IMPROVED CRYPTOANALYSIS OF THE SELF-SHRINKING P-ADIC CRYPTOGRAPHIC GENERATOR

Borislav Stoyanov

Abstract: The Self-shrinking p-adic cryptographic generator (SSPCG) is a fast software stream cipher. Improved cryptoanalysis of the SSPCG is introduced. This cryptoanalysis makes more precise the length of the period of the generator. The linear complexity and the cryptography resistance against most recently used attacks are invesigated. Then we discuss how such attacks can be avoided. The results show that the sequence generated by a SSPCG has a large period, large linear complexity and is stable against the cryptographic attacks. This gives the reason to consider the SSPSG as suitable for critical cryptographic applications in stream cipher encryption algorithms.

Keywords: Cryptoanalys, FCSRs, Encryption Algorithm, Stream Cipher, Self-Shrinking p-adic Cryptographic Generator.

ACM Classification Keywords: G.3 [Probability and Statistics]: Random Number Generation; E.3 [Data Encryption]; F.2.2 [Nonnumerical Algorithms and Problems]: Computations on discrete structures

Conference: The paper is selected from Sixth International Conference on Information Research and Applications – i.Tech 2008, Varna, Bulgaria, June-July 2008

Introduction

Stream ciphers have several properties that make them suitable for use in telecommunication applications. But apart from the security tried to obtain, the main property that makes stream ciphers distinguishable from block ciphers is that they are in general fast and have low hardware complexity. Stream ciphers process the plaintext character by character, so no buffering is required to accumulate a full plaintext block.

Most stream ciphers are based on simple devices that are easy to implement and run efficiently. A common example of such a device is the linear feedback shift register (LFSR). Such simple devices produce predictable output given some previous output. This is due to the linear property of the device. Therefore, in order to use LFSRs in cryptographical primitive, and particularly in a stream cipher, the linearity must be destroyed [Yilmaz, 2004]. Unfortunately, the classical fast and cheap LFSRs are vulnerable to the so-named "Berlekamp-Massey crypto attack" [Lidl, Niederreiter, 1983], [Oorshot, Menezes, Vanstone, 1997], [Schneier, 1996].

Having in mind the advantages of the stream ciphers with simple structure, recently some theorists have used new approach of stream cipher design and have proposed a few new architectures named Shrinking generator [Coppersmith, Krawczyk, Mansour, 1994] and Self-Shrinking generator [Meier, Staffelbach, 1998]. With regard to positive features of the two generators and Feedback with Carry Shift Registers (FCSRs) [Klapper, Goresky, 1994], [Xu, 2000] the SSPCG [Tasheva, 2005], [Tasheva, Bedzhev, 2005], [Tasheva, Bedzhev, Stoyanov, 2005] have created. The results show that the SSPCG is a promising candidate for high-speed encryption applications due to its simplicity and provable properties.

In this paper, the SSPCG is further investigated with main focus on the period, linear complexity and resistance against the recently used cryptographic attacks. The improved cryptoanalysis shows SSPCG suitable for critical cryptographic applications.

Description of the Self-shrinking p-adic cryptographic generator

In contrast with the classic Self-Shrinking generator the SSPCG architecture (Fig. 1) uses a p-adic FCSR instead of LFSR. This allows the generator to produce a number in the range 0 to p−1 (p-its) in one step (a_i = [0, 1, …,

p−1]). TheSSPCG selects a portion of the output p-adic FCSR sequence by controlling of the p-adic FCSR itself using the following algorithm:

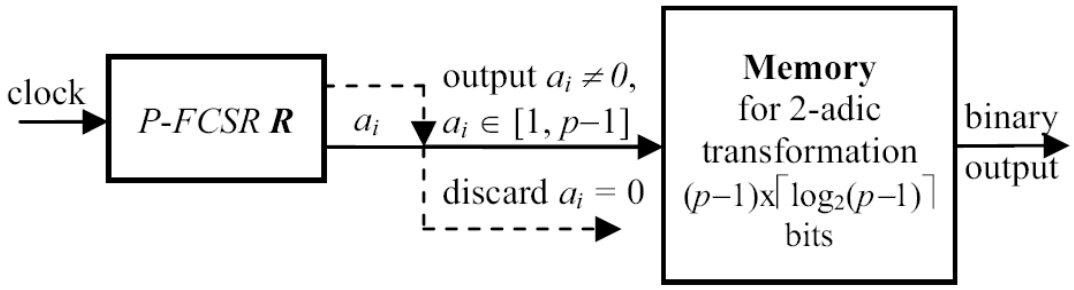

Fig. 1 Self-shrinking p-adic cryptographic generator

Definition 1: The algorithm of the Self-Shrinking p-adic Generator (Fig. 1) consists of the following steps:

1. The p-adic FCSR R is clocked with clock sequence with period τ_0.

2. If the p-adic FCSR output number is not equal to 0 ($a_i \neq 0$), the output bit forms a part of the p-adic SSPCG sequence. Otherwise, if the output number of the p-adic FCSR is equal to 0 (ai = 0), the p-adic output number of SSPG is discarded.

