Clock-Controlled Shift Registers for Key-Stream Generation

Alexander Kholosha

Department of Mathematics and Computer Science
Technische Universiteit Eindhoven, P.O. Box 513,
5600 MB Eindhoven, The Netherlands
A.Kholosha@tue.nl

Abstract. In this paper we estimate the period of the sequence generated by a clock-controlled LFSR with an irreducible feedback polynomial and an arbitrary structure of the control sequence, as well as some randomness properties of this sequence including element distribution and the autocorrelation function. Also we construct and analyze a specific key-stream generator that applies clock-control. Finally, we present a comprehensive survey of known correlation attacks on clock-controlled registers and their memoryless combiners.

1 Introduction

Linear feedback shift registers (LFSR) are known to allow fast implementation and produce sequences with large period and good statistical properties (if the feedback polynomial is chosen appropriately). But inherent linearity of these sequences results in susceptibility to algebraic attacks and that is the prime reason why LFSR's are not used directly for key-stream generation. A well-known method for increasing the linear complexity preserving at the same time a large period and good statistical properties, is a nonlinear transformation applied to several phases of the same LFSR (filter generator) or to the outputs of several LFSR's (combination generator) [25, 26]. An alternative way to achieve the same goal is to control the LFSR clock. On the other hand, key-stream generators based on regularly clocked LFSR's are susceptible to basic and fast correlation attacks. Using irregular clocking reduces the danger from correlation attacks and provides practical immunity to fast correlation attacks.

The basic building block that we want to use for constructing a key-stream generator, consists of a control register CR and a clock-controlled generating register GR. A control register generates a sequence of nonnegative integers $a = \{a_i\}_{i \geq 0}$ and cycles periodically with period π. Hereafter in this paper by period we mean least period of a sequence being opposite to multiple period. A generating register is an LFSR over $P = \mathrm{GF}(q)$ with *irreducible* feedback polynomial $f(x)$ of degree $m > 1$ and order M. Let $b = \{b(i)\}_{i \geq 0}$ denote the output sequence from the GR when clocked regularly and α be a root of $f(x)$ in the splitting field of $f(x)$. In some cases further in this paper primitiveness of

$f(x)$ will be required. Then $\lambda = q^m - 1$ will denote the maximal possible order of $f(x)$. Let also S denote $\sum_{k=0}^{\pi-1} a_k$.

In the clock-controlled mode, the output sequence $u = \{u(t)\}_{t\geq 0}$ is generated in the following way. The initial output is $u(0) = b(a_0)$. Further, after the output $u(t-1)$ has been generated, the CR specifies the nonnegative integer a_t, the GR is shifted a_t times and then produces the next output $u(t)$. After that, the CR is shifted once to be ready for the next iteration. Thus, the general form of an output sequence element is

$$u(t) = b\left(\sum_{i=0}^{t} a_i\right) \quad \text{for} \quad t \geq 0\ . \tag{1}$$

In the sequel, by irregular clocking will we mean the above type of clock control applied to the GR. According to the classification in [26, p.101], the described clock control technique is a forward clock control (as opposed to feedback clock control). A comprehensive survey on clock-controlled shift registers can be found in [17].

In order to ensure security of a key-stream generator against the Berlekamp-Massey algorithm, its output sequence should have large period and high linear complexity. On the other hand, good statistical properties of the output sequence prevent the reconstruction of statistically redundant plaintext from the known ciphertext. That is the reason why these characteristics are discussed in details further in this paper.

Section 2 contains some results about uniform decimation of linear recurring sequences in the field $P = \mathrm{GF}(q)$. These results are further used in Section 3. Theorem about certain properties of sequences, obtained by uniform decimation, is formulated, and proof along novel lines is given. This theorem is a slight generalization of known results. Here, we also derive some new conditions for sequences, obtained by uniform decimation, to reach their maximum linear complexity.

The period of the output sequence generated by an arbitrary clock-controlled LFSR with an irreducible feedback polynomial and an arbitrary structure of the control sequence is estimated in Section 3. A sufficient condition for this period to reach its maximal value is formulated. Results from Section 2 are used to define some specific configurations of clock-controlled arrangements with a maximal period of the output sequence. The special case when the degree m of $f(x)$ is a prime number is studied in detail. Relevant recommendations for estimating the linear complexity are also presented. Sections 2 and 3 extend the results earlier published in [21].

In Section 4, we discuss randomness properties of clock-controlled LFSR output sequences. The deviation of the number of occurrences of elements in a full period of u from the "ideal" value is estimated when $\gcd(S, M) = 1$. Also we estimate the autocorrelation function of the output sequence for the special case that the GR is an m-LFSR and $\gcd(S, \lambda) = 1$.

In Section 5 we construct a key-stream generator based on the one suggested by Geffe in [5]. Unlike the Geffe generator that has three binary input

m-sequences, our generator runs over the field $P = \mathrm{GF}(q)$ and combines multiple inputs having arbitrary periods. In particular, this implies that clock-controlled shift registers can be used as inputs. The original Geffe generator can not be used for key-stream generation since its combining function is zero-order correlation immune and correlation attacks are applied easily. Using clock-controlled registers and multiple inputs makes this generator immune against fast correlation attacks and less susceptible to basic attacks. We analyze some relevant algebraic properties of the suggested generator.

Clock-controlled registers and their memoryless combiners are susceptible to certain types of correlation attacks, of which the complexity depends on the parameters chosen for the control register and the generating register, and on the correlation characteristics of the combining function. Section 6 contains a survey of correlation attacks published so far and provides relevant recommendations for selecting secure parameters of clock-controlled arrangements. Still, one can notice a general lack of empirical data on the practical efficiency of these attacks. Furthermore, these attacks can be defeated by adding a uniform noise to the key-stream.

2 Decimation of Linear Recurring Sequences

Following are some results about sequences obtained by uniform decimation of linear recurring sequences with irreducible characteristic polynomial. These results will be used further to estimate the period of a sequence generated by a clock-controlled LFSR.

Definition 1. *Let l and k be arbitrary nonnegative integers and $k > 0$. Then sequence $v = \{v(i)\}_{i\geq 0}$ defined by $v(i) = u(l + ki)$ for $i \geq 0$ is called the uniform (l, k)-decimation of sequence $u = \{u(i)\}_{i\geq 0}$. Also we will say that v is obtained by uniform (l, k)-decimation of u.*

Let $f(x)$ be an irreducible polynomial of degree $m > 0$ and order M over $P = \mathrm{GF}(q)$. Further, taking into account the fact that $Q = \mathrm{GF}(q^m)$ is the splitting field of $f(x)$, let α be a root of $f(x)$ in an extension field $Q = \mathrm{GF}(q^m)$ of P. Let $m(k)$ denote the degree of $R_k = P(\alpha^k)$ over P. Let also $f_k(x)$ denote the minimal polynomial of α^k over P. Note that $f_k(x)$ is irreducible in $P[x]$. Then directly from the definition of extension degree it follows that $\deg f_k(x) = m(k)$ and evidently $m(k) \mid m = m(1)$.

We denote the set of all homogeneous linear recurring sequences in P with characteristic polynomial $f(x)$ by $L_P(f)$. If degree of $f(x)$ is m then $L_P(f)$ is an m-dimensional vector space over P. Item (a) of the following theorem is a particular case of [7, Proposition] and has also been partially proved in [25, pp. 144-147] and [23, pp. 285-287]. Item (b) generalizes [27, Lemma 17]. We shall present a proof of the theorem along novel lines.

Theorem 1. *Under the conditions imposed above, let l and k be arbitrary nonnegative integers and $k > 0$, then:*

(a) *The uniform (l,k)-decimation defines a homomorphism of the vector space $L_P(f)$ onto $L_P(f_k)$. This homomorphism is an isomorphism if and only if $m(k)=m$.*

(b) *If $f(x)$ is a primitive polynomial and if u is a nonzero sequence belonging to $L_P(f)$, then every nonzero sequence $w \in L_P(f_k)$ can be obtained as a uniform (l,k)-decimation of u using exactly $q^{m-m(k)}$ different values of $l \in \{0,\ldots,\lambda-1\}$, and the zero sequence can be obtained similarly using exactly $q^{m-m(k)}-1$ different values of $l \in \{0,\ldots,\lambda-1\}$.*

Proof.

(a) Let us use the representation of linear recurring sequences in finite fields in terms of trace function. By [22, p. 406, Theorem 8.24] if $f(x)$ is irreducible then for any $u \in L_P(f)$ there is a unique $\theta \in Q = \mathrm{GF}(q^m)$ such that $u(i) = \mathrm{Tr}_{Q/P}(\theta\alpha^i)$ $(i=0,1,2,\ldots)$. Since $\alpha^k \in R_k$, applying uniform (l,k)-decimation to u we get

$$\begin{aligned} v(i) = u(l+ki) &= \mathrm{Tr}_{Q/P}(\theta\alpha^l(\alpha^k)^i) = \mathrm{Tr}_{R_k/P}\left(\mathrm{Tr}_{Q/R_k}(\theta\alpha^l(\alpha^k)^i)\right) = \\ &= \mathrm{Tr}_{R_k/P}\left(\left(\mathrm{Tr}_{Q/R_k}(\theta\alpha^l)\right)(\alpha^k)^i\right) = \mathrm{Tr}_{R_k/P}(b_l(\alpha^k)^i) \quad (i=0,1,2,\ldots)\ , \end{aligned}$$

where $b_l = \mathrm{Tr}_{Q/R_k}(\theta\alpha^l) \in R_k$. Thus, $v \in L_P(f_k)$.
It is obvious that uniform (l,k)-decimation of a sum of sequences from $L_P(f)$ is a sum of corresponding uniform (l,k)-decimation sequences in $L_P(f_k)$. Thus, uniform decimation defines a homomorphism of $L_P(f)$ *in* $L_P(f_k)$.
Now we have to prove that this homomorphism is a surjective map. For any $w \in L_P(f_k)$ there exists a uniquely determined $\eta \in R_k$ such that $w(i) = \mathrm{Tr}_{R_k/P}(\eta(\alpha^k)^i)$ $(i=0,1,2,\ldots)$. Thus, w can be obtained by uniform (l,k)-decimation of a sequence from $L_P(f)$ if and only if $\eta = \mathrm{Tr}_{Q/R_k}(\theta\alpha^l)$ for some $\theta \in Q$. The number of such θ is equal to the number of solutions of the equation $\mathrm{Tr}_{Q/R_k}(x) = \eta$ in the field Q. This number is equal to $|\ker(\mathrm{Tr_{Q/R_k}})| = q^{m-m(k)} \geq 1$ since Tr_{Q/R_k} function is a nonzero linear mapping of the field Q to the field R_k.
The final statement of Item (a) follows from the fact that homomorphism of a finite-dimensional vector space *onto* another vector space is an isomorphism if and only if their dimensions are equal.

