Arab Gulf Journal of Scientific Research, 23 (1), pp 1-6 (2005)

Original Paper Ref. No 2319

A Generator of One Linear Feedback Shift Register

مولد تسجيل ازاحي ذو تغذية مرتدة خطية وحيدة

علي عادل قانصو

Ali Adel Kanso

King Fahd University of Petroleum and Minerals (HCC),
Faculty of Sciences, Department of Mathematics, P.O. Box 2440, Hail, KSA
akanso@hotmail.com

جامعة الملك فهد للبترول والمعادن، كلية العلوم، قسم الرياضيات، ص.ب. 2440، حائل، المملكة العربية السعودية

Abstract: A keystream generator that is made up of a single linear feedback shift register and two sets of non-negative integers is presented for use in stream cipher applications. When the linear feedback shift register is primitive and the elements of the two sets are carefully chosen, the output sequence of the generator has a long period and high linear complexity. Lower bounds are provided for the appearance of all patterns of reasonable length, and for some correlation attacks. The output sequences of this generator may have some applications in cryptography and spread spectrum communications.

Keywords: Linear Feedback Shift Registers; New Self-Shrinking Generator; Stream Ciphers.

المستخلص: يقدم هذا البحث فكرة جديدة عن مولد تسجيل ازاحي، ذو تغذية مرتدة خطية وحيدة، وذلك بتوظيف فئتين من الأعداد الموجبة، لإستخدامها في تطبيقات التشفير الفيضية. يوضح البحث انه عند اختيار المسجل الخطي ذو التغذية المرتدة الأولى، وكذلك عناصر الفئتين المذكورتين بدقة، فان متوالية المخرجات لهذا المولد ستكون لها دورة طويلة وتعقيدات خطية عالية. يبين البحث، أيضاً، الحدود الدنيا التي سوف تظهر للتركيبات المختلفة، مقبولة الطول، كما يبين الحدود الدنيا لعوامل الاختراق ذات الصلة. وبناء على نتائج هذا البحث، فان هذا المولد يمكن استخدامه في تطبيقات حماية البرمجيات وكذلك في مجال الاتصالات.

كلمات مدخلية: تسجيلات ازاحية، تغذية خطية، مولد التضاؤل الذاتي، التشفيرات الفيضية.

Introduction

Cipher generators are usually subdivided into block ciphers and stream ciphers. Block ciphers operate with a fixed transformation on large blocks of plaintext, data (typically 128 bits in modern ciphers) and decrypt them as a single unit, whereas stream ciphers operate with time-varying transformation on individual plaintext bits.

A binary additive stream cipher is a synchronous stream cipher in which, the keystream, the plaintext and the ciphertext are sequences of binary digits. The output of the keystream generator, called the keystream sequence, $(z_1, z_2, z_3, ...)$, is added (modulo 2) bit-wise to the plaintext sequence $(m_1, m_2, m_3, ...)$, to produce the ciphertext sequence $(c_1, c_2, c_3, ...)$. Each secret key as input to the keystream generator corresponds to an output sequence. Since the secret key is shared between the sender and the receiver, the receiver can decrypt by adding (modulo 2) the output of the keystream generator to the ciphertext sequence, to obtain the plaintext sequence.

The goal in stream cipher design is to efficiently produce sequences with long periods, high linear complexities, and good statistical properties. Linear feedback shift registers (LFSRs) are known to produce sequences with long periods and good statistical properties, but can not be used directly in stream cipher applications because they have low linear complexities, (Golomb, 1982). Nevertheless, (LFSRs) are widely used as components inside stream ciphers. There are several methods to increase the linear complexity. One method is, to use several (LFSRs) and combine the output from each of them, using a Boolean function. Another method is, to use one (LFSR) to control outputs of other (LFSRs). There are two different control models. One is the clock-controlled generators, such as the stop/go generator, (Beth, *et al.* 1984) and Kanso's clock-controlled alternating step generator, (Kanso, 2003), and the other model is, the shrinking generators, such as the shrinking generator (Coppersmith, *et al.* 1994), and new self-shrinking generator, (Kanso, 2003).

