_1 is discarded.

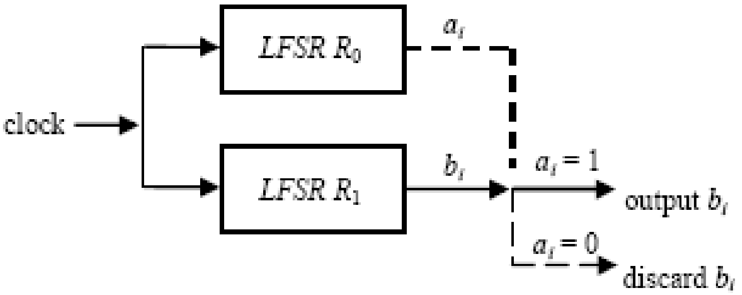

Fig. 1. Shrinking stream cipher

Suppose that the connection polynomials of R_0 and R_1 are chosen uniformly at random from the set of all primitive polynomials of degrees L_0 and L_1 over $\boldsymbol{Z_2}$. Then the distribution of patterns in output sequence is almost uniform.

The self-shrinking generator is based on the shrinking principle. It requires only one maximal length LFSR. The self-shrinking cipher requires a tuple (a_{2i}, a_{2i+1}) as input and outputs a_{2i+1} if and only if a_{2i} = 1.

The 2-adic summation-shrinking bitstream generator is proposed in [29] with the period and linear complexity.

In [30] the N-adic summation-shrinking generator is proposed, Fig.2.

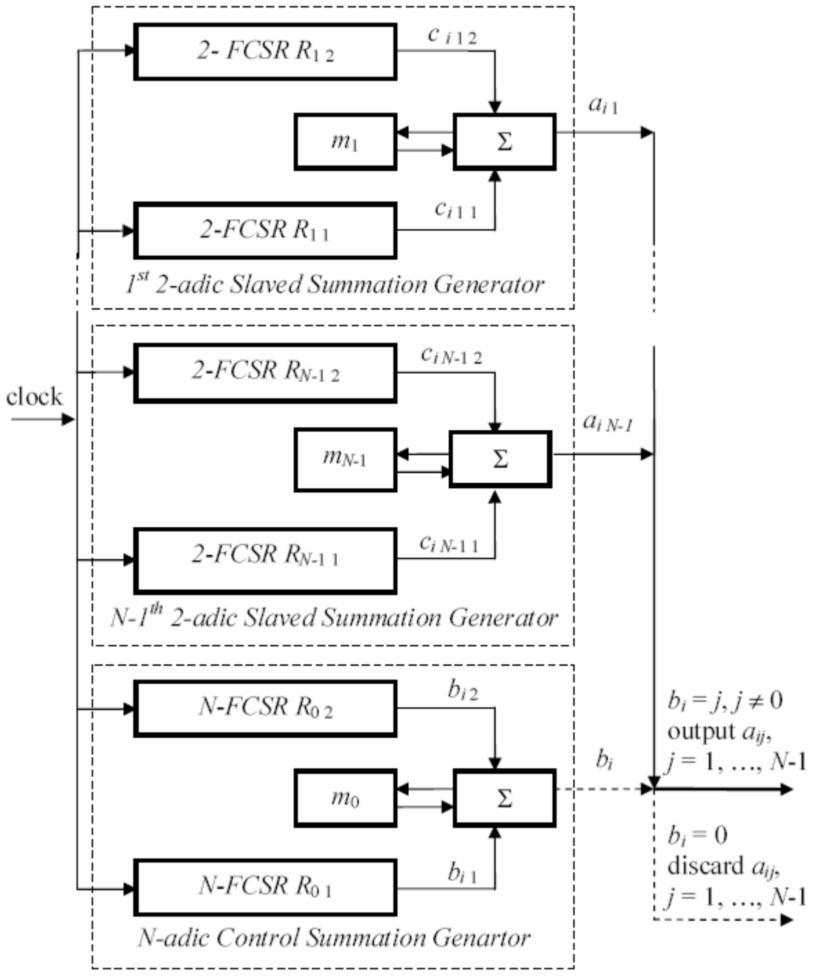

Fig.2 N-adic Summation-Shrinking Generator

The results from statistical analysis show that the sequence generated by the cipher is uniform, scalable, uncompressible, whit large period; consistent and unpredictable.

Recent attacks against summation, shrinking and self-shrinking stream ciphers

Regardless of big period and high linear complexity the summation stream cipher is vulnerable to correlation attacks of Meier [14], Meier and Staffelbach [22], [23], Dawson [9] and to the attacks of 2-adic complexity of Klapper and Goresky [21]. These attacks are feasible if the summation stream cipher is constructed from low degree polynomials LFSRs.