(b) Let us fix an arbitrary positive integer k. For any $w \in L_P(f_k)$ there exists a uniquely determined $\eta \in R_k$ such that $w(i) = \mathrm{Tr}_{R_k/P}(\eta(\alpha^k)^i)$ $(i = 0,1,2,\ldots)$. From the the proof of Item (a) is follows that $w = v$ if and only if $\eta = b_l = \mathrm{Tr}_{Q/R_k}(\theta\alpha^l)$. Sequence u is nonzero thus $\theta \neq 0$.
Since $f(x)$ is a primitive polynomial, α has order $\lambda = q^m - 1$. It follows that the set of elements $\{\theta\alpha^l \mid l \in 0,\ldots,\lambda-1\}$ is equal to Q^* that is a multiplicative group of the field Q. Tr_{Q/R_k} function is a linear map of the field Q to the field R_k. The number of $l \in 0,\ldots,\lambda-1$ such that $\eta = b_l$ is equal to the number of *nonzero* solutions of the equation $\mathrm{Tr}_{Q/R_k}(x) = \eta$ in the field Q. The total number of solutions is equal to $|\ker(\mathrm{Tr_{Q/R_k}})| = q^{m-m(k)}$. If $\eta \neq 0$, all solutions of the equation $\mathrm{Tr}_{Q/R_k}(x) = \eta$ are nonzero and the

number we are looking for is equal to $q^{m-m(k)}$. If $\eta = 0$ then $x = 0$ is also a solution and the number we are looking for is equal to $q^{m-m(k)} - 1$. $\square$

Polynomial $f_k(x)$ is the minimal polynomial of α^k, so it is irreducible. Since the order of α^k (that is equal to the order of $f_k(x)$) is given by $\frac{\operatorname{ord}\alpha}{\gcd(k, \operatorname{ord}\alpha)} = \frac{M}{\gcd(k,M)}$, we conclude that $f_k(x)$ has order M if and only if k is relatively prime to M. Further, if $\gcd(k, M) = 1$ then $f_k(x)$ has degree m. Indeed, the degree of $f_k(x)$ is equal to the least value of t, $t > 0$, for which $(\alpha^k)^{q^t} = \alpha^k$ or equivalently $\alpha^{k(q^t-1)} = 1$. But $\operatorname{ord}\alpha = M$ and $\gcd(k, M) = 1$. It follows that $M \mid q^t - 1$ and thus that $t = m$.

Corollary 1. *Let* $\gcd(k, M) = 1$. *Then every uniform* (l, k)*-decimation sequence of any nonzero sequence* $u \in L_P(f)$ *is equal to a nonzero sequence belonging to* $L_P(f_k)$ *and none nonzero sequence* $w \in L_P(f_k)$ *can be obtained as a uniform* (l, k)*-decimation of* u *using more then one value of* $l \in \{0, \ldots, M-1\}$.

Proof. When applying the uniform decimation with parameters $l \geq 0$ and $k > 0$ to sequences in $L_P(f)$ we can assume that $l < M$ since all these sequences have the multiple period M. Moreover, if we fix some arbitrary value of $0 \leq \tilde{l} < M$, then for any $l > 0$, the uniform (l, k)-decimation of any nonzero sequence from $L_P(f)$ is equal to the uniform $(\tilde{l}, k)$-decimation of some other nonzero sequence from $L_P(f)$. Thus, for any fixed value of $\tilde{l}$, $0 \leq \tilde{l} < M$, the set containing uniform (l, k)-decimation sequences of any nonzero sequence $u \in L_P(f)$, when $k > 0$ is fixed and l takes all possible nonnegative values, is equal to the set containing uniform $(\tilde{l}, k)$-decimation sequences of some M-cardinal subset of nonzero sequences in $L_P(f)$. Now since $m = m(k)$, the statement easily follows from Item (a) of Theorem 1. $\square$

Corollary 2. *If the degree* m *of polynomial* $f(x)$ *is a prime number then* $m(k) = m$ *if and only if* k *is not a multiple of* $\frac{M}{\gcd(M,q-1)}$. *Moreover, if* $\frac{M}{\gcd(M,q-1)} \nmid k$, *then every uniform* (l, k)*-decimation sequence of any nonzero sequence* $u \in L_P(f)$ *is equal to a nonzero sequence belonging to* $L_P(f_k)$ *and none nonzero sequence* $w \in L_P(f_k)$ *can be obtained as a uniform* (l, k)*-decimation of* u *using more then one value of* $l \in \{0, \ldots, M-1\}$.

Proof. Since $m(k) \mid m$ and m is prime, only two alternatives are possible: either $m(k) = m$ or $m(k) = 1$, in which case $(\alpha^k)^q = \alpha^k$. So, $m(k) = 1$ if and only if M divides $k(q-1)$, i.e.

$$\left.\frac{M}{\gcd(M, q-1)}\,\right|\, k \ .$$

The rest of the proof goes the same way as in Corollary 1. $\square$

Corollary 3. *If* $f(x)$ *is a primitive polynomial and* $k \leq q^{m/2}$ *then* $\deg f_k(x) = m$. *Moreover, under these conditions, every uniform* (l, k)*-decimation sequence of any nonzero sequence* $u \in L_P(f)$ *is equal to a nonzero sequence belonging to* $L_P(f_k)$ *and every nonzero sequence* $w \in L_P(f_k)$ *can be obtained as a uniform* (l, k)*-decimation of* u *using a unique value of* $l \in \{0, \ldots, \lambda - 1\}$.

Proof. By virtue of Theorem 1, Item (a), all uniform (l, k)-decimation sequences of u belong to $L_P(f_k)$ and we have to prove that $m(k) = m$.

By definition, $\operatorname{ord} \alpha^k = \frac{\lambda}{\gcd(k,\lambda)} \mid (q^{m(k)} - 1)$ and $m(k) \mid m$, as was noted before. Hence, if $m(k) < m$ then $m(k) \leq \frac{m}{2}$ and therefore $\frac{\lambda}{\gcd(k,\lambda)} \leq q^{m/2} - 1$, i.e. $\gcd(k, \lambda) \geq q^{m/2}+1$. In particular, $k \geq q^{m/2}+1$ that contradicts the condition imposed.

Therefore, $m(k) = m$ and by Theorem 1, Item (b), the zero sequence can be obtained as a uniform (l, k)-decimation of u using exactly $q^{m-m(k)} - 1 = 0$ different values of $l \in \{0, \ldots, \lambda - 1\}$. So, all uniform (l, k)-decimation sequences of u are nonzero. Every nonzero linear recurring sequence $w \in L_P(f_k)$ can be obtained as a uniform (l, k)-decimation of u using exactly $q^{m-m(k)} = 1$ value of $l \in \{0, \ldots, \lambda - 1\}$. □

3 Period and Linear Complexity of Clock-Controlled LFSR

In this section, we continue to use the terminology and notations introduced in Section 1. As a generalization of Definition 1 of a uniform decimation, we can consider the output sequence u, obtained from (1) as a *nonuniform* decimation of b according to the control sequence a as follows:

$$u(i + j\pi) = b(\sigma(i) + jS) \quad \text{for} \quad 0 \leq i < \pi,\ j \geq 0\ , \tag{2}$$

where $S = \sum_{k=0}^{\pi-1} a_k$ and $\sigma(i) = \sum_{k=0}^{i} a_k$. Hence, any uniform (i, π)-decimation of u is a uniform $(\sigma(i), S)$-decimation of b. By Theorem 1, Item (a), the latter decimation belongs to $L_P(f_S(x))$. The output sequence u consists of π such sequences interleaved and belongs to $L_P(f_S(x^\pi))$.

Since the period of the sequence b divides the order M of $f(x)$, we conclude that all elements of a can be reduced modulo M without any effect on the output sequence u. So, from now on we assume without loss of generality that all elements of a being nonnegative integers less than M.

It is obvious that the minimum of the degrees of irreducible factors of $f_S(x^\pi)$ provides a lower bound for the linear complexity of the output sequence u and the lowest possible order of any irreducible factor of $f_S(x^\pi)$ gives a lower bound for the period of u.