This paper contains a proposal for a new stream cipher, called *Generator of One Linear Feedback Shift Register* (*GOLFSR*). The (*GOLFSR)* uses one (LFSR) and two disjoint finite sets of distinct non-negative integers. The secret key is often used to provide a value for the initial state of the (LFSR),

and the elements of the two disjoint sets.

The paper is constructed as follows:

(I) In the remainder of this section, we provide a full description of (LFSRs).

(II) In the second section, the construction of the generator is presented.

(III) In the third section, the properties of randomness of the output sequences of the generator such as, period, and linear complexity, and good statistical properties are established.

(IV) The fourth section presents a number of cryptanalytic attacks that can be applied to the generator.

(V) In the fifth section, a comparison between the introduced generator and related work is given.

(VI) Finally, the last section consists of the conclusion of this paper.

(I) Background

An (n-stage) linear feedback shift register (LFSR) is a device that generates binary sequences. An (LFSR) is made up of two parts: a shift register, (A), and a linear feedback function, (Q), (Golomb, 1982). The shift register, (A), consists of (n stages, $A_0, A_1, ..., A_{n-1}$), each of which contains one bit, (0 or 1). The contents of these stages at a given time (t) is known as, the state of the register (A) and is denoted by:

$$[\underline{A}_t = \underline{A}_0(t), \underline{A}_1(t), ..., A_{n-1}(t).$$

(Where at time $t = 0$ the state $\underline{A}_0 = A_0\ 0$),

$(A_1(0), ..., A_{n-1}(0)$ is called the initial state of A)].

The linear feedback function (Q), is a function that maps the state of (A) to the bit, (0 or 1), and it is of the form,

$$[Q(A_0(t), A_1(t), ...,$$

$$A_{n-1}(t)) = (C_0A_0(t) \oplus C_1A_1(t) \oplus ... \oplus C_{n-1}A_{n-1}(t)],$$

for some binary constants ($C_0, C_1, ..., C_{n-1}$) called the feedback coefficients. The feedback coefficients ($C_0, C_1, ..., C_{n-1}$), determine a polynomial

$$(C_0 \oplus C_1x^1 ... \oplus C_{n-1}x^{n-1} \oplus x^n)$$

of degree (n) associated with the feedback function (Q). We write ($h(x)$) to denote this polynomial, and call it, *the characteristic feedback polynomial* of the feedback shift register. Therefore, any (n-stage) (LFSR) can be uniquely described by a characteristic polynomial ($h(x)$) over the finite field of order 2.

When the register (A) is clocked at a time interval, the contents of (A) are shifted one bit to the left (i.e. the content of (Ai) is transferred into (A_{i-1} (i=1, 2, ..., n-1)) and the new content of (A_{n-1}) is computed by applying the feedback function (Q) to the old contents of (A). The above can be expressed as follows:

$$[A_i(t+1) = A_{i+1}(t),\ i = 0,\ 1,\ ....,\ n\text{-}2$$

$$A_{n-1}(t+1) = Q(A_0(t), ..., A_{n+1}(t)]$$

The binary sequence (A_t) generated by this device is the sequence of contents of the (0^{th}) stage (A_0) of (A) for all (t). [i.e. The sequence,

$$[A_t) = A_0, A_1, A_2, ...$$

where $A_t = A_0, (t) \in GF(2)$ for t = 0, 1, 2, ...].

The state sequence of this device is given by the sequence of states of the register (A):

$$[\underline{A}_t) = \underline{A}_0, \underline{A}_1, \underline{A}_2, ...$$

Where, $\underline{A}_t = A_0(t), A_1(t), ..., A_{n-1}(t)$ for $t = 0, 1, 2, ...]$

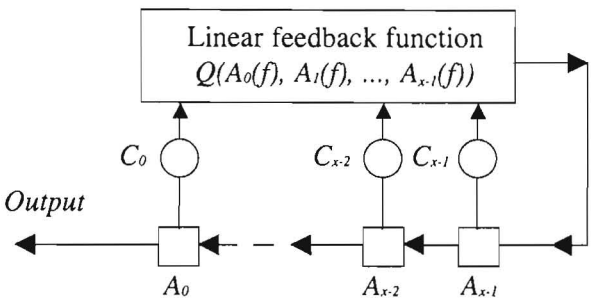

Fig.1 : *An n-stage, Linear Feedback Shift Register (LFSR)*

Since the output sequence of a linear feedback shift register (LFSR) is the content of the (0^{th}) stage of the register, each of the output sequence ($\underline{A}_t$) and the state sequence ($\underline{A}_t$) determine the other.

