KEYSTREAM SEQUENCES WITH A GOOD LINEAR COMPLEXITY PROFILE FOR EVERY STARTING POINT

Harald Niederreiter

Mathematical Institute, Austrian Academy of Sciences
Dr.-Ignaz-Seipel-Platz 2
A-1010 Vienna, Austria

1. INTRODUCTION AND PROBABILISTIC RESULTS

The linear complexity profile was introduced by Rueppel [7], [8, Ch. 4] as a tool for the assessment of keystream sequences with respect to randomness and unpredictability properties. In the following let F be an arbitrary field. We recall that a sequence of elements of F is called a kth-order linear feedback shift register (LFSR) sequence if it satisfies a kth-order linear recursion with constant coefficients from F. The zero sequence $0,0,\ldots$ is viewed as an LFSR sequence of order 0. Now let S be an arbitrary sequence $s_1,s_2,\ldots$ of elements of F. For a positive integer n the (local) linear complexity $L_n(S)$ is defined as the least k such that $s_1,s_2,\ldots,s_n$ form the first n terms of a kth-order LFSR sequence. The sequence $L_1(S),L_2(S),\ldots$ of integers is called the linear complexity profile (LCP) of S. For basic facts about the LCP see [4], [7], [8, Ch. 4].

The study of the LCP leads to the requirement that the LCP of a keystream sequence should simulate the LCP of a random sequence. Typical features of the LCP of a random sequence were investigated in [5], [7], [8, Ch. 4]. An additional requirement was pointed out by Piper [6], namely that a keystream sequence should have an acceptable LCP for every starting point. In other words, if S_m is the shifted sequence $s_{m+1},s_{m+2},\ldots$, then S_m should have an acceptable LCP for every $m = 0,1,\ldots$. In the present paper we are mainly concerned with this requirement.

A basic technical device in this work is the identification of the sequence S with its generating function $\sum_{i=1}^{\infty} s_i x^{-i}$, viewed as an element of the field $G = F((x^{-1}))$ of formal Laurent series in x^{-1} over F (compare also with [4]). For the probabilistic theory we take F to be the finite field F_q with q elements, where q is an arbitrary prime power. Note that in practical stream cipher applications we have the binary case $q = 2$. The uniform probability measure on F_q assigns

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 523-532, 1990.

the measure $1/q$ to each element of F_q. This probability measure induces the complete product probability measure h on the set F_q^∞ of all sequences of elements of F_q by a standard procedure of probability theory (see [2, Sec. 4]). It is easily seen that the measure h is the same as the Haar measure used in [5] when the latter measure is transferred from the set of all generating functions to the set F_q^∞. We say that a stated property of elements of F_q^∞ holds h-almost everywhere (h-a.e.) if the property holds for all elements of a subset of F_q^∞ of h-measure 1. A property that holds h-a.e. can be viewed as a typical property of a random sequence of elements of F_q.

Theorem 1. Let Π be a property of elements of F_q^∞ that holds h-a.e. Then the set of all $S \in F_q^\infty$ for which Π holds simultaneously for all shifted sequences S_m, $m = 0,1,\ldots,$ has h-measure 1.

Proof. Let P be the set of all elements of F_q^∞ which have the property Π and let V be the set of all $S \in F_q^\infty$ for which $S_m \in P$ for all $m = 0,1,\ldots$. Let τ be the unilateral shift operator on F_q^∞ defined by

$$\tau(s_1,s_2,\ldots) = (s_2,s_3,\ldots) \quad \text{for } (s_1,s_2,\ldots) \in F_q^\infty.$$

Then $S_m = \tau^m S$, thus $S_m \in P$ if and only if S lies in the mth iterated inverse image $\tau^{-m}P$. Therefore $V = \bigcap_{m=0}^{\infty} \tau^{-m}P$. Now τ is measure-preserving with respect to h by [1, Ch. 1], and so $h(\tau^{-m}P) = h(P) = 1$ for all m. Thus we get $h(V) = 1$. □

Theorem 2. If $F = F_q$, then h-a.e. we have

$$\lim_{n\to\infty} \frac{L_n(S_m)}{n} = \frac{1}{2} \quad \text{for } m = 0,1,\ldots,$$

$$\limsup_{n\to\infty} \text{inf} \quad \frac{L_n(S_m) - (n/2)}{\log n} = \pm \frac{1}{2 \log q} \quad \text{for } m = 0,1,\ldots.$$

Proof. This follows from Theorem 1 and [5, Theorems 7 and 10]. □

From Theorem 1 one can deduce various other probabilistic results. For example, all the probabilistic results in [5] hold simultaneously for all shifted sequences S_m, with Theorem 2 just covering two instances that are easy to state. In particular, the results about the distribution of partial quotients in the continued fraction expansion of a random generating function S hold simultaneously for all S_m. In a nutshell, Theorem 1 provides the basis for saying that Piper's requirement is met by random sequences of elements of F_q.