In [16] for $P = \mathrm{GF}(2)$ and *primitive* GR feedback it was shown that maximum linear complexity πm of the output sequence u can be obtained only if the multiplicative order of 2 modulo $\frac{\lambda}{\gcd(S,\lambda)}$ is equal to m. Furthermore, when the control sequence a and initial state vector of the GR are chosen at random and uniformly, a lower bound on the probability that the output sequence has maximum linear complexity is established. By appropriate choice of π and m this bound can be made arbitrary close to 1 with πm arbitrarily large, provided that $\pi \leq 2^m$.

From equation (2) it easily follows that the period of u divides $\frac{\pi M}{\gcd(S,M)}$, since $\operatorname{ord} f_S(x) = \operatorname{ord} \alpha^S = \frac{M}{\gcd(S,M)}$ and u consists of π interleaved sequences belonging to $L_P(f_S(x))$. From [10, Lemma 1] it follows that if u is nonzero then its period is a multiple of $\frac{\pi' M}{\gcd(S,M)}$ where π' is the product of all prime factors of π, not necessarily distinct, which are also factors of $\frac{M}{\gcd(S,M)}$. This provides the lower bound for the period. In particular, if every prime factor of π also divides $\frac{M}{\gcd(S,M)}$, then the period of u reaches the maximal value $\frac{\pi M}{\gcd(S,M)}$. We also note that zero output sequences can be generated even if the initial state of the GR is nonzero and $f(x)$ is primitive. This will be illustrated in Example 2.

By Corollary 1, if S is relatively prime to M then $f_S(x)$ is irreducible of degree m and order M. For $P = \mathrm{GF}(2)$ and such an $f_S(x)$, Theorem 2 in [2] provides an exact lower bound for the degree of any irreducible factor of $f_S(x^\pi)$. From this theorem it easily follows that if $f(x)$ is primitive, if $\gcd(S, \lambda) = 1$, and if every prime factor of π also divides λ, then $f_S(x^\pi)$ is irreducible. In this case the linear complexity of u reaches its maximal possible value: πm (this is equal to the degree of $f_S(x^\pi)$).

In many cases the period of sequence u can be determined more precisely. The following theorem, that was earlier published in [21], extends [17, Theorem 4]. Recently, in [10, Theorem 2] Golić generalized this result for an arbitrary GR having an LFSR structure. We provide the proof here for its simplicity and universality of some tricks used.

Theorem 2. *The output sequence u is periodic. If for $l \in \{0, \dots, M-1\}$ the uniform (l, S)-decimation sequences of b are all distinct, then the period of u is equal to*

$$\tau(\pi, M, S) = \frac{\pi M}{\gcd(S, M)} \ .$$

Proof. Put $\tau = \frac{\pi M}{\gcd(S,M)}$. We shall first prove that τ is a multiple period of u.

As was noted before, the output sequence u is a homogeneous linear recurring sequence with characteristic polynomial $f_S(x^\pi)$ and consists of π interleaved sequences belonging to $L_P(f_S(x))$, where $f_S(x)$ is the minimal polynomial of element α^S over P. Thus, the period of any such nonzero uniform S-decimation is equal to $\frac{M}{\gcd(S,M)}$ that is the multiplicative order of element α^S in P^*. Hence, the sequence u is periodic and $\tau(\pi, M, S) \mid \pi \frac{M}{\gcd(S,M)} = \tau$.

Let us consider two uniform π-decimation sequences of the output u, the first one starting from $u(0)$ and the second from $u(\tau(\pi, M, S))$. These decimation sequences are equal since $\tau(\pi, M, S)$ is the period of u. On the other hand, according to (2) the same sequences are uniform (k_0, S) and (t_0, S)-decimation sequences of b for some $k_0 = a_0 \geq 0$ and $t_0 \geq k_0$. Then, according to the hypothesis of the theorem, $k_0 \equiv t_0 \pmod{M}$.

Let us also consider two uniform π-decimation sequences of u where the first one starts from $u(1)$ and the second from $u(\tau(\pi, M, S)+1)$. These decimation sequences are equal and they are uniform (k_1, S) and (t_1, S)-decimation sequences of b for some $k_1 \geq k_0$ and $t_1 \geq t_0$. Thus, $k_1 \equiv t_1 \pmod{M}$.

Finally, consider pairs of uniform π-decimation sequences that start from $u(2)$ and $u(\tau(\pi, M, S)+2)$, from $u(3)$ and $u(\tau(\pi, M, S)+3)$ and so on. Corresponding values of k_i and t_i satisfy the equivalence

$$k_i \equiv t_i \pmod{M} \quad (i = 0, 1, 2, \ldots) \ , \tag{3}$$

where $k_{i+1} \geq k_i$ and $t_{i+1} \geq t_i$.

From (1), we have $k_{i+1} - k_i = a_{i+1}$ and $t_{i+1} - t_i = a_{\tau(\pi,M,S)+i+1}$. It follows from the the congruence relations in (3) and from the assumption that $0 \leq a_i < M$, that $k_{i+1} - k_i = t_{i+1} - t_i$ and thus that $a_{i+1} = a_{\tau(\pi,M,S)+i+1}$ $(i = 0, 1, 2, \ldots)$. This shows that

$$\pi \mid \tau(\pi, M, S) \ . \tag{4}$$

It is clear that $t_i - k_i$ $(i = 0, 1, 2, \ldots)$ is equal to the number of regular steps (with no clock control) the GR is making each time when the whole automaton generates $\tau(\pi, M, S)$ output elements. By virtue of (4), $t_i - k_i = \frac{\tau(\pi,M,S)}{\pi} S$ since if the CR makes a full period then the GR makes S steps. Thus, according to (3), $M \mid \frac{\tau(\pi,M,S)}{\pi} S$, from which it directly follows that

$$\frac{M}{\gcd(S, M)} \;\Big|\; \frac{\tau(\pi, M, S)}{\pi} \quad \text{and} \quad \tau \mid \tau(\pi, M, S) \ .$$

This proves the theorem. □

Let assume that b is a nonzero sequence. Then, according to Theorem 1, Item (a), all the uniform (l, S)-decimation sequences of b for $l \in \{0, \ldots, M - 1\}$ are distinct if $m(k) = m$ (see [10, Proposition 2], where a similar fact was proved for an arbitrary GR having LFSR structure).

Proposition 1. *Let $f(x)$ be a primitive polynomial of degree m, so it has the maximal possible order $\lambda = q^m - 1$. Then all uniform (l, S)-decimation sequences of b are distinct for $l \in \{0, \ldots, \lambda - 1\}$ if and only if for any $l \in \{0, \ldots, \lambda - 1\}$ the uniform $(l, \gcd(S, \lambda))$-decimation of b is nonzero.*

Proof. Let us first consider the congruence $xS \equiv y \gcd(S, \lambda) \pmod{\lambda}$ where $x \geq 0$ and $y \geq 0$. It is evident that for any fixed value of $x = 0, 1, 2, \ldots$ this congruence is solvable with respect to y and for any fixed value of $y = 0, 1, 2, \ldots$ it is solvable with respect to x. Thus, for any $l \geq 0$ a uniform (l, S)-decimation of b contains exactly the same elements as a uniform $(l, \gcd(S, \lambda))$-decimation.

Suppose now that for some $k, t \in \{0, \ldots, \lambda - 1\}$ with $k \neq t$, the uniform (k, S) and (t, S)-decimation sequences of b are equal. By Theorem 1, Item (b), they can be equal if and only if $q^{m-m(S)} \geq 2$ and this is so if and only if for some $l \in \{0, \ldots, \lambda - 1\}$ the uniform (l, S)-decimation of b is zero. But then the uniform $(l, \gcd(S, \lambda))$-decimation is zero too. □

Corollary 4. *Let b be a nonzero sequence and suppose that one of the following two conditions holds*

(a) degree m of $f(x)$ is prime and S is not a multiple of $\frac{M}{\gcd(M,q-1)}$,
(b) $f(x)$ is a primitive polynomial (so, of order $\lambda = q^m - 1$) and $\gcd(S, \lambda) \leq q^{m/2}$.

Then the period of u is equal to $\tau(\pi, M, S) = \frac{\pi M}{\gcd(S,M)}$.

Proof. If condition (a) holds, we can apply Corollary 2 and if condition (b) holds, we can apply Corollary 3. In both cases, Proposition 1 shows that for $l \in \{0, \dots, M-1\}$ all uniform (l, S)-decimation sequences of b are distinct. The proof is finished by applying Theorem 2. $\square$

Note that if $f(x)$ is primitive one has $M = \lambda = q^m - 1$. Some other sufficient conditions to apply Theorem 2 can be found in [10, Proposition 4].

Note 1. Let us consider the case when m, the degree of $f(x)$, is a prime number and $\frac{M}{\gcd(M,q-1)} \mid S$. Then $\frac{M}{\gcd(M,S)} \mid q-1$ and hence, $\tau(\pi, M, S) \mid \pi(q-1)$ since $\tau(\pi, M, S) \mid \pi \frac{M}{\gcd(M,S)}$.

By Corollary 2, $m(\gcd(S, M)) = m(S) = 1$ (since $\operatorname{ord} \alpha^{\gcd(S,M)} = \operatorname{ord} \alpha^S$) and $f_S(x) = x - \alpha^S$. Let p denote the element α^S in P. Thus, the output sequence u is a homogeneous linear recurring sequence with characteristic polynomial $f_S(x^\pi) = x^\pi - p$ and consists of π interleaved sequences having the form of a geometric progression with ratio p and initial element $u(i) = b(\sigma(i))$ ($i = 0, \dots, \pi - 1$). We can get the $\frac{\pi M}{\gcd(M,S)}$-long period of u by taking the elements of the following array in a row-by-row order.

$$\begin{array}{ccc} u(0) & \dots\dots & u(\pi-1) \\ u(0)p & \dots\dots & u(\pi-1)p \\ \vdots & & \vdots \\ u(0)p^j & \dots\dots & u(\pi-1)p^j \\ \vdots & & \vdots \\ u(0)p^{\xi-1} & \dots\dots & u(\pi-1)p^{\xi-1} \end{array}, \tag{5}$$

where $\xi = \frac{M}{\gcd(M,S)}$. If $b(\sigma(i)) = 0$ for all $i \in \{0, \dots, \pi - 1\}$, then u is a zero sequence. Further we assume that $b(\sigma(i)) \neq 0$ for some i.