There are few attacks against shrinking stream cipher. The main attack is divide-and-conquer, which performs exhaustive search among all of possible initial states and minimal polynomials of controlling LFSR [6].

Courtois and Meier propose algebraic attack against LFSR-oriented stream ciphers with filter as a nonlinear part [8]. The adapting of this attack to the LFSR-oriented stream ciphers with memory is made from Armknecht и Krause [1].

Gollic and O'Connor propose in [17] correlation attack, which is experimentally analyzed in [28]. Studies [15], [17] and [19] propose correlation attacks with reduced complexity on the base of searching for the specific subsequences in the output keystream of the cipher.

A breakthrough in attacking shrinking stream cipher is achieved by Biryukov and Shamir with the compromised attack "time-memory-data" [2], generalized by Hong and Sarkar in [18]. The parameters to attack are the time T for the real phase, the memory M – hard discs and the enemy owned data size D. Is used the formula $TM^2D^2 = S^2$, where S is the searching space size.

Some modifications of the shrinking stream cipher attacks exist in the studies [3], [4], [5], [7], [10], [11], [12], [13], [16], [20], [87], [31], [33] and [34].

Attacks against shrinking stream cipher are also applicable against self-shrinking stream cipher if it is LFSRs constructed. There are attacks directly oriented against self-shrinking stream cipher [24], [26], [32], [35], but not sufficiently effective.

There are no other published attack methods against 2-adic summation-shrinking and N-adic summation-shrinking stream ciphers.

Conclusion

This is a short survey on recent attack methods against summation, shrinking and self-shrinking stream ciphers. It can be useful as a starting point for further cryptanalytic research.

Acknowledgement

This work is supported by Shumen University, section “Scientific research” under the grant № / 2008.

References:

1. Armknecht F., M. Krause. Algebraic Attacks on Combiners with Memory, CRYPTO 2003, LNCS Vol. 2729, pp. 162-175.
2. Biryukov A., A. Shamir. Cryptanalytic Time/Memory/Data Tradeoffs for Stream Ciphers, ASIACRYPT 2000, LNCS Vol. 1976, Springer-Verlag, 2000, pp.1-13.
3. de Canniere C., J. Lano, B. Preneel. Comments on the Rediscovery of Time Memory Data Tradeoffs, p. 5, http://ecrypt.eu.org/stream/papers/040.pdf.
4. Canteaut A., M. Trabbia. Improved Fast Correlation Attacks Using Parity-Check Equations of Weight 4 and 5, Advances in Cryptology, EUROCRYPT 2000, LNCS Vol. 1807, Sringer-Verlag, 2000, pp. 573-588.
5. Chambers W., D. Gollmann. Lock-in Effect in Cascades of Clock-controlled Shift-registers, Advances in Cryptology, EUROCRYPT ’88, LNCS Vol. 330, 1988, pp. 331-343.
6. Coppersmith D., H. Krawczyk, Y. Mansour. The Shrinking Generator, Proceedings of Crypto ‘93, Springer-Verlag, 1994, pp. 22-39.
7. Courtois N. Fast Algebraic Attacks on Stream Ciphers with Linear Feedback, CRYPTO 2003, LNCS Vol. 2729, pp. 176-194.
8. Courtois N., W. Meier. Algebraic Attacks on Stream Ciphers with Linear Feedback, EUROCRYPT 2003, LNCS Vol. 2656, pp. 345-359.
9. Dawson E. Cryptanalysis of Summation Generator, Advances in Cryptology, AUSCRYPT ’92, LNCS Vol. 718, 1993, pp. 209-215.
10. Ekdahl P., W. Meier, T. Johansson. Predicting the Shrinking Generator with Fixed Connections, EUROCRYPT 2003, LNCS Vol. 2656, pp. 330-344.
11. Golic J. Computation of Low-Weight Parity-Check Polynomials, Electronic Letters, Vol. 32, No. 21, October 1996.
12. Golic J. Correlation Analysis of the Shrinking Generator, CRYPTO 2001, LNCS Vol. 2139, pp. 440-457.
13. Golic J. Cryptanalysis of Alleged A5 Stream Cipher, In W. Fumy, editor, Advances in Cryptology, EUROCRYPT ’97, LNCS Vol. 1233, Springer-Verlag, Berlin, 1997, pp. 239-255.
14. Golic J. Edit distances and probabilities for correlation attacks on clock-controlled combiner with memory, IEEE Transactions on Information Theory, Vol.47, No. 3, 2001, pp. 1032 – 1041.
15. Golic J. Linear Models for Keystream Generators, IEEE Transactions on Computers, Vol. 45, No. 1, January 1996, pp. 41-49.
16. Golic J. Towards Fast Correlation Attacks on Irregularly Clocked Shift Registers, Advances in Cryptology, EUROCRYPT ’95, LNCS Vol. 921, Springer-Verlag, 1995, pp. 248-262.
17. Golic J., L. O’ Connor. Embedding and Probabilistic Correlation Attacks on Clock-Controlled Shift Registers, Advances in Cryptology, EUROCRYPT ’94, LNCS Vol. 950, Springer-Verlag, 1995, pp. 230-243.
18. Hong J., P. Sarkar. Rediscovery of Time Memory Tradeoffs, Cryptology ePrint Archive, Report 2005/090, 2005, p. 25, http://eprint.iacr.org/2005/090.
19. Johansson T. Reduced Complexity Correlation Attacks on Two Clock-Controlled Generators, Advances in Cryptology, ASIACRYPT ’98, LNCS Vol. 1541, Springer-Verlag, 1998, pp. 342-357.
20. Johansson T., F. Jonsson. Fast Correlation Attacks Through Reconstruction of Linear Polynomials, Advances in Cryptology, CRYPTO 2000, LNCS Vol. 1880, Springer-Verlag, pp. 300-315.
21. Klapper A., M. Goresky. Cryptanalysis Based on 2-adic Rational Approximation, Advances in Cryptology, CRYPTO ’95, LNCS Vol. 963, Springer-Verlag, N. Y., 1995, pp. 262-273.
22. Meier W., O. Staffelbach. Correlation Properties of Combiners with Memory in Stream Ciphers, Advances in Cryptology, EUROCRYPT ’90, LNCS Vol. 473, 1991, pp. 204-213.
23. Meier W., O. Staffelbach. Correlation Properties of Combiners with Memory in Stream Ciphers, Journal of Cryptology, Vol. 5, 1992, pp. 67-86.
24. Meier W., O. Staffelbach. The Self-Shrinking Generator, Advances in Cryptology, EUROCRYPT ’94, LNCS Vol. 950, 1995, pp. 205-214.
25. Menezes A., P. van Oorshot, S. Vanstone. Handbook of Applied Cryptography, CRC Press, 1997, p. 780, http://www.cacr.math.uwaterloo.ca/hac.