2. SEQUENCES WITH A GOOD LINEAR COMPLEXITY PROFILE

We introduce a class of sequences for which the LCP is close to that of a random sequence and for which this property is retained under shifts. Put $\operatorname{Log} t = \max(1, \log t)$ for $t \geq 1$.

Definition 1. A sequence S of elements of the field F has a good LCP if there exists a constant C (which may depend on S) such that

$$|L_n(S) - \frac{n}{2}| \leq C \operatorname{Log} n \quad \text{for} \quad n = 1,2,\ldots .$$

If $F = F_q$, then it follows from [5, Theorem 10] that the property of having a good LCP holds h-a.e. For further analysis we need the connection between the LCP and continued fractions as developed in [4]. Every $S \in G$ has a unique continued fraction expansion

$$S = A_0 + 1/(A_1 + 1/(A_2 + \ldots)) =: [A_0, A_1, A_2, \ldots]$$

with $A_j \in F[x]$ for $j \geq 0$ and $\deg(A_j) \geq 1$ for $j \geq 1$. This expansion is finite for rational S and infinite for irrational S. The polynomials $A_j, j \geq 1$, are called the partial quotients and $A_0 =: \operatorname{Pol}(S)$ is the polynomial part of S. The polynomials P_j and Q_j are defined as in [4] and P_j/Q_j is called a convergent. We note that

$$\deg(Q_j) = \sum_{i=1}^{j} \deg(A_i) \quad \text{for} \quad j \geq 1. \tag{1}$$

Then we have the following formula [4, Theorem 1].

Lemma 1. For any sequence S of elements of F and any $n \geq 1$ we have $L_n(S) = \deg(Q_j)$, where $j \geq 0$ is uniquely determined by the condition

$$\deg(Q_{j-1}) + \deg(Q_j) \leq n < \deg(Q_j) + \deg(Q_{j+1}). \tag{2}$$

Proposition 1. If the generating function of a sequence S is irrational and $\deg(A_j) \leq C \operatorname{Log} j$ for all $j \geq 1$, where C is a constant, then

$$|L_n(S) - \frac{n}{2}| \leq \frac{C}{2} \operatorname{Log} n \quad \text{for all} \quad n \geq 1.$$

Proof. Consider an n satisfying (2) and first assume $j \geq 2$. Then $L_n(S) = \deg(Q_j)$ by Lemma 1, hence using (1) we get

$$|L_n(S) - \tfrac{n}{2}| = |\deg(Q_j) - \tfrac{n}{2}| \leq \tfrac{1}{2} \max(\deg(A_j), \deg(A_{j+1}))$$

$$\leq \tfrac{C}{2} \operatorname{Log}(j+1) \leq \tfrac{C}{2} \operatorname{Log}(\deg(Q_j) + 1) \leq \tfrac{C}{2} \operatorname{Log} n.$$

The proposition is easily checked for $j = 0$ and $j = 1$. □

Proposition 2. If a sequence S satisfies $|L_n(S) - (n/2)| \leq C \operatorname{Log} n$ for some constant $C \geq 1$ and all $n \geq 1$, then its generating function is irrational and

$$\deg(A_j) < (4C \operatorname{Log} C + 8C) \operatorname{Log} j \quad \text{for all } j \geq 1. \tag{3}$$

Proof. The given condition on $L_n(S)$ implies $\lim_{n\to\infty} L_n(S) = \infty$, and so the generating function of S is irrational. To prove (3) we proceed by contradiction, and we let j be the least index such that the inequality in (3) does not hold. First assume $j = 1$, so that

$$\deg(A_1) \geq 4C \operatorname{Log} C + 8C.$$

For $n = \deg(A_1) - 1$ we have $n \geq 4C \operatorname{Log} C + 7C$ and also $L_n(S) = 0$ by Lemma 1. Thus

$$|L_n(S) - \tfrac{n}{2}| = \tfrac{n}{2} \geq \frac{4C \operatorname{Log} C + 7C}{2 \log(4C \operatorname{Log} C + 7C)} \log n$$