II. Construction

The Generator of One Linear Feedback Shift Register (GOLFSR), is composed of a single linear feedback shift register, and two finite disjoint sets of distinct non-negative integers, (S_1) and (S_2), at any time (t), the state of the generator is represented by the state of (LFSR) (A) at time (t). i.e. $\underline{G}_t = \underline{A}_t$.

Suppose that the register (A) has (n-stages) and characteristic feedback polynomial ($f(x)$).

Let ($\underline{A}_0 = A_0(0), A_1(0), ..., A_{n-1}(0)$), be the initial state of (LFSR (A)).

Suppose that

$(S_1 = \{a_1, a_2, ..., a_k\})$, and, $(S_2 = \{b_1, a_2, ..., b_m\})$. Select a window ($W$) of size ($w$) that consists of the first (w) consecutive stages of (LFSR (A))

(i.e. $A_0, A_1, ..., A_{w-1}$) such that ($w < n$).

Define a function (F) that acts on the state of (A) at a given time (t) to determine the integer value represented in the selected (w) fixed stages such that: At any time (t),

$$[F(\underline{A}_t) = [2^{w-1}A_{i_0}(t) + ... + 2^0 A_{i_{w-1}}(t)],\ (Eq.\ 1)$$

for ($w < n$) and ($i_0, i_1, ..., i_{w-1} \in \{0, 1, 2, ..., n\text{-}2\}$)]

At any time (t), the output of the generator is defined to be:

$$\begin{cases} (1), \text{ if } F(\underline{A_t}) \in S_1 \\ (0), \text{ if } F(\underline{A_t}) \in S_2 \\ \text{No output, otherwise.} \end{cases}$$

The output sequence of the generator, may also be described in terms of the output sequence (A_t) of the linear feedback shift register (LFSR, A), and the two sets (S_1) and (S_2).

Acting on its own, suppose that (A) produces an output sequence

$$[(A_t) = A_0, A_1, A_2, \ldots.]$$

For an (LFSR), the state sequence is related to the corresponding output sequence of the (LFSR) in the following way: At time (t), the state of (LFSR (A)).

$$[(A_t) = A_0, (t) \ldots., A_{n-1}(t) = A_t \ldots., A_{t+n-1}.]$$

Therefore, one can write the function (F) in terms of the output bits of (A).

Define a function (F_A) that acts at a given time (t) on certain bits of (A_t) to determine the output bit of the generator, such that:

[At time (t), $(F_A(t) = F(A_t, A_{t+1}, \ldots., A_{t+n-1}) = F(\underline{A_t})$].

[The output sequence (Z_t) of the generator is given by].

$$Z_t = \begin{cases} 1, \text{ if } F_A(\underline{t}) \in S_1 \\ 0, \text{ if } F_A(t) \in S_2 \\ \text{No output, otherwise.} \end{cases}$$

(III) Properties of the Output Sequence (Z_t)

Suppose that (LFSR, (A)) has initial state (A_0), and primitive characteristic feedback polynomial $(f(x))$ of degree (n). Then the output sequence

$$[(A_t) = A_0, A_1, A_2, \ldots.]$$

is an (m-sequence) of period (N) = (2^n-1) (Golomb, 1982).

Let $(S_1) = \{2^w-1\}$ and $(S_2) = \{2^w-2\}$. Let (Z_t) denote the resulting output sequence of this generator.

In the following lemmas, the period and the linear complexity of the output sequence (Z_t) are established. Finally, it is shown that the output sequence of the generator has good statistical properties.

