Research on the Self-shrinking 2-adic Cryptographic Generator

B. Stoyanov, Al. Milev

Abstract — **The Self-shrinking 2-adic cryptographic generator (SS2CG) is investigated in this paper. The period and the linear complexity of the generated sequenced has been presented. The SS2CG generator is developed by suitable software and the speed of generated pseudorandom sequence is tested through a fast software stream cipher. The cryptography resistance of the output generated pseudorandom sequence is analyzed and statistic researches are evaluated by NIST test suite. The generated sequence has a large period, large linear complexity and is stable against the cryptographic attacks. The SS2CG is suitable for critical cryptographic applications in stream cipher encryption algorithms for increasing security in wireless networks and communication system.**

Keywords — **Cryptanalysis, Encryption Algorithm, FCSRs, Stream Cipher, Self-Shrinking 2-adic Cryptographic Generator, wireless network security.**

I. INTRODUCTION

THE stream ciphers are an important tool which can be used to provide security services in the communication information systems and different kind of networks. The performance quality of the hardware and software stream cipher applications depends on their crypto resistance, speed and effectiveness. Mostly the crypto resistance of a stream cipher is connected with it ability to generate nonlinear Pseudo Random Sequence (PRS) with enormous period, uniform distribution of *p*-tuples for a large range of *p* and with good (usually lattice-like) structure in high dimensions.

In order to achieve high performance velocity and cost-effective implementation, on the one hand the Pseudo Random Number Generator (PRNG) architecture must be simple and on the other it must combine fast and cheap elements like Linear Feedback Shift Registers (LFSRs) [1], [2] and [3] and Feedback with Carry Shift Registers (FCSRs) [3]-[6] with some nonlinear functions. Recently, some authors [7], [8] and [9] have used this new approach of stream cipher design and have proposed some new architectures like Shrinking Generator [7] and [8] and Self Shrinking Generator (SSG) [9] and [10]. The architectures appeared to be the promising candidates for high-speed encryption applications due to their simplicity and provable properties.

The research made in [11] point that it is possible to construct self shrinking 2-adic pseudorandom generator with good properties. The generalized p-adic pseudorandom SSG is investigated in [12] and properties of 5-adic SSG generator are given. Additional researches are done in [13] and an improved crypto analysis of the p-adic SSG is shown in [14].

The paper is organized as follows. First, the basics of the pseudorandom FCSR and shrinking and self-shrinking generators are recalled. After that, a FCSR self-shrinking 2-adic generator is suggested. Finally, the properties of the 2-adic FCSR SSG are analyzed and possible application areas are discussed.

II. BASICS OF FCSR AND SELF-SHRINKING GENERATORS

The analysis of FCSR sequences involves a completely different mathematical toolkit and instead of arithmetic in finite fields, we use arithmetic in the 2-adic numbers.

An FCSR is a feedback shift register together with a small amount of auxiliary memory. In its simplest form, the cells in the register consist of bits (0 or 1), while the memory contains a 2 nonnegative integer

Definition [2], [3]. A 2-adic feedback with carry shift register with Galois architecture of length L (Fig. 1) consists of L stages (or delay elements) numbered $0,1,2,....L-1$, each capable to store one 2-adic (0, 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 a part of the output sequence;

2. The sum modulo 2 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.

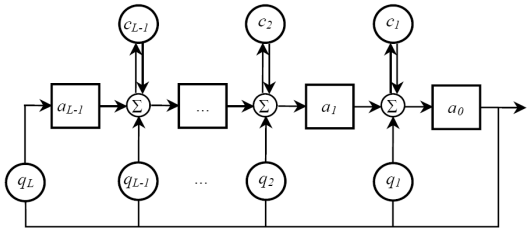

Fig. 1 Galois FCSR

This work is supported by University of Shumen, section "Scientific research" under the grant number № RD-05-290/ 11.03.2009

B. Stoyanov (PhD) is with the Faculty of Computer Informatics, University of Shumen "Bishop Konstantin Preslavsky", Shumen, Bulgaria, (phone: 359-54-830495; e-mail: bpstoyanov@yahoo.com).