If $\pi \mid \tau(\pi, M, S)$ then $\tau(\pi, M, S) = \pi j$ where j is the smallest integer in $\{1, \dots, \frac{M}{\gcd(M,S)}\}$ with the property that $b(\sigma(i)) = \alpha^{Sj} b(\sigma(i))$ for all $i \in \{0, \dots \pi - 1\}$. Since not all of $b(\sigma(i))$ are zero, the smallest j with this property is in fact equal to $\frac{M}{\gcd(M,S)}$. Thus, $\tau(\pi, M, S) = \frac{\pi M}{\gcd(M,S)}$.

Suppose now that $\tau(\pi, M, S)$ is not a multiple of π. Since u is periodic and its period has the pattern of (5), there exist some $j \in \{0, \dots, \frac{M}{\gcd(M,S)} - 1\}$ and $i \in \{1, \dots, \pi - 1\}$ such that

$$\begin{pmatrix} 1 & 0 & \dots & 0 & -p^j & \dots & 0 \\ & \ddots & \ddots & & \ddots & \ddots & \\ 0 & & & & & 0 & -p^j \\ -p^{j+1} & 0 & & & & & 0 \\ 0 & \ddots & \ddots & & & \ddots & \vdots \\ \vdots & & \ddots & \ddots & & \ddots & 0 \\ 0 & \dots & 0 & -p^{j+1} & 0 & & 1 \end{pmatrix} \begin{pmatrix} u(0) \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ u(\pi-1) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix}, \tag{6}$$

where the ones are on the diagonal, the $-p^j$ entry in the first row is in column $i+1$ and the $-p^{j+1}$ entry in the first column is in row $(\pi-i)+1$. Let $D(\pi,-p^j,-p^{j+1},\pi-i)$ denote the determinant of this $\pi\times\pi$ matrix, which $\pi-i$ entries are equal to $-p^j$. It is not difficult to see that

$$D(\pi,-p^j,-p^{j+1},\pi-i)=\begin{cases} D(i,-p^{2j+1},-p^{j+1},\pi-i), & \text{if} \quad i>\pi/2,\\ D(\pi-i,-p^j,-p^{2j+1},\pi-2i), & \text{if} \quad i<\pi/2,\\ (1-p^{2j+1})^{\pi/2}, & \text{if} \quad i=\pi/2, \end{cases}.$$

We can apply this rule repeatedly to prove that $D(\pi,-p^j,-p^{j+1},\pi-i)=(1\pm p^{kj+t(j+1)})^l$ for some $k,t,l>0$ such that $(k+t)l=\pi$. Thus, if $D(\pi,-p^j,-p^{j+1},\pi-i)=0$ then $p^{kj+t(j+1)}=\pm1$ and so $\frac{M}{\gcd(S,M)}\mid 2(kj+t(j+1))$.

If integers $j\in\{0,\ldots,\frac{M}{\gcd(M,S)}-1\}$ and $i\in\{1,\ldots,\pi-1\}$ exist such that $D(\pi,-p^j,-p^{j+1},\pi-i)=0$ then (6) has nonzero solutions. If, in this case, one can find a control sequence with parameters π and S and an initial state vector for the GR such that $(b(\sigma(0)),\ldots,b(\sigma(\pi-1)))$ is a nonzero solution of (6) then the multiple period of u is equal to $\pi j+i$. This number is less than $\frac{\pi M}{\gcd(M,S)}$.

Note 2. If S is relatively prime to M, it follows from Corollary 1 and Theorem 2 that the period of u reaches the maximal value πM (this is Theorem 4 in [17]).

If conditions of Theorem 2, Proposition 1 and Corollary 4 do not hold then the period of the decimated sequence may be equal to or smaller than $\frac{\pi M}{\gcd(S,M)}$. This can be seen in the following examples.

Example 1. Let $f(x)=x^4+x+1$ (a primitive polynomial over $P=\mathrm{GF}(2)$) and $a=(2,3)^\infty=\{2,3,2,3,\ldots\}$ be the control sequence with period $\pi=2$. If we set the initial state vector of the GR equal to $(1,1,1,1)$ then $b=(1,1,1,1,0,0,0,1,0,0,1,1,0,1,0)^\infty$ which has period 15. The output sequence u for this clock-controlled arrangement is equal to $(1,0,1)^\infty$ with period 3.

In our case $S=5$ and $\gcd(S,\lambda)=\gcd(5,15)=5$ and this exceeds $q^{m/2}=4$. Thus, the condition (b) of Corollary 4 does not hold. Otherwise, the period would be equal to 6. Condition (a) of Corollary 4 is not applicable too, since $m=4$ is not prime (although S is not a multiple of $\frac{\lambda}{q-1}=15$). Proposition 1 can not be used either, since the uniform $(4,5)$-decimation sequence of b is zero. The uniform $(0,5)$-decimation sequence and $(1,5)$-decimation sequence of b are equal, so Theorem 2 is not applicable too.

On the other hand if the control sequence is equal to $(3,2)^\infty$ with the same value of $S=5$ then $u=(1,0,0,1,1,1)^\infty$. In this case the period is maximal although conditions of Theorem 2, Proposition 1 and Corollary 4 do not hold.

Finally, if we take the control sequence equal to $(1,2)^\infty$ then $\gcd(S,\lambda)=\gcd(3,15)=3$ and the condition (b) of Corollary 4 holds. In this case, the output sequence is $(1,1,0,0,1,0,1,0,1,1)^\infty$. So, the period of u is 10 and that is equal to $\frac{\pi\lambda}{\gcd(S,\lambda)}$.

Example 2. Let $P=\mathrm{GF}(3)$ and $f(x)=x^3+2x+1$, so $f(x)$ is a primitive polynomial over P. Let $a=(2,5,6)^\infty$ with period $\pi=3$ be the control sequence. If we set the initial state vector of the GR equal to $(2, 0, 1)$ then $b = (2, 0, 1, 1, 1, 0, 0, 2, 0, 2, 1, 2, 2, 1, 0, 2, 2, 2, 0, 0, 1, 0, 1, 2, 1, 1)^\infty$. The output sequence u for this clock-controlled arrangement is equal to $(1, 2)^\infty$ with period 2. But if the initial state vector of the GR is equal to $(0, 1, 1)$ and the control sequence is equal to $(4, 1, 2, 6)^\infty$ then the output sequence is zero. In both cases $S = 13$ and S is equal to $\frac{\lambda}{q-1}$. Thus, the condition (a) of Corollary 4 does not hold. Indeed, if that condition would hold, the period would be equal to 6 for the first case and 8 for the second.

On the other hand if the initial state vector of the GR is set to $(2, 0, 1)$ and the control sequence is equal to $(7, 6)^\infty$ with the same value of $S = 13$ then $u = (2, 1, 1, 2)^\infty$. In this case the period is maximal although condition of Corollary 4, Item (a), does not hold.

If CR-outputs a_i take only bit values 0 and 1 then the arrangement is called a *stop-and-go* generator and is described in [1]. In our notation, S for this type of generator is equal to the number of ones in the full period of a. In particular, if the CR is an m-LFSR over GF(2) with a primitive feedback polynomial of degree n and order $\pi = 2^n - 1$, then CR-outputs take the value one 2^{n-1} times over the period and $S = 2^{n-1}$. Thus, if $q = 2$ and $f(x)$ is primitive then $\gcd(S, \lambda) = \gcd(2^{n-1}, 2^m - 1) = 1$ and by Corollary 4 $\tau(\pi, \lambda, S) = \pi\lambda$. For the particular case when $n = m$, we get that $\pi = \lambda$ and by [2, Theorem 2] the polynomial $f_S(x^\pi)$ is irreducible. In this case the linear complexity of the output sequence has its greatest possible value $n(2^n - 1)$ equal to the degree of $f_S(x^\pi)$. Due to these features of the output sequence, it is reasonable to use it further for clock controlling the third m-LFSR. It turns out to be possible to extend this system further to an arbitrary number of LFSR's. Such an arrangement is called an *m-sequence cascade* and has been considered in [17]. Many other types of cascades were suggested in the literature (see [17] for the review) but they are not the subject of the present paper.

4 Randomness Properties of Clock-Controlled LFSR

The discussion presented in Section 3 leads to the conclusion that the control sequence a plays only a secondary role when the period and linear complexity of clock-controlled LFSR's are concerned. By that we mean that using different clock sequences one can generate different output sequences having the same period and linear complexity. However, the clocking procedure has a major influence on randomness properties of the output sequence. It is obvious that if the GR generates a nonzero sequence, then by selecting an appropriate control sequence one can get any periodic sequence in GF(q) as output sequence. Thus, when choosing a control sequence one should pay attention not only to the period and linear complexity of output but also should take randomness properties into account. Hereafter we continue to use the terminology and notations introduced in Sections 1 and 3.