3. The shrunken p-adic SSPG output sequence is transformed in 2-adic sequence in which every p-adic number is presented with $\lceil \log_2(p-1) \rceil$ binary digits, where $\lceil x \rceil$ is the smallest integer which is greater or equal to x. Every output number i from 1 to p−1 of p-adic SSPCG sequence is depicted with p−adic expansion of the number:

$$i-1+\frac{2^{\lceil \log_2(p-1) \rceil}-(p-1)}{2} \qquad (1)$$

The SSPCG uses the generalization of 2-adic FCSRs with stage contents and feedback coefficients in Z/(p) where p is a prime number, not necessarily 2.

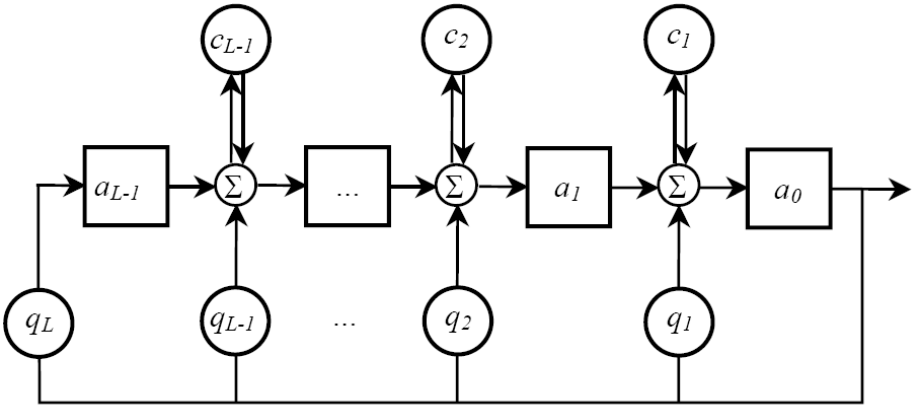

Fig. 2 Galois FCSR

Definition 2: A p-adic feedback with carry shift register with Galois architecture of length L (Fig. 2) consists of L stages (or delay elements) numbered 0, 1, …, L-1, each capable to store one p-adic (0, 1, …, p-1) number and having one input and one output; and a clock which controls the movement of data. During each clock cycle the following operations are performed:

1. The content of stage 0 is output and forms part of the output sequence;

2. The sum modulo p after stage i is passed to stage i - 1 for each i, $1 \le i \le L-1$;

3. The output of the last stage 0 is introduced into each of the tapped cells simultaneously, where it is fully added (with carry) to the contents of the preceding stages.

The $q_1, q_2, \ldots, q_L$ are the feedback multipliers and the cells denoted with $c_1, c_2, \ldots, c_{L-1}$ are the memory (or carry) bits. If $q = -1+q_1p + q_2p^2 +\ldots+ q_Lp^L$ is the base p expansion of a positive integer $q \equiv -1 \pmod p$, then q is a connection integer for a FCSR with feedback coefficients $q_1, q_2, \ldots, q_L$ in Z/(p).

With each clock cycle, the integer sums $\sigma_j = a_j + a_0 q_j + c_j$ is accumulated. At the next clock cycle this sum modulo p $a'_{j-1} = \sigma_n (\mathrm{mod}\, p)$ is passed on the next stage in the register, and the new memory values are $c'_{j-1} = \sigma_n (div\ p)$.

The nonlinearity of the proposed SSPG follows from the fact that it is unknown at which positions the FCSR sequence is shrunken. As a result the linear algebraic structure of the original FCSR sequence is destroyed. The software SSPG implementation is very fast because the pseudorandom generator produces $\lceil \log_2(p-1) \rceil$ binary digits in every step.

It is proved that the period of the SSPCG realized by maximum length p-adic FCSR of length L and connection integer q is $S_0 = T_0^* \lceil \log_2(p-1) \rceil$, where T_0^* is the number of output p-adic FCSR numbers different from 0.

The self-shrunken output SSPCG sequence generated by maximum length p-adic FCSR of length L and connection integer q is a balanced sequence.

The results from statistical analysis show that the sequence generated by SSPG is uniform, scalable, uncompressible and unpredictable.

Improved cryptoanalysis of the Self-shrinking p-adic cryptographic generator

In this section novel results concerning period, linear complexity, and cryptoresistance of SSPCG sequences are presented.