- Period and Linear Complexity

We prove exponential bounds on the period and linear complexity of sequences, produced by the Generator of One Linear Feedback Shift Register (GOLFSR). In the case of the period, this bound is tight; for the linear complexity, there is a gap by a factor of (2) between the lower and upper bound.

After (N) = (2^n-1) clock pulses have been applied to (A), then it is back in its initial state $(\underline{A_0})$. Hence, the state sequence of the generator has period

$$(P_s) = (N) = (2^n-1).$$

Note that for $(w)=(1)$, at time (t), the integer value in the (0^{th}) stage of (A) is the element of the set $(S_1)=(1)$ or the set $(S_2)=(0)$.

Thus by definition, the output of the generator, is the contents of the (0^{th}) stage of (A). Therefore, the sequence (Z_t) produced by the generator is actually the (m)-sequence (A_t) itself.

The properties of (m-sequences) are well known (Golomb, 1982). Thus, we will establish the properties of the generator for (w>1). Thus, assume (w > 1), in a full period of (A), the number of states, in which the window (W), that consists of the first (w) consecutive stages of (A), (for w > 1), represents the integer values (2^w-1) and (2^w-2) is (2^{n-w}) (Golomb, 1982). Therefore, (N) = (2^n-1) after clock pulses, have been applied to (A) the generator produces,

$$[M = 2(2^{n-w}) = 2^{n-w+1} \text{ output bits}].$$

In the next lemma, we show that the period of the output sequence (Z_t) is equal to (2^{n-w+1}).

★ Lemma 1

The period of the output sequence

$$[(Zt) \text{ is equal to } 2^{n-w+1}].$$

★ Proof

Since the $(n$-stage) linear feedback shift register is chosen to produce an (m-sequence) (A_t), then every non-zero $(n$-bit) pattern appears exactly once in a full period $(N = 2^n-1)$ of (A_t). Hence, in a full period the $(n$-bit) pattern (111...1) appears exactly once in (A_t). From the definition of the generator, it follows that over a full period of (A_t) the (n-w+1-bit) pattern (111...1) appears exactly once in a cycle of length (2^{n-w+1}) of the output sequence (Z_t). Therefore, the period of the output sequence (Z_t) is $(P = 2^{n-w+1})$.

Next, we establish the linear complexity (L), of the output sequence (Z_t).

★ Definition 2

The linear complexity (L) of a periodic sequence (Z_t) is equal to the degree of its minimal polynomial. The minimal polynomial is defined, as the characteristic feedback polynomial of the shortest (LFSR) that can generate the sequence (Z_t).

★ Lemma 3

The linear complexity (L) of the output sequence (Z_t) satisfies $(L > 2^{n-w})$.

* Proof

Let $(Q(x))$ denote the minimal polynomial of (Z_t). From the previous lemma the period of (Z_t) is

$$[(P = 2^{n-w+1}). \text{ Hence over } (GF(2)),$$

$$(x^P-1) \text{ can be written as } (x^P-1) = (x-1)^P]$$

Thus, the condition $(Q(x))$ divides (x^P-1) implies that,

$[(Q(x))$ is of the form $(Q(x) = (x-1)^L)]$, where (L)

is the linear complexity of the sequence (Z_t). We claim that $(L > 2^{n-w})$.

Assume $(L \le 2^{n-w})$, then $(Q(x) = (x-1)^L)$ would divide $(x-1)^{2^{n-w}} = (x^{2^{n-w}}-1)$, but then the period of (Z_t) is at most (2^{n-w}), (Lidl *et al.* 1986) contradicting lemma 1. Therefore, the linear complexity (L) of the output sequence (Z_t) satisfies $(L > 2^{n-w})$:

● Statistical Properties

In this section, we count the exact appearance of the number of ones and zeroes in a full period $(P = 2^{n-w+1})$ of sequence (Z_t), then we move on to provide lower bounds for the appearance of all patterns of reasonable length.