since the function $t/\log t$ is increasing for $t \geq e$. By distinguishing between the cases $1 \leq C \leq e$ and $C > e$ one shows that

$$4 \operatorname{Log} C + 7 > 2 \log(4C \operatorname{Log} C + 7C) \quad \text{for all } C \geq 1,$$

and so $|L_n(S) - (n/2)| > C \operatorname{Log} n$, a contradiction. Now let $j \geq 2$. Then with $C_1 = 4C \operatorname{Log} C + 8C$ we have $\deg(A_i) < C_1 \operatorname{Log} i$ for $1 \leq i < j$. Together with (1) we get

$$\log \deg(Q_j) < \log(\deg(A_j) + C_1 \sum_{i=1}^{j-1} \operatorname{Log} i) \leq \log(\deg(A_j) + C_1(j-1) \operatorname{Log} j).$$

Since the function $t^{-1}\log(t + C_1(j-1) \operatorname{Log} j)$ is decreasing for $t \geq e$ and since $\deg(A_j) \geq C_1 \operatorname{Log} j$, it follows that

$$\log \deg(Q_j) < \frac{\log(C_1 j \operatorname{Log} j)}{C_1 \operatorname{Log} j} \deg(A_j).$$

For $n = \deg(Q_{j-1}) + \deg(Q_j)$ we have by Lemma 1 and (1),

$$|L_n(S) - \tfrac{n}{2}| = |\deg(Q_j) - \tfrac{1}{2}(\deg(Q_{j-1}) + \deg(Q_j))| = \tfrac{1}{2}\deg(A_j)$$

$$> \frac{C_1 \operatorname{Log} j}{2 \log(C_1 j \operatorname{Log} j)} \log \deg(Q_j) > \frac{C_1 \operatorname{Log} j}{2 \log(C_1 j \operatorname{Log} j)} \log \tfrac{n}{2}.$$

Now $n \geq \deg(A_j) + 2\deg(A_{j-1}) \geq C_1 \operatorname{Log} j + 2$, and so

$$|L_n(S) - \tfrac{n}{2}| > \frac{C_1 \operatorname{Log} j}{2 \log(C_1 j \operatorname{Log} j)} \left(1 - \frac{\log 2}{\log(C_1 \operatorname{Log} j + 2)}\right) \log n.$$

Therefore, to arrive at the contradiction $|L_n(S) - (n/2)| > C \operatorname{Log} n$, it suffices to show that

$$(2 \operatorname{Log} C + 4)\left(1 - \frac{\log 2}{\log(C_1 \operatorname{Log} j + 2)}\right) \geq \frac{\log(C_1 j \operatorname{Log} j)}{\operatorname{Log} j}. \tag{4}$$

To prove (4), we first consider $j = 2$. Then (4) attains the simpler form

$$(2 \operatorname{Log} C + 4)\left(1 - \frac{\log 2}{\log(C_1 + 2)}\right) \geq \log(2C_1).$$

We have

$$(2 \operatorname{Log} C + 4)\left(1 - \frac{\log 2}{\log(C_1 + 2)}\right) \geq (2 \operatorname{Log} C + 4)\left(1 - \frac{\log 2}{\log 14}\right) > (1.47)\operatorname{Log} C + 2.94.$$

For $1 \leq C \leq e$ it follows that

$$(2 \operatorname{Log} C + 4)\left(1 - \frac{\log 2}{\log(C_1 + 2)}\right) > 4.41 > \log(24e) \geq \log(24C) = \log(2C_1).$$

Since the function $(0.47)t - \log(t+2)$ is increasing for $t \geq 1$, we obtain $(0.47)t + 0.86 > \log(t+2)$ for $t \geq 1$, and so

$$(0.47)\log C + 0.86 > \log(\log C + 2) \quad \text{for } C \geq e.$$

It follows that

$$(1.47)\log C + 2.94 > \log C + \log 8 + \log(\log C + 2) = \log(2C_1) \quad \text{for } C \geq e,$$

hence (4) is shown for $j = 2$. For $j \geq 3$ we have

$$1 - \frac{\log 2}{\log(C_1 \operatorname{Log} j + 2)} \geq 1 - \frac{\log 2}{\log(12 \log 3 + 2)} > 0.74.$$

