A Note On Self-Shrinking Lagged Fibonacci Generator

Moon K. Chetry and W. B. Vasantha Kandaswamy
(Corresponding author: Moon K. Chetry)

Department of Mathematics, Indian Institute of Technology Madras, Chennai-600036, India
(Email: moon@iitm.ac.in)

(Received Nov. 24, 2008; revised and accepted Feb. 9, 2009)

Abstract

Lagged Fibonacci Generators (LFG) are used as a building block of key-stream generator in stream cipher cryptography. In this note, we have used the self-shrinking concept in LFG and given an upper bound $\frac{2^{n+m}}{8}$ for the self-shrinking LFG, where n is the number of stage and m is the word size of the LFG. We have also shown that the bound is attained by all the LFGs of degree $n < 28$, result supported by experiments.

Keywords: Cryptography, LFG, LFSR, stream cipher

1 Introduction

In 1994, Meier and Staffelbach [5] proposed the 'self-shrinking generator', a stream cipher based on irregular decimation of the output of a linear-feedback shift register (LFSR), inspired by a related construction (using two registers) of Coppersmith, Krawczyk and Mansur [3]. 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. In this paper, we have used self-shrinking concept in LFG and found an upper bound for the shrunken output sequence. Meier et. al. in their paper [5] proved that the period of the self-shrunken sequence obtained from an m-sequence of an LFSR of length n is a divisor of 2^{n-1}. Their experiments have shown that for all m-LFSRs of length $n < 20$ the self-shrunken sequences attain maximum period 2^{n-1} except for $n = 3$, where for the recursion $a_n = a_{n-2} + a_{n-3}$, the period of the self-shrunken sequence is 2 instead of $2^{3-1} = 4$. In this paper, it was shown that the for self-shrinking lagged fibonacci generator, the upper bound which is proved as $\frac{2^{n+m}}{8}$ is attained for all the LFGs of length $n < 28$ including $n = 3$.

This paper is organized as follows: A brief introduction in Section 1. In Section 2, we will quickly recall the basic theory of self-shrinking linear feed-back shift register generators to make the paper self contained. In Section 3, there will be an analysis of self-shrinking lagged fibonacci generator. We will give an upper bound of the period of the output sequence. Finally conclusion in Section 4.

2 Self-Shrinking Linear Feed-back Shift Register

The self-shrinking generator uses only one LFSR whose output sequence is shrunken under the control of the LFSR itself [5]. It may be defined as follows: Let $(s) = s_0, s_1, \cdots$ be the output of a binary LFSR of length n. So (s) is an m-sequence of period $2^n - 1$. At time k, we consider the pair (s_{2k}, s_{2k+1}) of terms from the output of the LFSR. If $s_{2k} = 1$, the term s_{2k+1} is output by the self-shrinking generator. If $s_{2k} = 0$, no term is output. For example, suppose the output (s) of a primitive LFSR is the sequence 100000100001100010100111101000111001001011011101100110101011111 $\cdots$ of period $2^6 - 1$, then the self-shrinking generator based on the LFSR will output the sequence 00000100100110000111111100101111 $\cdots$.

Below some properties of self-shrunken maximum length LFSR-sequence will be recalled. The proofs of given theorems can be found in [5].

Theorem 1. *The period P of a self-shrunken maximum length LFSR-sequence produced by an LFSR of length n satisfies:*

$$2^{\lfloor \frac{n}{2} \rfloor} \leq P \leq 2^{n-1}$$

Theorem 2. *The linear complexity L of a self-shrunken maximum length LFSR-sequence produced by an LFSR of length n satisfies:*

$$L \geq 2^{\lfloor \frac{n}{2} \rfloor - 1}$$

The experimental results, shown by Meier and Staffelbach [5], reveal that the period of all self-shrunken maximum length LFSR-sequence produced by an LFSR of length n, attain the bound 2^{n-1}, where $n < 20$ except for $n = 3$. They have also conjectured with the help of their experiments that the linear complexity does not exceed the value $2^{n-1} - (n+2)$, which was proved later by Blackburn [1] in 1999.

3 Self-Shrinking Lagged Fibonacci Generator

Lagged Fibonacci Generator are used as a building block of key stream generator in stream cipher cryptography [4, 6]. The maximum possible period $(2^n - 1) * 2^{m-1}$ of an n-stage lagged fibonacci generator with word size m, as proved by R. P. Brent [2] in 1994, is attained if the feed-back polynomial is a primitive trinomial of degree $n > 2$ and at least one of the initializations is of odd value. Full period $(2^n - 1) * 2^{m-1}$ is attained only by the most significant bit. If the bits are numbered from 1 (least significant bit) to m (most significant bit), then bit k has period p_k i.e $(2^n - 1) * 2^{k-1}$. So $p_m = (2^n - 1) * 2^{m-1}$. The self-shrinking lagged fibonacci generator may be defined as follows: Let $(s) = s_0, s_1, \cdots$ be the output of an LFG of length n and word size m. So (s) is an m-sequence of period $(2^n - 1) * 2^{m-1}$ [2]. At time k, we consider the pair (s_{2k}, s_{2k+1}) of terms from the output of the LFG. If s_{2k} is odd, the term s_{2k+1} is output by the self-shrinking generator. If s_{2k} is even, no term is output. For example, suppose the output (s) of a primitive LFG sequence with degree 4 and word size 3 is 321553620102112323555022524776365113624106516367115026520372 $\cdots$ of period $(2^4 - 1) * 2^{3-1} = 60$, then the self-shrinking generator based on the LFG will output the sequence 2531502666311022 $\cdots$ of period $\frac{2^{4+3}}{8} = 16$.