The appearance of ones and zeroes, in a full period of the output sequence (Z_t): in a full period of (LFSR A), the number of states in which the window (W) that consists of (w) fixed stages of (A), represents the integer values (2^w-1), and (2^w-2) is (2^{n-w}). By the definition of the generator, it follows that the number of ones and zeroes in a full period

$P = 2^{n-w+1}$ of (Z_t) is 2^{n-w}.

Thus, the generated sequence (Z_t) is balanced.

★ Lemma 4

In a full period of (Z_t) any subsequence $(Z_i, Z_{i+1}, ..., Z_{i+\beta-2}, Z_{i+\beta-1})$ of length $(\beta \le [n-(w-1)(k+1),]$, where (k) is the total number of zeroes in the subsequence,

$Z_i, Z_{i+1}, ..., Z_{i+\beta-2}$, *occurs:*

$$\begin{cases} 2^{n-(\beta+(\omega-1))} \text{ times for } k = 0, \\ \text{and at least} \quad \text{(Eq. 2)} \\ \sum_{i=0}^{\lambda} \binom{(k-1)+i}{i} 2^{\lambda-1} \text{ times, otherwise} \end{cases}$$

Where $\lambda = n-[\beta + (w-1)(k+1)]$.

★ Proof

The sequence (A_t) is an (m-sequence) of period (2^n-1). Thus, in a full period of (A_t) each non-zero subsequence of length $(h \le n)$ occurs (2^{n-h}) times, and the all-zero subsequence of length $(h < n)$ occurs $(2^{n-h}-1)$ times (Golomb, 1982).

Suppose we want to determine a lower bound on the number of times any subsequence

$(Z_i, Z_{i+1} ..., Z_{i+\beta-2}\ Z_{i+\beta-2})$

of length (β) occurs in a full period $(P = 2^{n-w+1})$ of (Z_t). For (k=0), the subsequence,

$[(Z_i, Z_{i+1} ..., Z_{i+\beta-2}\ Z_{i+\beta-1})$ (for $\beta \le n-(w-1)$)),

in which $(Z_i = Z_{i+1} = ... = Z_{i+\beta-2} = 1$ or

$Z_i = Z_{i+1} = ... = Z_{i+\beta-2} = 1, Z_{i+\beta-1} = 0)]$,

will occur in (Z_t) whenever the subsequence

$(A_j, ..., A_{j+w-1}, ..., A_{j+(w-1)\beta-1}$, in which

$(A_j = A_{j+1} = ... A_{j+w-2} = 1$ occurs in $(Z_t))$ the sequence (A_t). Obviously, this will occur $(2^{n-(\beta+(w-1))})$ times in a full period of (A_t). Hence, the subsequence

$(Z_i, Z_{i+1} ..., Z_{i+\beta-2}\ Z_{i+\beta-1})$ will occur $(2^{n-(\beta+(w-1))})$ times in a full period of (Z_t).

For $(k \ne 0)$, the subsequence

$[(Z_i, Z_{i+1} ..., Z_{i+\beta-2}\ Z_{i+\beta-1})$ (for $\beta \le [n-(w-1)(k+1)])]$ will occur in the output sequence (Z_t) at least whenever the subsequence

$(A_j, ..., A_{j+w-1}, ..., A_{j+(w-1)(k+1)+\beta-1})$, (of length $(\beta + (w-1)(k+1)$ less than or equal to (n), in which each bit of $(Z_i, ..., Z_{i+\beta-2}\ Z_{i+\beta-1})$ is preceeded by a string of (1's) of length (w-1), occurs in a full period of the sequence (A_t).

Moreover, $(Z_i, Z_{i+1}, ..., Z_{i+\beta-2}, Z_{i+\beta-1})$ the subsequence will occur from subsequences in which each (0) in $(A_j, ..., A_{j+w-1}, ..., A_{j+(w-1)(k+1)+\beta-1})$, is replaced by subsequences of (0's) of length (y) where $(1 \le y \le (\lambda+1))$ and $(\lambda = n - [\beta + (w-1)(k+1)])$.