Since the function $\log(C_1 t \log t)/\log t$ is decreasing for $t \geq e$, we obtain (4) for $j \geq 3$ if we can show that

$$(1.48)\text{Log } C + 2.96 \geq \frac{\log(3C_1 \log 3)}{\log 3}. \tag{5}$$

For $1 \leq C \leq e$ we have

$$(1.48)\text{Log } C + 2.96 = 4.44 > \frac{\log(36e \log 3)}{\log 3} \geq \frac{\log(3C_1 \log 3)}{\log 3},$$

hence (5) holds. The function $(0.62)t - \log(t+2)$ is increasing for $t \geq 1$, thus $(0.62)t + 0.67 > \log(t+2)$ for $t \geq 1$, and so

$$(0.62)\log C + 0.67 > \log(\log C + 2) \quad \text{for } C \geq e.$$

Adding $\log C + \log(12 \log 3)$ on both sides and then dividing by $\log 3$, we obtain (5). □

Theorem 3. A sequence S has a good LCP if and only if its generating function is irrational and there exists a constant C (which may depend on S) such that $\deg(A_j) \leq C \text{ Log } j$ for all $j \geq 1$.

Proof. This follows from Propositions 1 and 2. □

Note that the generating function of S is irrational if and only if S is not an LFSR sequence (see [4, Sec. 2]). We now use the valuation v on G introduced in [4, Sec. 3]. We also write $\text{Fr}(S) = S - \text{Pol}(S)$ for $S \in G$.

Lemma 2. If $S \in G$ and $f,g \in F[x]$ with $f \neq 0$ and $v(fS - g) < -v(f)$, then $f = DQ_j$ and $g = DP_j$ for some $j \geq 0$, where $D \in F[x]$ and $D \neq 0$.

Proof. We have $v(fS - g) < 0$, so [4, Lemma 3] can be applied and yields $f = \sum_{k=0}^{j} D_k Q_k$, $g = \sum_{k=0}^{j} D_k P_k$, where $D_k \in F[x]$, $v(D_k) < v(A_{k+1})$ for $0 \leq k \leq j$, and $D_j \neq 0$; moreover, if i is the least index with $D_i \neq 0$, then $v(fS - g) = v(D_i) - v(Q_{i+1})$. If we had $i < j$, then

$$v(fS - g) \geq v(D_i) - v(Q_j) \geq -v(Q_j) \geq -v(f),$$

a contradiction. Thus $i = j$, hence $f = DQ_j$ and $g = DP_j$ with $D = D_j$. □

Lemma 3. Let $S \in G$ and $f,g \in F[x]$ with $fg \neq 0$. Let $\frac{f}{g}S = [A'_0, A'_1, A'_2, \ldots]$ and let P'_j/Q'_j be the corresponding convergents. If $v(A'_j) > v(f) + v(g)$ for some $j \geq 1$, then there exists an $i \geq 1$ such that $v(A'_j) \leq v(A_i) + v(f) + v(g)$ and $v(Q_{i-1}) \leq v(Q'_{j-1}) + v(f)$.

Proof. By [4, eq. (6)] we have $v(Q'_{j-1}\frac{f}{g}S - P'_{j-1}) = -v(Q'_{j-1}) - v(A'_j)$, hence $v(A'_j) > v(f) + v(g)$ implies $v(fQ'_{j-1}S - gP'_{j-1}) < -v(fQ'_{j-1})$. Then Lemma 2 yields $fQ'_{j-1} = DQ_{i-1}$ and $gP'_{j-1} = DP_{i-1}$ for some $i \geq 1$, where $D \in F[x]$ and $D \neq 0$. It follows that $v(Q_{i-1}) \leq v(DQ_{i-1}) = v(Q'_{j-1}) + v(f)$. Moreover,

$$\begin{aligned} v(A'_j) &\leq v(A_j) - v(Q_{i-1}) + v(Q'_{j-1}) + v(f) \\ &= -v(Q_{i-1}) - v(fQ'_{j-1}S - gP'_{j-1}) + v(f) + v(g) \\ &= -v(Q_{i-1}) - v(DQ_{i-1}S - DP_{i-1}) + v(f) + v(g) \\ &\leq -v(Q_{i-1}) - v(Q_{i-1}S - P_{i-1}) + v(f) + v(g) = v(A_i) + v(f) + v(g), \end{aligned}$$

where we used again [4, eq. (6)] in the last step. □

Theorem 4. If S has a good LCP and $f,g \in F[x]$ with $fg \neq 0$, then the sequence with generating function $Fr(\frac{f}{g}S)$ has a good LCP.