We give below an upper bound of a self-shrinking lagged fibonacci generator. Our experiments also gives a strong feeling that the bound is attained for all LFGs.

Theorem 3. *The period P of a self-shrunken maximum length lagged fibonacci generator sequence produced by an LFG of length n and word size m satisfies*

$$P \leq \frac{2^{n+m}}{8}$$

Proof. We can view a lagged fibonacci generator of length n and word size m as a scrambler of m LFSRs each of length n with the same feed-back connection polynomial. The Ist LFSR corresponds to the 1stbit (least significant bit) of each of the m-sized word of the LFG. Similarly for other LFSRs. For all the LFSRs carry bit will be used as the input to the next LFSRs. Contents(1 or 0) of the the kth $(k = 1, 2, \cdots, n)$ cell of the ith $(i = 1, 2, \cdots, m)$ LFSR is the ith $(i = 1, 2, \cdots, m)$ bit of the kth cell word of the LFG. The period of the ith $(i = 1, 2, \cdots, m)$ LFSR is $(2^n - 1) * 2^{i-1}$. Within the full period $(2^n - 1) * 2^{m-1}$ of the LFG, the m-sequence of the 1st LFSR (whose period is $2^n - 1$) will be repeated 2^{m-1} times, the m-sequence of 2nd LFSR (whose period is $2(2^n - 1)$) will be repeated $\frac{2^{m-1}}{2}$ times. Continuing this way the m-sequence of the m-th LFSR (whose period is $(2^n - 1) * 2^{m-1}$) will occur once. In each clock an LFG will produce m-bit of output. As there is a one-one correspondence between $\{0, 1\}^m$ to Z_{2^m}, we can consider each m-bit word as an element of Z_{2^m} (i.e in $\{0, \cdots, 2^m - 1\}$) under the operation modulo 2^m. Now applying the self-shrinking concept in the LFG as described in [5] for LFSR, we will regularly clock the LFG to get a sequence $s = (s_0, s_1, s_2, \cdots)$ of period $(2^n - 1) * 2^{m-1}$ where $s_i \in \{0, \cdots, 2^m - 1\}$ and consider the sequence of pairs of the values $((s_0, s_1), (s_2, s_3), \cdots)$. If the first number of the pair is odd take the second number as the output of the LFG otherwise discard the both. Now, we can see that odd (even) value in the 1st cell in the LFG corresponds to an 1 (0) in the 1st cell of the 1st LFSR. Essencially, we can say whenever there is odd (even)value in the 1st cell of the LFG, there is an 1 (0) in the 1st cell of the 1st LFSR and conversely whenever there is an 1(0) in the 1st cell of the 1st LFSR, there is an odd (even) value in the 1st cell of the corresponding LFG. So we can establish an one to one relationship between self-shrunken LFG sequence and the self-shrunken sequence of the 1st (least significant) LFSR.

In a full LFG period i.e $(2^n - 1) * 2^{m-1}$, 1st LFSR sequence (whose period is $2^n - 1$)will repeat 2^{m-1} times and it is clear that within consecutive $2(2^n - 1)$ cycles of the 1st LFSR the self shrunken sequence of the 1st LFSR will occur once. The maximum period of the self shrunken sequence of the 1st LFSR is 2^{n-1} [5], so in $2(2^n - 1)$ cycles of the LFG output sequence least significant bit of the self shrunken LFSR sequence occur once and as least significant bit or the 1st LFSR output bit repeat 2^{m-1} times in one full period of the LFG, so self-shrunken sequence of the LFG will repeat after $2^{n-1} * \frac{2^{m-1}}{2}$ times. Hence we can say that the maximum period of the self-shrunken LFG sequence is $\frac{2^{n+m}}{8}$. □

4 Conclusions

In this paper we have used the self-shrinking concept to LFG and gives an upper bound $\frac{2^{n+m}}{8}$ for the self-shrinking lagged fibonacci generator, where n is the number of stage and m is the word size of the LFG. Our experiments have shown that the bound is attained by all the LFGs of degree $n < 28$, including $n = 3$, for which [5] shown that bound is not attained for the self-shrunken LFSR sequence.

References

[1] S. R. Blackburn, "The linear complexity of the self-shrinking generator", *IEEE Transactions on Information Theory*, vol. 45, no. 6, Sep. 1999.

[2] R. P. Brent, "On The periods of generalized Fibonacci recurrences", *Mathematics of Computation*, vol. 63, no. 207, pp. 389-401, July 1994,

[3] D. Coppersmith, H. Krawczyk and Y. Mansour, "The shrinking generator", *Proceedings of Crypto 93*, Springer-verlag, pp. 22-39, 1994.

[4] A. D. Elbayoumy and S. J. Shepherd, "Stream or block cipher for securing VoIP?," *International Journal of Network Security*, vol. 5, no. 2, pp. 128-133, 2007.

[5] W. Meier and O. Staffelbach, "The self-shrinking generator", *Proceedings of Advances in Cryptology, EuroCrypt '94*, Springer-Verlag, pp. 205-214, 1998.

[6] A. M. D. Rey and G. R. Sánchez, "On the security of "Golden" cryptography, *International Journal of Network Security*, vol. 7, no. 3, pp. 448-450, 2008.

[7] B. Schneier, *Applied Cryptography*, John Willey & Sons, New York, 1996.

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

Moon K. Chetry obtained his PhD in Mathematics from Indian Institute of Technology, Madras in the year 2005. His research interests include: Stream Cipher Cryptography, Finite Fields and Group Rings. He has published 7 research papers.

W. B. Vasantha Kandaswamy is an Associate Professor in the Department of Mathematics, Indian Institute of Technology, Madras. She received her PhD from Madras University. She has more than 200 research papers to her credit.