Al. Milev (PhD) is with the Faculty of Computer System and Technology, University of Shumen "Bishop Konstantin Preslavsky", Shumen, Bulgaria, (phone: 359-54-872457, e-mail: alex_milev@yahoo.com).

The $q_1, q_2, ..., q_L$ are the feedback multipliers and the cells denoted with $c_1, c_2, ..., c_{L-1}$ are the memory (or carry) bits. If $q = -1 + q_1.2 + q_2 2^2 + q_3.2^3 + ... + q_L.2^L$ is the base 2 expansion of a positive integer $d_0 \equiv -1 (\mathrm{mod}\, 2)$, then d_0 is a connection strong 2-prime integer [10] for a FCSR with feedback coefficients $q_1, q_2, ..., q_L$ in $Z/(2)$.

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 2 $a'_{j-1} = \sigma_n (\mathrm{mod}\, 2)$ is passed on the next stage in the register, and the new memory values are $c'_{j-1} = \sigma_n (div\ 2)$.

The constructed pseudorandom sequences with this generator have good properties but they are susceptible to many of existed crypto attacks [2],[3] and [6]. In order to increase crypto resistance of attacks, shrinking and self-shrinking generators have been developed [7]-[10].

The shrinking generator [7],[8] consists of two linear feedback shift registers (LFSR) A and B generating the m-sequences $(a_i)_{i\geq 0}$ (denoted as A sequence) and $(b_i)_{i\geq 0}$ (denoted as B sequence), respectively. The keystream sequence $(z_j)_{j\geq 0}$ is constructed from these two sequences according to the following selection rule: For every clock *i*, consider the selection bit b_i. If $b_i = 1$, the output is a_i. Otherwise, discard both b_i and a_i. This way, a nonlinear keystream is generated. Even a cryptanalyst who knows part of the keystream sequence can not tell easily which $(z_j)_{j\geq 0}$ corresponds to which a_i, since the length of the gaps (i.e. the number of a_i that have been discarded) is unknown. It is proved that the shrinking generator has good algebraic and statistical properties.

The self-shrinking generator [9]-[10] is a modified version of the shrinking one. It could be constructed by using LFSR and FCSR as well. The close relationship between shrinking and self-shrinking generator is shown in figure 2.

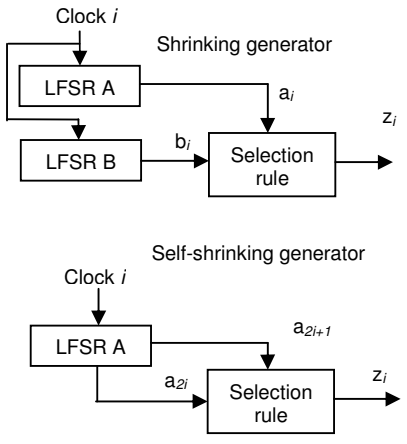

Fig.2 Shrinking and self-shrinking generator

The self-shrinking generator in fig.2 requires only one LFSR (FCSR) A, whose length will be denoted by L. The LFSR generates a sequence $(a_i)_{i\geq 0}$ in the usual way. The selection rule is the same as for shrinking generator, using the even bits $a_0, a_2, a_4, ...$ as B-bits and the odd bits $a_1, a_3, a_5, ...$ as A-bits in the above sense. Thus, the self-shrinking rule requires a couple (a_{2i}, a_{2i+1}) as input and outputs a_{2i+1} if $a_{2i} = 1$.

Notwithstanding this similarity, the self-shrinking generator has shown even more resistance to cryptanalysis than the shrinking generator [6],[14].

III. 2-ADIC FCSR SELF-SHRINKING GENERATORS

In this section 2-adic FCSR self shrinking generator is suggested.

Definition: 2-adic self shrinking pseudorandom generator consists of 2-FCSR R_0, which generates non-uniformly keystream *K* as shown in fig.3.