First, we will remind that the period of p-adic FCSR is $T_0 = 2d$, where the connection integer $q = 2d + 1$ [Goresky, Klapper, 2002], and p_0 and q are strong p-prime numbers [Xu, 2000]. Since the output sequence of the SSPCG is balanced each different from p-its will have

$$T_0^p \approx \left\lceil \frac{T_0}{p} \right\rceil \tag{2}$$

number of appearances in a period T_0. Due to of the fact that there is an exit only in different from 0 p-its, then T_0^* acquires the following appearance:

$$T_0^* \approx (p-1)\left\lceil \frac{T_0}{p} \right\rceil \tag{3}$$

Then the period of the SSPCG S_0 could be found with the help of the following expression:

$$S_0 \approx (p-1)\left\lceil \frac{T_0}{p} \right\rceil \lceil \log_2(p-1) \rceil = (p-1)\left\lceil \frac{2d}{p} \right\rceil \lceil \log_2(p-1) \rceil \tag{4}$$

From (4) follows that linear complexity has the following value:

$$\lambda(Z) \ge \log_2\left((p-1)\left\lceil \frac{2d}{p} \right\rceil \lceil \log_2(p-1) \rceil \right) \tag{5}$$

Both the Shrinking Generator and Self-Shrinking Generator use the LFSRs and have a simple structure. Despite of this fact no successful cryptanalytic attack for both generators has been published so far.

Due to the nonuniform exit from the SSPCG it is impossible to apply the p-adic Rational Approximation attack [Xu, 2000].

All attacks acting against the Self-Shrinking pseudorandom generator [Zenner, Krause, Lucks, 2001] are unapplicable, due to the fact that they act against the generator constructed by LFSRs.

With a respect of [Zenner, Krause, Lucks, 2001] we recommend the design of the including FCSR to be upper than 256 memory cells in order to hinder the cryptographic attacks time-memory-data and Backtracking Algorithm.

Conclusion

The calculation of the period and the linear complexity of the SSPCG gives an opportunity of more successful software realization of this generator due to the greater security, due to using easily generated p-prime numbers. The impossibility for attacking the SSPCG with the familiar cryptographic attacks increases the reliability in the properties of the generator.

The SSPCG is one example of a nonlinear combining function. The results presented in previous section mostly have a straightforward extension to general nonlinear combining functions in algebraic normal form.

On the basis of the simplified design the SSPCG shows properties of a successful candiate as a main or slave pseudorandom generator in stream cipher encryption.

Bibliography

[Coppersmith, Krawczyk, Mansour, 1994] D. Coppersmith, H. Krawczyk, Y. Mansour. The Shrinking Generator. Proceedings of Crypto 93, Springer-Verlag, pp. 22-39, 1994.

[Goresky, Klapper, 2002] M. Goresky, A. Klapper. Fibonacci and Galois Representations of Feedback-With-Carry Shift Registers. IEEE Trans. Inform. Theory, vol. 48, 2002, pp. 2826−2836.

[Klapper, Goresky, 1994] A. Klapper, M. Goresky. 2-adic Shift Register. Fast Software Encryption, Second International Workshop. Lecture Notes in Computer Science, vol. 950, Springer Verlag, N. Y., 1994, pp.174-178

[Lidl, Niederreiter, 1983] R. Lidl, H. Niederreiter. Finite Fields. Addison-Weslley Publishing Company, London, England, 1983.

[Meier, Staffelbach, 1998] W. Meier, O. Staffelbach. The Self-Shrinking Generator. Proceedings of Advances in Cryptology, EuroCrypt '94, Springer-Verlag, pp. 205-214, 1998.

[Oorshot, Menezes, Vanstone, 1997] P. van Oorshot, A. Menezes, S. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[Schneier, 1996] B. Schneier. Applied Cryptography. John Wiley & Sons, New York, 1996

[Tasheva, 2005] Zh. Tasheva. An Algorithm for Fast Software Encryption. International Conference on Computer Systems and Technologies - CompSysTech 2005, Technical University, Varna, Bulgaria, 16-17 June 2005, pp.II.18-1-II.18-6.

[Tasheva, Bedzhev, 2005] Zh. Tasheva, B. Bedzhev. Software Implementation of p-adic Self-shrinking Generator for Aerospace Cryptographic Systems. Scientific Conference "SPACE, ECOLOGY, SAFETY" with International Participation, 10–13 June 2005, Varna, Bulgaria, pp. 439-444.

[Tasheva, Bedzhev, Stoyanov, 2005] Zh. Tasheva , B. Bedzhev, B. Stoyanov. Self-Shrinking p-adic Cryptographic Generator. XL International Scientific Conference on Information, Communication and Energy Systems and Technologies, ICEST 2005, Nic, Serbia and Montenegro, June 29-July 1, 2005, pp.7-10.

[Xu, 2000] J. Xu. Stream Cipher Analysis Based on FCSRs, PhD Dissertation, University of Kentucky, 2000, http://www.cs.engr.uky.edu/etd/theses/uky-cocs-2000-d-002/.

[Yilmaz, 2004], E. Yilmaz. Two Versions of the Stream Cipher Snow. Master Thesis, The Graduate school of natural and applied sciences of Middle east technical university, 2004, p. 60.

[Zenner, Krause, Lucks, 2001] E. Zenner, M. Krause, S. Lucks. Improved Cryptanalysis of the Self-Shrinking Generator. LNCS, Vol. 2119, 2001, pp. 21-35.

Authors' Information

Borislav Stoyanov – Assistant Prof., PhD in the Faculty of Computer Informatics, Shumen University; http://crypt.co.nr, e-mail: bpstoyanov@yahoo.com