26. Mihaljevic M. A Faster Cryptanalysis of the Self-Shrinking Generator, In J. Pieprzyk and J. Seberry, editors, Advances in Cryptology, ACISP ’96, LNCS Vol. 1172, Sringer-Verlag, Berlin, 1996, pp. 182-189.
27. Rueppel R. Correlation Immunity and the Summation Generator, Advances in Cryptology, CRYPTO ’85, LNCS Vol. 218, 1986, pp. 260-272.
28. Simpson L., J. Golic, E. Dawson. A Probabilistic Correlation Attack on the Shrinking Generator, Information Security and Privacy ’98, Brisbane, LNCS Vol. 1438, Springer-Verlag, 1998, pp. 147-158.
29. Stoyanov B. 2-adic Summation-Shrinking Generator, Western European Workshop on Research in Cryptology, WEWORC 2005, Leuven, Belgium, 5-7 July, 2005, pp. 103-104.
30. Tasheva Zh., B. Bedzhev, B. Stoyanov. N-adic Summation-Shrinking Generator. Basic properties and empirical evidence, http://eprint.iacr.org/2005/06.
31. Wagner D. A Generalized Birthday Problem, Advances in Cryptology, CRYPTO 2002, LNCS Vol. 2442, Springer-Verlag, 2002, pp. 288-303.
32. Yang L., K. Chen, X. Wang. Cryptanalysis of Self-Shrinking Generator, Electronics Letters, Vol. 39, Issue 22, 30 October, 2003, pp. 1586-1590.
33. Zeng K., C. Yang, T. Rao. On the Linear Consistency Test (LCT) in Cryptanalysis with Applications, Advances in Cryptology, CRYPTO ’89, LNCS Vol. 435, Springer Verlag, 1990, pp. 164-174.
34. Zenner E. On Cryptographic Properties of LFSR-based Pseudorandom Generators, PhD Thesis, University of Mannheim, Germany, 2004, p. 114.
35. Zenner E., M. Krause, S. Lucks. Improved Cryptanalysis of the Self-Shrinking Generator, Advances in Cryptology, ACIPS 2001, LNCS Vol. 2119, 2001, pp. 21-35.