As was noted above, the output sequence u consists of π interleaved sequences, all members of $L_P(f_S(x))$. If S is relatively prime to M then by virtue of Corollary 1, $f_S(x)$ is also irreducible of degree m and order M. If h is the least common multiple of M and $q-1$ then according to [22, p. 450],

$$\left|Z(0) - \frac{(q^{m-1}-1)M}{q^m-1}\right| \le \left(1-\frac{1}{q}\right)\left(\frac{M}{h} - \frac{M}{q^m-1}\right) q^{m/2}$$
$$\left|Z(b) - \frac{q^{m-1}M}{q^m-1}\right| \le \left(\frac{M}{h} - \frac{M}{q^m-1} + \frac{h-M}{h} q^{1/2}\right) q^{(m/2)-1} \quad \text{for} \quad b \neq 0 \ ,$$

where $Z(b)$ is the number of occurrences of element $b \in P$ in the M-long period of a linear recurring sequence belonging to $L_P(f_S(x))$. Now if we multiply the right hand parts of both inequalities by π we can estimate the deviation between the actual number of occurrences of elements $b \in P$ in the πM-long period of u (see Note 2) and the ideal value. If $h \approx M$ and M is sufficiently large then this deviation is comparatively small.

In particular, if $f(x)$ is primitive and $\gcd(S, \lambda) = 1$ then polynomial $f_S(x)$ is also primitive. Thus, any sequence belonging to $L_P(f_S(x))$ is an m-sequence. So, any nonzero element of P appears q^{m-1} times in its λ-long period and 0 appears $q^{m-1}-1$ times. As a consequence, any nonzero element of P appears πq^{m-1} times in the $\pi\lambda$-long period of the output sequence u and 0 appears $\pi(q^{m-1}-1)$ times (note that by Corollary 4 the period of u is equal to $\pi\lambda$).

If CR-outputs a_i take only the values 1 or 2 and $P = \mathrm{GF}(2)$, then all l-tuples of length $l \le (m+1)/2$ appear in the output sequence with the same frequency as in the original m-sequence b (as pointed out in [26, p. 103]).

Let us further estimate the autocorrelation function of the output sequence of the clock-controlled LFSR. The autocorrelation function provides an important randomness test, since it measures the degree of dependence between a sequence and its various phase shifts. A requirement concerning the autocorrelation is included in Golomb's randomness postulates for pseudo random sequences [18, p. 25]. It thus can be adopted as a quality measure for pseudo random sequences.

According to [23, p. 463], if $s = \{s_i\}_{i\ge 0}$ is a sequence in $\mathrm{GF}(q)$ of period r and χ is a nontrivial additive character of $\mathrm{GF}(q)$, then the corresponding *autocorrelation function* of s is defined by

$$C(h) = \sum_{i=0}^{r-1} \chi(s_i)\overline{\chi}(s_{i+h}) \quad \text{for} \quad h = 0, 1, \ldots, r-1 \ ,$$

where $\overline{\chi}$ denotes the conjugate character. Golomb's randomness postulate for the autocorrelation function of s requires it to be two-valued:

$$C(h) = \begin{cases} r, & \text{for} \quad h = 0, \\ K, & \text{for} \quad 0 < h < r \end{cases} . \tag{7}$$

Let us assume that $f(x)$ is primitive and $\gcd(S, \lambda) = 1$. Then the autocorrelation function of $u(t)$ (with period $\tau = \pi\lambda$) can be expressed as follows.

$$C(h) = \sum_{i=0}^{\tau-1} \chi(u(i))\overline{\chi}(u(i+h)) = \sum_{i=0}^{\pi-1}\sum_{j=0}^{\lambda-1} \chi(u(i+j\pi))\overline{\chi}(u(i+j\pi+h)) \stackrel{(2)}{=}$$

$$\overset{(2)}{=} \sum_{i=0}^{\pi-1}\sum_{j=0}^{\lambda-1} \chi(b(jS+\sigma(i)))\overline{\chi}(b(jS+\sigma(i+h)) =$$

$$= \sum_{i=0}^{\pi-1} A(\sigma(i+h)-\sigma(i)) = \begin{cases} \sum_{i=0}^{\pi-1} A\left(\sum_{k=i+1}^{i+h} a_k\right), & \text{for} \quad h \neq 0, \\ \pi A(0), & \text{for} \quad h = 0 \end{cases} ,$$

where $A(h)$ is the autocorrelation function of an m-sequence h in $\mathrm{GF}(q)$ of period $\lambda = q^m - 1$. The following proposition is due to Zierler [27, p. 45].

Proposition 2. *If h is not a multiple of $t = \lambda/(q-1)$ then*

$$A(h) = q^{m-2} \sum_{a,b \in \mathrm{GF}(q)} \chi(a)\overline{\chi}(b) - 1 \ .$$

Further, there exists a primitive element ξ of $\mathrm{GF}(q)$ such that for $j = 0, 1, 2, \ldots$

$$A(jt) = q^{m-1} \sum_{a \in \mathrm{GF}(q)} \chi(a)\overline{\chi}(\xi^j a) - 1 \ .$$

Example 3. Let $q = p$ be a prime. The canonical additive character of $\mathrm{GF}(p)$ is of the form $\chi(a) = e^{2\pi i a/p}, \ a \in \mathrm{GF}(p)$. Now

$$\sum_{a,b \in \mathrm{GF}(p)} \chi(a)\overline{\chi}(b) = \sum_{j,k=0}^{p-1} e^{2\pi i j/p} e^{-2\pi i k/p} = \sum_{j=0}^{p-1} e^{2\pi i j/p} \sum_{k=0}^{p-1} e^{-2\pi i k/p} = 0 \ .$$

So that if h is not a multiple of t then by Proposition 2 $A(h) = -1$. If h is a multiple of t and $h = jt$, let $\mu = \xi^j$ then

$$\sum_{a \in \mathrm{GF}(q)} \chi(a)\overline{\chi}(\mu a) = \sum_{k=0}^{p-1} e^{2\pi i k/p} e^{-2\pi i \mu k/p} = \sum_{k=0}^{p-1} e^{2\pi i k(1-\mu)/p} = 0 \ ,$$

providing $\mu \neq 1$ (i.e. $h \not\equiv 0 \pmod{\lambda}$). Thus, $A(0) = \lambda$ while $A(h) = -1$ if h is not a multiple of λ.

We conclude from the above that if the generating register in a clock-controlled arrangement is an m-LFSR over $\mathrm{GF}(p)$ (where p is prime) and $\gcd(S, \lambda) = 1$, then the autocorrelation function $C(h)$ of $u(t)$ is equal to $-\pi$ for all the values of $h \neq 0$ for which $\sum_{k=i+1}^{i+h} a_k$ is not a multiple of λ for all $i = 0, 1, \ldots, \pi-1$. Thus, for such h the autocorrelation satisfies Golomb's postulate (7). The normalized autocorrelation is in this case equal to $-\lambda^{-1}$ and for large values of λ that is close to 0.

In particular, for the stop-and-go generator, when the control register is a binary m-LFSR of period $\pi = 2^n - 1$ and if $q = 2$ then

$$C(1) = \sum_{i=0}^{\pi-1} A(a_{i+1}) = 2^{n-1}A(1) + (2^{n-1}-1)A(0) =$$
$$= (2^{n-1}-1)(2^m-1) - 2^{n-1} \sim 2^{n+m-1} \ .$$

This fact reveals strong intersymbol dependency between the output sequence u and its 1-step phase shift. That is easily accounted for, since the previous key-stream symbol is copied to the next position every time when the control register generates 0. A dependency on the key-stream symbols of the preceding symbols constitutes a considerable weakness of a key-stream generator.

5 Generalized Geffe Generator

Combining linear feedback shift registers with a memoryless nonlinear function F is a well-known way to increase the period and the linear complexity of the key-stream, as well as to reduce the correlation between the key-stream sequence and the LFSR sequences that are used as input of F, see [25, 26]. The key-stream generator discussed in this section is a memoryless combiner based on a specific combining function that implements a nonuniform decimation of input sequences. The key-stream sequence is obtained by irregularly interleaving the decimated sequences. Both decimation and interleaving operations are controlled by the same sequence being one of combining function inputs. This construction can be seen as a generalization of the Geffe generator from [5].

First, we need to fix an arbitrary order for all the elements in the finite field $P = \mathrm{GF}(q)$. Further in this section, the elements of P will be enumerated as $p_0, \dots, p_{q-1}$. Let the combining function F from P^{q+1} to P be defined by $F(p_j, x_0, \dots, x_{q-1}) = x_j$ for $j = 0, \dots, q-1$. Thus, the first argument of F defines which of the remaining q arguments is chosen as an output of the function. Let us assume that a periodic sequence $a = \{a_i\}_{i \geq 0}$ in P (we will also call it the control sequence of F) with the period π and linear complexity $\hat{L}$ is fed to the first argument of F and that q periodic sequences $b^j = \{b_i^j\}_{i \geq 0}$ $(j = 0, \dots, q-1)$ in P with periods λ_j and linear complexity L_j respectively are fed to the remaining q arguments. Let $u = \{u_i\}_{i \geq 0}$ denote the output sequence generated by the function F.

It is clear that the output sequence u is an irregularly interleaved set of q nonuniform decimation sequences of b^j $(j = 0, \dots, q-1)$, when both the decimation and the interleaving operations are controlled by the sequence a. When $q = 2$, the nonuniform decimation is equivalent to the shrinking operation [4] controlled by $\{a_i\}_{i \geq 0}$ and $\{a_i \oplus 1\}_{i \geq 0}$, applied to sequences b^1 and b^0 respectively. The period and linear complexity of u are estimated further in this section.

Before we can continue, we need some preliminary lemmas. The first one is a special case of a fundamental result on the period of nonuniformly decimated sequences, as established in [19, Theorem 3].