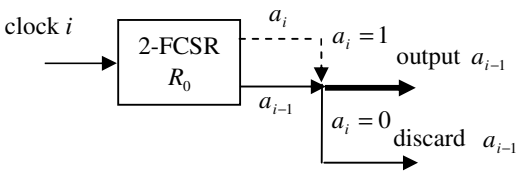

Fig.3. 2-adic 2-FCSR SSG

The work of SSG begins with the choice of strong 2-prime connection number d_0 which defines feedbacks of the register. Then R_0 is clocked once in order to receive first output bit a_0. During all clock cycle for any $i > 1$ the following steps are performed:

1. The 2FCSR R_0 is clocked;
2. If the $a_i = 1$ then a_{i-1} forms a part from the output sequence; otherwise the output is discarded.
3. Repeat step 1.

The output sequence will be analyzed in section IV.

IV. PROPERTIES OF 2-ADIC FCSR SSG

Now the properties of 2-adic FCSR self shrinking generator will be analyzed.

A. *Period and linear complexity*

Let A is the output sequence of 2-FCSR R_0 with $d_0 = 2p_0 + 1$ strong 2-prime connection number.

Then its period will be $T_0 = d_0 - 1 = 2p_0$.

Let *K* is the result key sequence with period S_0 formed by the 2FCSR self shrinking generator and applied over the sequence A.

Let 2FCSR R_0 is again in its initial state after applied T_0 clock cycles.

The 2FCSR self shrinking generator outputs key bit in

the moment $i > 0$ only if $a_i = 1$.

After applying T_0 clock cycles the output bits of R_0 are balanced and the generated bits "1"will be p_0.

Hence the generated bits from 2FCSR self shrinking generator will be p_0 as well. It addresses the fact that the period S_0 divide p_0. This is impossible because p_0 is a prime number.

Consequently

$$S_0 = p_0 \tag{1}$$

Expression (1) defines that the linear complexity satisfies the following:

$$\lambda(K) \geq \log_2(p_0 + 1) \tag{2}$$

B. Analysis of crypto resistance

All attacks which are possible to affect the function of the Self-Shrinking pseudorandom generator [15] are inapplicable, due to the fact that they act against the generator constructed by LFSRs [3].

That's why constructing 2-adic FCSR self shrinking pseudorandom generator will significantly increase crypto resistance against multiple crypto attacks.

With a respect of [15] we recommend the design of the including FCSR to be upper than 512 memory cells in order to hinder the time-memory-data and the Backtracking Algorithm attacks.

C. Software modeling

The research of the 2-FCSR Self Shrinking Generator has been modeled by the Class p_adic using Visual C++. In order to generate 1000 sequences with 106 bits, the initial state of pseudorandom generator is renewed with new connection number d_0 after generation of every one sequence.

To analyze the properties of the output sequence more than 100 tests have been made with various initial states.

For investigation and analysis of the constructed 2-adic FCSR SSG 1000 strong 2-prime numbers in the interval 2073707 up to 3493163 have been used.

All generated keystream sequences are put together in one output file with volume 953MByte.

D. Statistical results

The output file is analyzed statistically by using NIST test suite. As it is known, in the NIST test suite [16] are included 15 tests - frequency (monobit), frequency within a block, runs, longest-run-of-ones in a block, binary matrix rank, discrete Fourier transform (spectral), non-overlapping template matching, overlapping template matching, Maurer's Universal statistical, linear complexity, serial, approximate entropy, cumulative sums, random excursions, random excursions variant. The results of the analysed generated pseudorandom sequence are given in Table 1.