The total number of these subsequences in a full period of the original sequence (A_t) is:

$$\sum_{i=0}^{\lambda} \binom{(k-1)+i}{i} 2^{\lambda-1}$$

The subsequence $(Z_i, ..., Z_{i+\beta-2}, Z_{i+\beta-1})$, may also occur from other subsequences such as,

$[(A_j, ..., A_{j+w-1}, ..., A_{j+(w-1)(k+1)+\beta-1})$,

(for $(\beta) + (w-1)(k+1) > n)]$.

Therefore, in a full period $(P = 2^{n-w+1})$ of the output sequence (Z_t) any subsequence, $(Z_i, ..., Z_{i+\beta-2}, Z_{i+\beta-1})$ of length $(\beta \le [n-(w-1)(k+1)$, where (k) is the total number of zeroes in the subsequence $(Z_i, Z_{i+1}, ..., Z_{i+\beta-2})$ occurs $(2^{n-(\beta+(w-1))})$ times for (k=0), and at least

$$\sum_{i=0}^{\lambda} \binom{(k-1)+i}{i} 2^{\lambda-1}$$ *times, otherwise where* $\lambda = n-[\beta + (w-1)(k+1)]$

(IV) Cryptanalysis

A suitable stream cipher should be resistant against a known-plaintext attack. In a known-plaintext attack the cryptanalyst is given a plaintext, and the corresponding ciphertext, (in another words, the cryptanalyst is given a keystream), and the task is to reproduce the keystream somehow.

The most important general attacks on (LFSR-based), stream ciphers are correlation attacks. Basically, if a cryptanalyst can, in some way, detect a correlation between the known output sequence and the output of one individual (LFSR), this can be used in a divide and conquer attack on the individual

(LFSR). (Golic, *et al.* 1991); (Golic, *et al.* 1995); (Meier, *et al.* 1989); (Siegenthaler, 1984).

In this section we discuss some approaches for possible cryptanalytic attacks and their complexities. For cryptographic applications the key consists of the initial state, the size (w) of the selected window, the elements of the two sets (S_1) and (S_2), and, preferably, the characteristic feedback polynomial of the (LFSR). In order to assess the security of the generator, we assume that the characteristic feedback polynomial is known. With this assumption we estimate the difficulty of finding the initial state of the (LFSR).

We start with a general method for reconstructing the original sequence from the knowledge of a portion of the output sequence (Z_t). Assume that the size (w) of the window is known, and that (S_1) = $\{2^w-1\}$ and (S_2) = $\{2^w-2\}$. Assume that (Z_0, Z_1, ..., Z_{q-2}, Z_{q-1}) is the known portion of (Z_t). The bit (Z_0) is produced from the (w) bits (A_{j+1}, ..., A_{j+w-2}, A_{j+w-1}) of the sequence (A_t) where the index (j) is known.

Our aim is to reconstruct the sequence (A_t) in the forward direction, beginning with position (j). As we know (Z_0), we conclude that

$$(A_j = ... = A_{j+w-2} = 1), \text{ and, } (A_{j+w-1} = Z_0).$$

For the next (w) bits (A_{j+1} ...., A_{j+w}) there remain one possibility if (A_{j+w-1},$=Z_0 = 1$) that is ($A_{j+w} = Z_1$), otherwise (if A_{j+w-1},$=Z_0 = 0$) there remain two possibilities that is ($A_{j+w} = 0$, or, and so on. Let (k) be the total number of zeroes in the subsequence (Z_0, Z_1, ..., Z_{q-2}). For ($k \neq 0$), it can be shown by induction on (k) that the subsequence

(Z_0, Z_1, ..., Z_{q-2}, Z_{q-1}) arises from a total of:

$$[\Psi(n, k) = n-2)^{k-1} (n+k-2 \text{ (Esq. 3)}]$$

possible subsequences of (A_t). For (k=0), the subsequence (Z_0, Z_1, ..., Z_{q-2}, Z_{q-1}), zarises from one subsequence of (A_t). (i.e.) $\Psi(n, k) = 1$)

If a cryptanalyst obtains (q) consecutive bits of the sequence (Z_t), then, as (Z_t) is balanced, approximately half of these consecutive bits will be (0's) (i.e. k= $\frac{1}{2}$). So the subsequence

(Z_0, Z_1...., Z_{q-2}, Z_{q-1})

arises from approximately a total of:

$$[\Psi(n, \tfrac{q}{2}) = (n-2)\, \tfrac{q}{2}^{-1} (n+\tfrac{q}{2}^{-2}) \text{ (Eq. 4)}]$$

possible subsequences of (A_t).