Lemma 1. *Let $c = \{c_i\}_{i \geq 0}$ be a periodic sequence with the period T and let sequence $c' = \{c'_i\}_{i \geq 0}$ be a uniform d-decimation of c for some integer $d > 0$. Then c' is periodic and if T' denotes its period then*

(a) $T' \,\Big|\, \frac{T}{\gcd(T,d)}$ *;*
(b) If $\gcd(T, d) = 1$ *then* $T' = T$*.*

Let K denote the least common multiple of the periods of the sequences b^j $(j = 0, \ldots, q-1)$, so $K = \mathrm{lcm}(\lambda_0, \ldots, \lambda_{q-1})$ and let d denote $\gcd(\pi, K)$. It is obvious that K is equal to the period of the sequence of q-grams $B = \{(b_i^0, \ldots, b_i^{q-1})\}_{i\geq 0}$.

Lemma 2. *Suppose that sequence a contains all elements of P and that the q-gram sequence B with the period K contains a q-tuple that is equal to P in the sense of set equality. Suppose moreover that* $\gcd(\pi, K) = 1$. *Then $\tau = \pi K$.*

Proof. Under the hypothesis of the lemma, we can list a set of integers $t_j \geq 0$ $(j = 0, \ldots, q-1)$ such that $a_{t_j} = p_j$. Let us consider q uniform (t_j, π)-decimation sequences of the output u by taking $j = 0, \ldots, q-1$. Since π is the period of the control sequence a, the (t_j, π)-decimation of u is equal to the (t_j, π)-decimation of b^j. But hypothesis of the lemma claims that $\gcd(\pi, K) = 1$ whence it follows that $\gcd(\pi, \lambda_j) = 1$ for $j = 0, \ldots, q-1$. Hence by Lemma 1, Item (b), the period of the (t_j, π)-decimation of b^j is λ_j for $j = 0, \ldots, q-1$. But since these decimation sequences are decimation sequences of u as well, by Lemma 1, Item (a), $\lambda_j \mid \tau$ for $j = 0, \ldots, q-1$ and thus $K \mid \tau$.

Under the hypothesis of the lemma, there exists an integer $t \geq 0$ such that vector $(b_t^0, \ldots, b_t^{q-1})$ can be obtained by permutating the elements in $(p_0, \ldots, p_{q-1})$. Let us now consider the uniform (t, K)-decimation of the output sequence u. Since K is the period of the q-gram sequence B, this decimation is equal to the (t, K)-decimation of a which elements are substituted afterwards according to the rule defined by the permutation transforming $(p_0, \ldots, p_{q-1})$ into $(b_t^0, \ldots, b_t^{q-1})$. A one-to-one mapping applied to the elements of a sequence does not affect its period. Since $\gcd(\pi, K) = 1$, by Lemma 1, Item (b), the period of the (t, K)-decimation of a is π. But since this decimation is a decimation of u as well, by Lemma 1, Item (a), $\pi \mid \tau$.

Now since $K \mid \tau$, $\pi \mid \tau$ and $\gcd(\pi, K) = 1$ we can conclude that $\pi K \mid \tau$. On the other hand, it is obvious that $\tau \mid \pi K$ and thus $\tau = \pi K$. □

Theorem 3. *The sequence u is periodic. Let τ denote the period of u. Then $\tau \mid$* $\mathrm{lcm}(\pi, K)$. *Moreover, if sequence a is such that each of its uniform d-decimation sequences contains all the elements of P and the q-gram sequence B is such that all its uniform d-decimation sequences contain a q-tuple that is equal to P in the sense of set equality, then*

$$\frac{\pi K}{\gcd(\pi, K)^2} \,\Big|\, \tau \ .$$

Proof. It is obvious that in every $\mathrm{lcm}(\pi, K) = \mathrm{lcm}(\pi, \lambda_0, \ldots, \lambda_{q-1})$ steps all input sequences complete their full cycle. Since function F is memoryless, the output sequence u completes a full cycle as well in $\mathrm{lcm}(\pi, K)$ steps. Thus u is periodic and $\tau \mid \mathrm{lcm}(\pi, K)$.

Let us consider the q-gram sequence B. Since all sequences b^j $(j = 0, \ldots, q-1)$ are periodic with the period equal to λ_j respectively, it is obvious that the q-gram sequence B is periodic as well with the period equal to $\mathrm{lcm}(\lambda_0, \ldots, \lambda_{q-1}) = K$.

Now we fix an arbitrary $t \in \{0, \ldots, d-1\}$ and consider uniform (t,d)-decimation sequences of a, u and B. Let π_t, τ_t and K_t denote the respective periods of these decimation sequences. Then, by Lemma 1, Item (a),

$$\pi_t \;\left|\; \frac{\pi}{\gcd(\pi,d)} = \frac{\pi}{d}\right. , \quad \tau_t \mid \tau \quad \text{and} \quad K_t \;\left|\; \frac{K}{\gcd(K,d)} = \frac{K}{d}\right. . \tag{8}$$

Since $\gcd(\frac{\pi}{d}, \frac{K}{d}) = 1$, it follows that $\gcd(\pi_t, K_t) = 1$.

Let us now consider the memoryless combiner described above when uniform (t,d)-decimation sequences of the respective original sequences are fed into the arguments of F. Thus, the control sequence of F has period π_t and the q-gram sequence, feeding the rest of the arguments of F, has period K_t satisfying $\gcd(\pi_t, K_t) = 1$. We note that the output sequence of F has period τ_t since it is a uniform (t,d)-decimation of sequence u. So, the conditions of Lemma 2 are met and thus it follows that

$$\tau_t = \pi_t K_t \ , \tag{9}$$

for all $t \in \{0, \ldots, d-1\}$.

By (8), π_t divides $\frac{\pi}{d}$ for $t = 0, \ldots, d-1$ and therefore $\operatorname{lcm}(\pi_0, \ldots, \pi_{d-1}) \mid \frac{\pi}{d}$. Sequence a can be reconstructed by interleaving d sequences obtained by (t,d)-decimating of a for $t = 0, \ldots, d-1$ and thus $d \cdot \operatorname{lcm}(\pi_0, \ldots, \pi_{d-1})$ is a multiple period of a, that is $\pi \mid d \operatorname{lcm}(\pi_0, \ldots, \pi_{d-1})$. Hence $\operatorname{lcm}(\pi_0, \ldots, \pi_{d-1}) = \frac{\pi}{d}$. In the same way it is easy to show that $\operatorname{lcm}(K_0, \ldots, K_{d-1}) = \frac{K}{d}$.

From (8) it also follows that $\gcd(\pi_i, K_j) = 1$ $(i, j = 0, \ldots, d-1)$. Thus

$$\begin{aligned}
\operatorname{lcm}(\tau_0, \ldots, \tau_{d-1}) &\overset{(9)}{=} \operatorname{lcm}(\pi_0 K_0, \ldots, \pi_{d-1} K_{d-1}) = \\
&= \operatorname{lcm}(\operatorname{lcm}(\pi_0, K_0), \ldots, \operatorname{lcm}(\pi_{d-1}, K_{d-1})) = \\
&= \operatorname{lcm}(\pi_0, \ldots, \pi_{d-1}, K_0, \ldots, K_{d-1}) = \\
&= \operatorname{lcm}(\operatorname{lcm}(\pi_0, \ldots, \pi_{d-1}), \operatorname{lcm}(K_0, \ldots, K_{d-1})) = \\
&= \operatorname{lcm}(\pi_0, \ldots, \pi_{d-1}) \cdot \operatorname{lcm}(K_0, \ldots, K_{d-1}) = \frac{\pi K}{d^2} \ .
\end{aligned}$$

Also by (8), τ_t divides τ for $t = 0, \ldots, d-1$ and therefore $\operatorname{lcm}(\tau_0, \ldots, \tau_{d-1}) = \frac{\pi K}{d^2} \mid \tau$. □

The following lemma, that easily follows from [7, Proposition], will be needed to estimate the linear complexity of u.

Lemma 3. *Let $c = \{c_i\}_{i \geq 0}$ be a periodic sequence having linear complexity L and let $c' = \{c'_i\}_{i \geq 0}$ be a uniform d-decimation of c for some integer $d > 0$. Then there exists a polynomial $f_{(d)}(\cdot)$ annihilating c' as well as all d-decimation sequences of c, where the degree of $f_{(d)}(\cdot)$ is not greater then L.*

Proposition 3. *Let L denote the linear complexity of an output sequence u. Then $L \leq \pi(L_0 + \ldots + L_{q-1})$. If $q = 2$, the sequences b^0 and b^1 are nonzero, and the respective periods π, λ_0, and λ_1 are pairwise coprime then $L \geq (\hat{L} - 1)(L_0 + L_1 - 2)$.*

Proof. To prove an upper bound on the linear complexity of the sequence u it is sufficient to present a polynomial $P(\cdot)$ for which $P(u) = 0$ (i.e. P is an annihilating polynomial of u). Let us consider an arbitrary uniform π-decimation of u. Since π is the period of the control sequence a, this decimation is equal to the (t_j, π)-decimation of b^j for some $j \in \{0, \ldots, q-1\}$ and $t_j \in \{0, \ldots, \lambda_j - 1\}$. Then, by Lemma 3, there exists a polynomial $Q_j(\cdot)$ of degree not greater then L_j annihilating this decimation as well as all the other π-decimation sequences of b^j. The polynomial $Q_j(\cdot)$ also annihilates the uniform π-decimation of u that we consider.