Proof. We use the notation in Lemma 3 and recall that $v(f) = \deg(f)$ for any $f \in F[x]$. We have $Fr(\frac{f}{g}S) = [0,A'_1,A'_2,\ldots]$. The hypothesis and Theorem 3 yield $v(A_i) \leq C \operatorname{Log} i$ for all $i \geq 1$. Now let $j \geq 1$ be such that $v(A'_j) > v(f) + v(g)$. Then Lemma 3 implies $v(A'_j) \leq C \operatorname{Log} i + v(f) + v(g)$ and $i \leq v(Q_{i-1}) + 1 \leq v(Q'_{j-1}) + v(f) + 1$, thus

$$v(A'_j) \leq C \operatorname{Log}(v(Q'_{j-1}) + v(f) + 1) + v(f) + v(g). \tag{6}$$

This holds trivially if $v(A'_j) \leq v(f) + v(g)$, and so (6) holds for all $j \geq 1$. Now let $n \geq 1$ be arbitrary, then with a suitable $j \geq 0$ we get by Lemma 1 and (6),

$$\begin{aligned} |L_n(Fr(\tfrac{f}{g}S)) - \tfrac{n}{2}| &\leq \tfrac{1}{2}\max(v(A'_j), v(A'_{j+1})) \\ &\leq \tfrac{C}{2}\operatorname{Log}(v(Q'_j) + v(f) + 1) + \tfrac{1}{2}v(f) + \tfrac{1}{2}v(g) \\ &\leq \tfrac{C}{2}\operatorname{Log}(n + v(f) + 1) + \tfrac{1}{2}v(f) + \tfrac{1}{2}v(g) \leq C_1 \operatorname{Log} n \end{aligned}$$

with a suitable constant C_1. □

Corollary 1. If S has a good LCP, then every shifted sequence S_m, $m = 1,2,\ldots$, has a good LCP.

Proof. The generating function of S_m is given by $Fr(x^m S)$, and so the desired result follows from Theorem 4. □

For $S \in G$ we put $K(S) = \sup_{j \geq 1} \deg(A_j)$. If the sequence S has an irrational generating function and $K(S) < \infty$, then Theorem 3 shows that S has a good LCP. Thus by Corollary 1, every shifted sequence S_m has a good LCP. More precisely we have the following.

Theorem 5. Let $S \in G$ with $K(S) < \infty$ and $f,g \in F[x]$ with $fg \neq 0$. Then

$$K(\tfrac{f}{g}S) \leq K(S) + \deg(f) + \deg(g).$$

Proof. If in the notation of Lemma 3 we have $v(A'_j) > v(f) + v(g)$ for some $j \geq 1$, then by this lemma we get $v(A'_j) \leq K(S) + v(f) + v(g)$, and the latter inequality holds trivially if $v(A'_j) \leq v(f) + v(g)$. Recall also that $v(f) = \deg(f)$ for any $f \in F[x]$. □

Corollary 2. If $K(S) < \infty$, then $K(S_m) \leq K(S) + m$ for $m = 1,2,\ldots$.

Proof. This follows from Theorem 5 since the generating function of S_m is $Fr(x^m S)$. □

In particular, Corollary 2 shows that if $K(S) < \infty$, then $K(S_m) < \infty$ for all m. The result of Corollary 2 is in general best possible, as is proved by considering the following generalized Rueppel sequence S constructed in [3]. Let $F = F_2$ and let $s_i = 1$ if $i = 2^j - 1$ for some $j \geq 1$ and $s_i = 0$ otherwise. Then $K(S) = 1$ by [3, p. 232]. Now let $m = 2^j - 1$ for some $j \geq 1$. Then the generating function of S_m has the form x^{-2^j} + smaller powers, and so the first partial quotient of S_m has degree 2^j. Thus $K(S_m) \geq 2^j$. On the other hand, Corollary 2 yields $K(S_m) \leq K(S) + m = 2^j$, hence $K(S_m) = 2^j$. Thus for this sequence S we have $K(S_m) = K(S) + m$ for infinitely many m.

3. SEQUENCES WITH A UNIFORMLY GOOD LINEAR COMPLEXITY PROFILE

It follows from Corollary 1 that if S has a good LCP, then for every $m \geq 0$ there exists a constant C_m (which may depend on S and m) such that

$$|L_n(S_m) - \tfrac{n}{2}| \leq C_m \operatorname{Log} n \quad \text{for all } n \geq 1.$$

In this context it is of interest to consider the following notion.