For security reasons it is suggested to consider characteristic feedback polynomials of high hamming weight (Meier, *et al.* 1989). If the characteristic feedback polynomial is considered as part of the secret key, the reconstruction of the initial state has to be combined with an exhaustive search over all primitive characteristic feedback polynomials of degree n. Therefore, the complexity of the attack is increased by the factor $\varphi(2^n-1)$. Hence, the total complexity is:

$$\Omega_n(n, k) = \varphi(2^n-1) .\Psi(n, k) \text{ (Eq. 5)}$$

Furthermore, if the size (w) of the window is kept secret, then the complexity of the attack is ($w\Omega$) (n, k).

Thus, for maximum security, the key of the generator should consist of the initial state, the primitive characteristic feedback polynomial, the size (w) of the selected window, and the elements of the two sets (S_1) and (S_2). Subject to these constraints the generator has a security level approximately equal to ($w\Omega$) (n, k).

(V) Related Work

An interesting example of existing (LFSR) based constructions for comparison with the (GOLFSR), is the new self-shrinking generator (Kanso, 2003). The new self-shrinking generator can be seen as a special case of the (GOLFSR). It is actually a (GOLFSR) with the window (W) being the two first stages of (LFSR, A), and (S_1) = {3), (S_2), = {2}. Therefore, the (GOLFSR) may be seen as a generalisation of the new self-shrinking generator.

The advantage of this generator over any other stream cipher generator is that, one can generate a large family of sequences with long periods, high linear complexities, and good statistical properties, by simply selecting different values for (w).

(VI) Conclusion

From the theoretical results established, it is concluded that a (GOLFSR) of primitive (LFSR), and two sets (S_1) = $\{2^w-1\}$, (S_2), = $\{2^w-2\}$, generates sequences with long periods, high linear complexities, and good statistical properties. These characteristics and properties enhance its use, as building blocks, in stream cipher applications and spread spectrum communications.

References

Beth, T. and Piper, F. (1984) The Stop and Go Generator, Advances in Cryptology: Proceedings of Eurocrypt 84. Lecture Notes in Computer Sciences **209**: 88-92.

Coppersmith, D., Krawczyk, H. and Monsour, Y. (1994) The Shrinking Generator, Advances in Cryptology: Proceedings of Crypto 93. Lecture Notes in Computer Sciences **773**: 22-39.

Golic, J. and Mihaljevic, M. (1991) A Generalized Correlation Attack on a Class of Stream Ciphers Based on the Levenstein Distance. Journal of Cryptology **3**: 201.

Golic, J. (1995) Towards Fast Correlation Attacks on Irregularly Clocked Shift Registers, Proceedings of Cryptology: Eurocrypt 95. Lecture Notes in Computer Science **921**: 248-262.

Golomb, S. (1982) Shift Register Sequences. Aegean Park Press.

Kanso. A. (2003) Clock-Controlled Alternating Step Generator, Techno-Legal Aspects Information Society ands New Economy: An Overview. Formatex 12.

Kanso, A. (2003) New Self-Shrinking Generator. Proceedings of the Security and Protection of Information Conference 2003, IDET Brno, Czech Republic: 69.

Lidl, R. and Niederreiter, H. (1986) Introduction to Finite Fields and Their Applications. Cambridge University Press, UK.

Meier, W. and Staffelbach, O. (1989) Fast Correlation Attacks on Certain Stream Ciphers. Journal of Cryptology (**1**) (3): 159-176.

Siegenthaler, T. (1984) Correlation-Immunity of Non-linear Combining Functions for Cryptographic Applications. IEEE Trans. On Information Theory (**30**) (5): 776-780

Ref: 2319
Received 29/05/2004
In revised form 03/01/2005