Now let $Q(\cdot)$ be the least common multiple of polynomials $Q_0(\cdot), \ldots, Q_{q-1}(\cdot)$ where $Q_j(\cdot)$ is the polynomial annihilating any π-decimation of b^j. Then $Q(\cdot)$ annihilates any π-decimation of u and thus polynomial $P(\cdot) = Q(x^\pi)$ of degree not greater then $\pi(L_0 + \ldots L_{q-1})$ annihilates u. Thus the linear complexity of u is at most $\pi(L_0 + \ldots + L_{q-1})$.

The second part of the proposition follows from [6, Theorem 6] since the algebraic normal form of the combining function for $q = 2$ is $F(a, x_0, x_1) = a(x_0 \oplus x_1) \oplus x_0$. Condition $q = 2$ is required since only then the algebraic normal form of F is free from powers. $\square$

It remains an open problem how estimate a lower bound for the linear complexity of the output sequence u when $q > 2$.

If we assume that input sequences of the combining function F are sequences of uniform, independent and identically distributed random variables (i.e. purely random sequences) then its output sequence is purely random as well since the combining function of the generator is balanced. Thus the balance quality of the combining function ensures good statistical properties of the key-stream.

Sequences produced by linear feedback shift registers (clocked regularly or irregularly) could be used as inputs for function F in practical implementations of the key-stream generator described above. Let us note that the combining function F of the generator is memoryless, balanced and zero-order correlation immune (its output is correlated to inputs $x_0, \ldots, x_{q-1}$ and this correlation decreases if q is increased). Thus when all shift registers are clocked regularly, it is possible to apply the basic or fast correlation attack in order to reconstruct the initial state of shift registers that produce sequences b^j $(j = 0, \ldots, q-1)$. Therefore it is reasonable to use large q and clock-controlled LFSR's to generate sequences b^j $(j = 0, \ldots, q-1)$. We note that knowing the periods of the control and the generating registers, one can easily verify the condition of coprimality in Proposition 3. Memoryless combiners of clock-controlled LFSR's can also be susceptible to certain types of correlation attacks. This will be discussed further in Section 6. But the essential benefit of these combiners consists in their immunity against fast correlation attacks.

For practical implementation of the suggested generator it may be reasonable to select q as a power of 2, and to generate binary sequences a and b^j $(j = 0, \ldots, q-1)$, to feed them as input to the $q+1$-input combining function F. The control sequence is split into $\log_2 q$-long tuples that are used to index sequences b^j $(j = 0, \ldots, q-1)$. Following the first half of the proof of Lemma 2, it can be readily shown that if the control sequence splits into $\log_2 q$-tuples consisting of all q possible values and if $\gcd(\pi, K) = 1$ then $K \mid \tau$.

6 Correlation Attacks on Clock-Controlled Shift Registers and their Memoryless Combiners

We start with defining a statistical model for a correlation attack. In this section, we continue using notations introduced in Section 1. Assume that b is a purely random sequence in $P = \mathrm{GF}(2)$, i.e. it is a sequence of uniform, independent and identically distributed (i.i.d.) random variables, rather than the output of an LFSR. Also assume that the control sequence a consists of i.i.d. positive, integer valued, random variables that is independent of b. The random sequences a and b are combined according to (1) to generate the output random sequence u. Since the sequence a contains only positive elements, it is clear that u is a purely random sequence in P itself (for instance, this is not true for the output of stop-and-go generator).

Irregular clocking is called *constrained* if the range of elements in a is limited by some value and *unconstrained* otherwise. The secret key is assumed to control the initial state of generating register. The objective of a correlation attack is defined here as the reconstruction of the initial state of the GR from a given segment of the output sequence u, thereby knowing the GR length and the feedback polynomial (that can be arbitrary; so it is not necessarily linear and irreducible). The control sequence is unknown except for the probability distribution of the random variable a_i, $i \geq 0$. If $\overline{a}$ is the expected value of a_i then $p_d = 1 - 1/\overline{a}$ is called the *deletion rate*. The model for unconstrained clocking assumes independent deletions from b with probability p_d.

Let $\mathcal{D}$ be an arbitrary subset of the set of positive integers $\mathbb{Z}^+$. Then we say that a given string $Y^n = \{y_i\}_{i=0}^{n-1}$ of length n can be $\mathcal{D}$-*embedded* into a given string $X^m = \{x_i\}_{i=0}^{m-1}$ of length $m \geq n$ if there exists a string $D^n = \{d_i\}_{i=0}^{n-1}$ of length n such that all d_i's lie in $\mathcal{D}$ and $y_i = x\left(\sum_{j=0}^{i} d_i\right)$, $0 \leq i < n$. The embedding is called *constrained* if $\mathcal{D} \neq \mathbb{Z}^+$ and *unconstrained* otherwise.

Let $U^n = \{u(t)\}_{t=0}^{n-1}$ be an observed segment of the output sequence (an observed random value). We guess the initial state of the GR, and starting from this state, under regular clocking, generate an m-long segment X^m where $m \geq n$. The following hypothesis H_0 has to be tested against alternative H_1:

H_0 : X^m and U^n are independent (initial state of the GR is guessed incorrectly).
H_1 : X^m and U^n are correlated (initial state of the GR is guessed correctly and U^n can be obtained from X^m by the described above statistical model).

It follows from our assumption of the statistical model that each initial state of the GR gives rise to a conditional probability distribution on the set of all output sequences. Thus, hypothesis H_0 corresponds to a uniform distribution of U^n and alternative H_1 to a conditional distribution. Given an observed segment U^n, the optimal decision strategy (minimizing the probability of decision error) is to decide on the initial state that leads to the maximum posterior probability of U^n or, equivalently, the initial state whose corresponding sequence X^m has the maximum correlation with U^n.

Thus, for a correlation attack on irregularly clocked shift register, a measure for correlation between the output string produced by irregular clocking and the output of the GR, when clocked regularly, is required. Some possibilities have been suggested in the literature: the 'edit distance' [12], the 'embedding property' [13, 14, 9, 3], and the 'joint probability' [15, 13].

The basis for the *edit distance* correlation attack is a distance measure between two sequences of different length, suitably defined to reflect the transformation of the GR output sequence b to the output u according to the assumed statistical model. Thus, such distance measure should allow statistical discrimination between hypothesis H_0 and alternative H_1. Hypothesis H_0 is accepted if the distance between X^m and U^n is greater than a threshold estimated basing on the given probabilities of the decision errors. The 'constrained Levenshtein distance' (when the only edit operation is element deletion) was suggested in [12] as a possible distance measure for constrained clocking, although no analytical estimation of relevant probability distributions was given. It is also not clear how close the decision rule based on edit distance is to the one based on the maximum posterior probability (which is optimal for the given statistical model). The edit distance correlation attack does not seem to be very practical since its basic tool, the edit distance, is too general.

In the *embedding correlation* attack the objective is to find all possible initial states for the GR, such that for some $m \geq n$ a given segment $\{u(t)\}_{t=0}^{n-1}$ can be $\mathcal{D}$-embedded into the m-long output sequence of the GR produced under regular clocking, where $\mathcal{D}$ is the range of elements in a. The attack is successful if there are only few of such initial states. To check whether embedding is possible, one can use the direct matching algorithm for constrained embedding [3], which has computational complexity $O(nm)$, or one can use algorithms for calculating the Levenshtein distance [12, 24] for constrained and unconstrained clocking, respectively, which have computational complexity $O(n(m-n))$. Embedding is possible if and only if the distance is equal to $m-n$.

In [13] the unconstrained embedding attack is proved to be successful if and only if the deletion rate is smaller than $1/2$ and the length of the observed output sequence is greater than a value that is linear in the length of the GR (where $m = m(n)$ is chosen in such a way that $n\overline{a} \leq m(n)$ and $\lim_{n\to\infty} n/m(n) = 1/\overline{a}$). According to [14], if $d = \max \mathcal{D}$ and the length of X^m is chosen to be maximum possible, so equal to dn (if $a_0 = 0$), then the constrained embedding attack is successful if the length of the observed output sequence is greater than a value linear in the GR length and superexponential in d, and is not successful if this length is smaller than a value linear in the GR length and exponential in d. This proves that, by making d sufficiently large, one can not achieve theoretical security against the embedding attack but one can significantly improve the practical security. To determine the constrained embedding probability analytically appears to be a very difficult combinatorial problem. This problem has only been solved in [9] for the specific case when $\max \mathcal{D} = 2$.

It is obvious that embedding attacks are not optimal in general since they make no use of the probability distribution of the control sequence. The statistically optimal decision rule for distinguishing H_0 and H_1 has to be based on the joint probability and that is used as a basis for a *probabilistic correlation* attack. In this attack, one decides on the initial state with maximum joint probability of X^m and U^n. The problem of efficiently computing this probability for constrained clocking is solved in [15] with computational complexity $O(n(m-n))$. The recursive algorithm, presented in [13], allows to estimate the joint probability for unconstrained clocking if the distribution of the control sequence is geometric with average $1/p$. The computational complexity of this algorithm is $O(n(m-n))$. The length $m(n)$ should be chosen in such a way that $\lim_{n\to\infty} n/m(n) = p$. Then it can be proved that the unconstrained probabilistic attack is successful for any $0 \le p < 1$ provided that

$$n > r\frac{1-p}{C} \quad \text{where} \quad C \approx \left(1 - \frac{p}{2}\right)\log(2-p) + \frac{p}{2}\log p \ .$$

The correlation attack on the Shrinking Generator [4], proposed by Johansson in [20], is based on a MAP decoding algorithm for the deletion channel. This approach can as well be readily applied to the general model of a shift register under unconstrained clocking. A deletion rate p_d is used to define the deletion channel characteristics. If $p_d = 1/2$ then the model for unconstrained clocking is equivalent to the one of the Shrinking Generator. The suboptimal MAP decoding algorithm proposed in [20] is likely also to work for deletion rate values different from $1/2$ but that should be further examined by simulating the attack (since part of the suboptimal MAP decoding algorithm is based on simulation results).