Definition 2. A sequence S of elements of the field F has a uniformly good LCP if there exists a constant C (which may depend on S but not on m) such that

$$|L_n(S_m) - \frac{n}{2}| \leq C \text{ Log } n \quad \text{for all } m \geq 0 \text{ and } n \geq 1.$$

Theorem 6. If $F = F_q$, then the set of all sequences with a uniformly good LCP has h-measure 0.

Proof. Let W be the set in question. Let the sequence $S \in F_q^\infty$ be such that it contains somewhere a string of zeros of length $r \geq 1$, and let s_{k+1} be the first term of this string. Then $L_r(S_k) = 0$, hence if also $S \in W$, then it follows from Definition 2 that

$$|L_r(S_k) - \frac{r}{2}| = \frac{r}{2} \leq C \text{ Log } r.$$

This implies that r is bounded from above by a constant which depends only on C. Thus $W \subseteq B$, where B is the set of all $S \in F_q^\infty$ for which all strings of zeros have bounded length. We have $B = \bigcup_{r=1}^{\infty} B_r$, where B_r is the set of all $S \in F_q^\infty$ for which all strings of zeros have length $\leq r$. Fix $r \geq 1$, and for any integer $t \geq 0$ let $B_r^{(t)}$ be the set of all $S \in F_q^\infty$ with the following property: for each $j = 0,1,\ldots,t$ at least one of the terms $s_{j(r+1)+1}, s_{j(r+1)+2}, \ldots, s_{(j+1)(r+1)}$ is $\neq 0$. Then $B_r \subseteq \bigcap_{t=0}^{\infty} B_r^{(t)}$. The probability that at least one of any $r+1$ consecutive s_i is $\neq 0$ is given by $1 - q^{-r-1}$, and so $h(B_r^{(t)}) = (1 - q^{-r-1})^{t+1}$. It follows that

$$h(B_r) \leq h(\bigcap_{t=0}^{\infty} B_r^{(t)}) \leq (1 - q^{-r-1})^{t+1} \quad \text{for all } t \geq 0,$$

and letting $t \to \infty$ on the right we get $h(B_r) = 0$. This yields $h(B) = 0$, and so $W \subseteq B$ implies $h(W) = 0$. □

Theorem 6 shows that having a uniformly good LCP is not a typical property of a random sequence of elements of F_q. Sequences with a uniformly good LCP can also be characterized in terms of continued fraction expansions. Let $[0, A_1^{(m)}, A_2^{(m)}, \ldots]$ be the continued fraction expansion of the generating function of the shifted sequence S_m, $m = 0,1,\ldots$.

Theorem 7. A sequence S has a uniformly good LCP if and only if its generating function is irrational and there exists a constant C (which may depend on S but not on m) such that $\deg(A_j^{(m)}) \leq C \text{ Log } j$ for all $j \geq 1$ and $m \geq 0$.

Proof. This follows from Propositions 1 and 2. □

It is an open question whether there actually exists a sequence with a uniformly good LCP. Another open question is to decide whether there exists a sequence S for

which $\sup_{m=0,1,\ldots} K(S_m) < \infty$. A positive answer to the second question will of course imply a positive answer to the first question.

REFERENCES

[1] U. Krengel: Ergodic Theorems, de Gruyter, Berlin, 1985.

[2] M. Loève: Probability Theory, 3rd ed., Van Nostrand, New York, 1963.

[3] H. Niederreiter: Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences, Contributions to General Algebra 5 (Proc. Salzburg Conf., 1986), pp. 221-233, Teubner, Stuttgart, 1987.

[4] H. Niederreiter: Sequences with almost perfect linear complexity profile, Advances in Cryptology - EUROCRYPT '87 (D. Chaum and W. L. Price, eds.), Lecture Notes in Computer Science, Vol. 304, pp. 37-51, Springer, Berlin, 1988.

[5] H. Niederreiter: The probabilistic theory of linear complexity, Advances in Cryptology - EUROCRYPT '88 (C. G. Günther, ed.), Lecture Notes in Computer Science, Vol. 330, pp. 191-209, Springer, Berlin, 1988.

[6] F. Piper: Stream ciphers, Elektrotechnik und Maschinenbau 104, 564-568 (1987).

[7] R. A. Rueppel: Linear complexity and random sequences, Advances in Cryptology - EUROCRYPT '85 (F. Pichler, ed.), Lecture Notes in Computer Science, Vol. 219, pp. 167-188, Springer, Berlin, 1986.

[8] R. A. Rueppel: Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.