TABLE 1. RESULTS OF TESTING 2FCSR SELF SHRINKING GENERATOR CONDUCTED BY NIST TEST SUITE

	Statistical test	Result	Proportion	p-value	Comment
1	Frequency (monobit)	Pass	1	0.000100	
2	Frequency within a block	Pass	0.9970	0.153763	
3	Cumulative sums	Pass	1.0	0.0	
4	Runs	Pass	0.9890	0.0	
5	Longest-run-of-ones in a block	Pass	0.9830	0.000100	
6	Binary matrix rank	Pass	0.9910	0.686955	
7	Discrete Fourier transform (spectral)	Pass	0.9880	0.000181	
8	Non-overlapping template matching	Pass	0.9906	0.000562	52 proportion values are 1.0
9	Overlapping template matching	Pass	0.9920	0.041709	
10	Maurer's "Universal statistical"	Pass	0.9810	0.000110	
11	Approximate entropy	Pass	1.0	0.0	
12	Random excursions	Pass	0.9911	0.523180	Avg. values
13	Random excursions variant	Pass	0.9874	0.384253	Avg. values
14	Serial	Pass	1.0	0.0	
15	Linear complexity	Pass	0.9870	0.228367	

As a result of conducted experiments it has been noticed very good parameters of output pseudorandom sequence. It is 100% for the all tested sequences and 75% for allocation of p-values (generalized p-valueT). It should be noted that in 4 tests (frequency, serial, entropy and cumulative sums) all 1000 sequences pass proportion of the passed test sequences. In addition to this 52 P-valueT from the test for Non-overlapping template matching are with value of 1,0 as well. The output sequence has properties of uniform allocations, non-compressibility and non-frequency.

I. CONCLUSION

In this paper a 2-adic SSG is proposed. The results of the conducted research show that Self-shrinking 2-adic Cryptographic Generator could be used as key generator in critical crypto applications. Its simple structure guaranties

easy software and fast hardware implementation.

Possible application of this kind of pseudorandom generator could be wireless networks not only in local areas but wide regions as well where a strong encryption of data streams required.

REFERENCES

[1] Massey J. L., Some applications of coding theory in cryptography. In P. G. Farrell, editor, Codes and Ciphers: Cryptography and Coding IV, pages 33-47, Essex, England, Formara Ltd, 1995.

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

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

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

[5] Klapper, A., 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

[6] J. Xu. Stream Cipher Analysis Based on FCSRs, PhD Dissertation, University of Kentucky, 2000 Available http://www.cs.engr.uky.edu/

[7] Coppersmith D., H. Krawczyk, Y. Mansour. The shrinking generator, Advances in Cryptology – EUROCRYPT'93, vol.773 of LNCS, pp22-39, Berlin, 1993 Springer-Verlag

[8] Krawczyk H. The shrinking generator: Some practical considerations. In R. Andersen,editor Fast Software Encryption '93, vol.809 of LNCS,pp45-46, Berlin.1994, Springer-Verlag

[9] Meier W., O. Staffelbach, The self-shrinking generator. In A.De Santis, editor, Advances in Cryptology – EUROCRYPT '94, vol.950 of LNCS, pp205-214, Berlin, 1995, Springer-Verlag

[10] Blackburn S.R. The linear complexity of the self-shrinking generator. IEEE Transactions on Information Theory, 45(6):2073-2077, September 1999

[11] 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.

[12] 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.

[13] 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.

[14] Stoyanov, B., Improved Cryptoanalysis of the Self-Shrinking p-adic Cryptographic Generator, Advanced Studies in Software and Knowledge Engineering, 2008, ISSN 1313-0455 (printed), ISSN 1313-048X (online), ISSN 1313-0501 (CD/DVD), International Book Series "INFORMATION SCIENCE & COMPUTING", Number 4, Supplement to the International Journal "INFORMATION TECHNOLOGIES & KNOWLEDGE", Volume 2/2008, pp. 112-115,
Available:http://www.foibg.com/ibs_isc/ibs-04/IBS-04-p18.pdf

[15] E. Zenner, M. Krause, S. Lucks. Improved Cryptanalysis of the Self-Shrinking Generator. LNCS, Vol. 2119, 2001, pp. 21-35.G. Young, "Book style with paper title and editor," in Plastics, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 1–9.

[16] Rukhin, A., J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, "A Statistical Test Suite for Random and Pseudo-Random Number Generators for Cryptographic Application", NIST Special Publication 800-22 (with revision May 15, 2001), Available http://csrc.nist.gov/rng/.