All above mentioned correlation attacks on the initial state of the GR imply an exhaustive search over all possible initial states. Thus, their computational complexity remains exponential. A more efficient fast correlation attack having polynomial complexity was suggested in [8]. The primary objective of this attack is to reconstruct a segment of the control sequence a and then, when having obtained enough (little more than the length of the GR) consecutive terms of a at any point of time, it is possible to determine the initial state of the GR uniquely or almost uniquely. The feedback polynomial of the GR is now assumed to be linear. The algorithm devised in [8] consists in iterative recomputation of posterior probabilities for unknown elements of the control sequence. The convergence condition that has to hold for successful reconstruction is the following:

$$\sum_{\omega} N_{d,\omega}(1-p)^{\omega} > 1$$

for all $d \in \mathcal{D}$ whose probability is not very close to zero, where $\mathcal{D}$ is the range of elements in a, p is the deletion rate and $N_{d,\omega}$ denotes the number of the GR feedback polynomial multiples of weight $\omega + 1$, such that the distance between at least one pair of their adjacent feedback connections (taps) is equal to $d + 1$. Unfortunately, no technical details are known yet to support the theory.

Combining clock-controlled shift registers with a memoryless combining function makes embedding correlation attacks infeasible but edit distance and joint probability attacks are still applicable although less efficient. These attacks require the combining function to be known. If the combining function is zero-order correlation immune then its output is correlated to at least one input. In this case, one can apply the correlation attack based on edit distance or joint probability to reconstruct the initial state of the corresponding irregularly clocked LFSR, assuming that the known segment of its output sequence is combined with nonuniform additive noise. The idea of these attacks was described earlier in Section 6. The edit distance attack for the constrained clocking case can be based on the Levenshtein distance, as suggested in [12]. Except element deletion, an extra edit operation, namely element substitution, should be considered due to the additive noise. The attack based on the joint probability for constrained clocking case was devised in [15]. There are no fast correlation attacks on noised clock-controlled shift registers reported in the literature, thus these schemes seem to be very secure.

If the combining function of the clock-controlled registers is correlation immune or has memory, then correlation attacks based on many-to-one string edit distance and joint probability are still feasible, see [11]. The efficiency of these attacks depends on an available pair of mutually correlated feedforward linear transforms of the output sequence and input sequences respectively, in the same but now regularly clocked combiner. A large correlation coefficient, a small memory size and a small number of input sequences to the linear transform of the input increase the efficiency of the attack. A theoretical estimation of the conditions for these attacks to be successful seems to be a difficult, yet unsolved problem.

7 Conclusion

The period of the output sequence generated by an arbitrary clock-controlled LFSR with an irreducible feedback polynomial and an arbitrary structure of the control sequence is estimated. A sufficient condition for this period to reach its maximal value is formulated and some specific configurations of clock-controlled arrangements with a maximal period of the output sequence are defined. Further, we discuss randomness properties of clock-controlled LFSR output sequences. The deviation of the number of occurrences of elements in a full period from the "ideal" value and the autocorrelation function are estimated.

Finally, we generalize the Geffe generator for the case of multiple inputs with arbitrary periodical input sequences in the field GF(q). In particular, this implies that clock-controlled shift registers can be used as inputs. Using clock-controlled registers and multiple inputs makes this generator immune against fast correlation attacks and less susceptible to basic attacks. We analyze some relevant algebraic properties of the suggested generator.

Acknowledgment

The author is grateful to Henk van Tilborg for his comments that helped to improve this paper.

References

1. Thomas Beth and Fred C. Piper. The stop-and-go generator. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology: Proceedings of EuroCrypt '84*, volume 209 of *Lecture Notes in Computer Science*, pages 88–92, Berlin, 1985. Springer-Verlag.
2. William G. Chambers. Clock-controlled shift registers in binary sequence generators. *IEE Proceedings - Computers and Digital Techniques*, 135(1):17–24, January 1988.
3. William G. Chambers and Dieter Gollmann. Embedding attacks on step$[1..D]$ clock-controlled generators. *Electronic Letters*, 36(21):1771–1773, October 2000.
4. Don Coppersmith, Hugo Krawczyk, and Yishay Mansour. The shrinking generator. In Douglas R. Stinson, editor, *Advances in Cryptology - Crypto '93*, volume 773 of *Lecture Notes in Computer Science*, pages 22–39, Berlin, 1994. Springer-Verlag.
5. Philip R. Geffe. How to protect data with ciphers that are really hard to break. *Electronics*, 46(1):99–101, January 1973.
6. Jovan Dj. Golić. On the linear complexity of functions of periodic GF(q) sequences. *IEEE Transactions on Information Theory*, 35(1):69–75, January 1989.
7. Jovan Dj. Golić. On decimation of linear recurring sequences. *Fibonacci Quarterly*, 33(5):407–411, November 1995.
8. Jovan Dj. Golić. Towards fast correlation attacks on irregularly clocked shift registers. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *Advances in Cryptology - EuroCrypt '95*, volume 921 of *Lecture Notes in Computer Science*, pages 248–262, Berlin, 1995. Springer-Verlag.
9. Jovan Dj. Golić. Constrained embedding probability for two binary strings. *SIAM Journal on Discrete Mathematics*, 9(3):360–364, August 1996.
10. Jovan Dj. Golić. Periods of interleaved and nonuniformly decimated sequences. *IEEE Transactions on Information Theory*, 44(3):1257–1260, May 1998.
11. Jovan Dj. Golić. Edit distances and probabilities for correlation attacks on clock-controlled combiners with memory. *IEEE Transactions on Information Theory*, 47(3):1032–1041, March 2001.
12. Jovan Dj. Golić and Miodrag J. Mihaljević. A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance. *Journal of Cryptology*, 3(3):201–212, 1991.
13. Jovan Dj. Golić and Luke O'Connor. Embedding and probabilistic correlation attacks on clock-controlled shift registers. In Alfredo De Santis, editor, *Advances in Cryptology - EuroCrypt '94*, volume 950 of *Lecture Notes in Computer Science*, pages 230–243, Berlin, 1995. Springer-Verlag.
14. Jovan Dj. Golić and Luke O'Connor. A cryptanalysis of clock-controlled shift registers with multiple steps. In Ed Dawson and Jovan Dj. Golić, editors, *Cryptography: Policy and Algorithms*, volume 1029 of *Lecture Notes in Computer Science*, pages 174–185, Berlin, 1996. Springer-Verlag.

15. Jovan Dj. Golić and Slobodan V. Petrović. A generalized correlation attack with a probabilistic constrained edit distance. In Rainer A. Rueppel, editor, *Advances in Cryptology - EuroCrypt '92*, volume 658 of *Lecture Notes in Computer Science*, pages 472–476, Berlin, 1993. Springer-Verlag.
16. Jovan Dj. Golić and Miodrag V. Živković. On the linear complexity of nonuniformly decimated PN-sequences. *IEEE Transactions on Information Theory*, 34(5):1077–1079, September 1988.
17. Dieter Gollmann and William G. Chambers. Clock-controlled shift registers: a review. *IEEE Journal on Selected Areas in Communications*, 7(4):525–533, May 1989.
18. Solomon W. Golomb. *Shift Register Sequences*. Holden-Day series in information systems. Holden-Day, San Francisco, 1967. Reprinted by Aegean Park Press, 1982.
19. G.R.Blakley and G.B.Purdy. A necessary and sufficient condition for fundamental periods of cascade machines to be product of the fundamental periods of their constituent finite state machines. *Information Sciences: An International Journal*, 24(1):71–91, June 1981.
20. Thomas Johansson. Reduced complexity correlation attacks on two clock-controlled generators. In Kazuo Ohta and Dingyi Pei, editors, *Advances in Cryptology - AsiaCrypt '98*, volume 1514 of *Lecture Notes in Computer Science*, pages 342–356, Berlin, 1998. Springer-Verlag.
21. Alexander A. Kholosha. Some problems of generating pseudo-random sequences using finite state automata. In *Tractates of the Institute of Modelling Problems in Power Engineering of the National Academy of Sciences of Ukraine, Issue 1*, pages 74–90. Svit, Lviv, 1998. (in Russian).
22. Rudolf Lidl and Harald Niederreiter. *Finite Fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Addison-Wesley, Amsterdam, 1983.
23. Rudolf Lidl and Harald Niederreiter. *Introduction to Finite Fields and Their Applications*. Cambridge University Press, Cambridge, 1986.
24. Miodrag J. Mihaljević. An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure. In J. Seberry and Y. Zheng, editors, *Advances in Cryptology - AusCrypt '92*, volume 718 of *Lecture Notes in Computer Science*, pages 349–356, Berlin, 1993. Springer-Verlag.
25. Rainer A. Rueppel. *Analysis and Design of Stream Ciphers*. Communications and Control Engineering Series. Springer-Verlag, Berlin, 1986.
26. Rainer A. Rueppel. Stream ciphers. In Gustavus J. Simmons, editor, *Contemporary Cryptology: the Science of Information Integrity*, pages 65–134. IEEE Press, New York, 1992.
27. Neal Zierler. Linear recurring sequences. *Journal of the Society for Industrial and Applied Mathematics*, 7(1):31–48, March 1959.