ON FUNCTIONS OF LINEAR SHIFT REGISTER SEQUENCES*

Tore Herlestam

Dept. of Computer Engineering
University of Lund
P.O. Box 118
S-221 00 LUND, Sweden

and

Dept. of Signal Security
General Staff of Defense
Bankogårdsgatan 74
S-252 60 HELSINGBORG, Sweden

Abstract

This paper is intended as an overview, presenting several results on the linear complexity of sequences obtained from functions applied to linear shift register sequences. Especially for cryptologic applications it is of course highly desirable that the linear complexity be as large as possible, and not only to get a huge period. The theory reviewed in this paper contains several criteria on how to achieve such goals.

1. INTRODUCTION

In what follows we shall consider shift register sequences $(x_k)_{k\geq 0}$, over a finite field GF(q), q a prime power. Two well-known models for shift registers are in use. The Fibonacci model consists of cascaded memory boxes. The contents of each box is multiplied by a feedback coefficient before being taken to a common summing device to produce the feedback element. The feedback coefficients are numbered $c_1, c_2, ..., c_n$ from the feedback terminal.

In the Galois model adders are inserted between the memory boxes, the system output is multiplied by the feedback coefficients, numbered $c_1, c_2, ..., c_n$ from the output terminal, and the products are taken to the adders.

In both cases the same shift register recurrence is obtained:

$$x_k = c_1 x_{k-1} + c_2 x_{k-2} + \ldots + c_n x_{k-n}, \quad k \geq n.$$

Three different methods for handling this recurrence are in use. The linear algebraic (matrix) method is the most commonly used (e.g. Golomb (1967)), in particular in coding theory. Here the

---

*This research was supported in part by the National Swedish Board for Technical Development under grants 81-3323, 83-4364, and 85-3759 at the University of Lund.

F. Pichler (Ed.): Advances in Cryptology - EUROCRYPT '85, LNCS 219, pp. 119-129, 1986.

state $(x_{k-1}, x_{k-2}, \ldots, x_{k-n})$ of the Fibonacci model is transformed by the next-state-function

$$\begin{pmatrix} x_k \\ x_{k-1} \\ \vdots \\ x_{k-n+1} \end{pmatrix} = \begin{pmatrix} c_1 & \ldots & c_{n-1} & c_n \\ 1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix} \begin{pmatrix} x_{k-1} \\ x_{k-2} \\ \vdots \\ x_{k-n} \end{pmatrix}$$

most often written in the transposed form

$$(x_k, x_{k-1}, \ldots, x_{k-n+1}) = (x_{k-1}, x_{k-2}, \ldots, x_{k-n}) \begin{pmatrix} c_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & 0 & \ldots & 1 \\ c_n & 0 & \ldots & 0 \end{pmatrix}$$

by means of the so-called companion matrix. By iteration

$$\begin{pmatrix} x_{k-1} \\ x_{k-2} \\ \vdots \\ x_{k-n} \end{pmatrix} = \begin{pmatrix} c_1 & \ldots & c_{n-1} & c_n \\ 1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{pmatrix}^{k-n} \begin{pmatrix} x_{n-1} \\ x_{n-2} \\ \vdots \\ x_0 \end{pmatrix}$$

where $(x_{n-1}, x_{n-2}, \ldots, x_0)$ is the starting state of the Fibonacci model of the register.

A closely related finite automaton model is used by Nyffeler (1975).

Rewriting the shift register recurrence as a homogeneous linear difference equation

$$x_k - c_1 x_{k-1} - c_2 x_{k-2} - \ldots - c_n x_{k-n}, k \geq n,$$

we can apply the classical technique as used by Selmer (1966) and Key (1976) among others. Here the characteristic polynomial

$$c(t) = t^n - c_1 t^{n-1} - \ldots - c_n$$

plays a dominant role.

If the characteristic polynomial is factorized over its splitting field GF(q^s),

$$c(t) = \prod_j (t - z_j)^{m_j}, \; z_j \in \mathrm{GF}(q^s) \text{ with multiplicity } m_j \,,$$

then the general solution of the difference equation can be written

$$x_k = \sum_{j,r} A_{jr} \binom{k+r-1}{r} z_j^k, \; A_{jr} \in \mathrm{GF}(q^s).$$

Note that, compared with difference or differential equations over the field of reals or the complex numbers, $\binom{k+r-1}{r}$ is used instead of k^r in order to achieve linear independence over GF(q).

Finally, the generating function method, used by Zierler (1959), can be applied to the shift register recurrence. Here the feedback polynomial

$$\mathrm{f}(t) = 1 - c_1 t - c_2 t^2 - \ldots - c_n t^n,$$

reciprocal to the characteristic polynomial, plays a major role. The shift register sequence $(x_k)_{k\geq 0}$, is identified with the formal power series

$$x(t) = \sum_{k=0}^{\infty} x_k t^k$$

and then the shift register equation is equivalent to

$$\mathrm{f}(t)x(t) = \mathrm{x}^*(t)$$

a polynomial of degree < deg f, so that

$$x(t) = \frac{\mathrm{x}^*(t)}{\mathrm{f}(t)},$$

a rational form over GF(q).

Note that $(x_0, x_1, \ldots, x_{n-1})$ is the starting state of the Fibonacci model, while $(x_0^*, x_1^*, \ldots, x_{n-1}^*)$ is the starting state of the Galois model.

Zierler also introduced the linear spaces over GF(q)

$$G(\mathrm{f}) = \{\, \mathrm{x}^*/\mathrm{f};\ \deg \mathrm{x}^* < \deg \mathrm{f}\},$$

consisting of all shift register sequences with f as feedback polynomial.

The rational forms x=x^*/f are ideally suited to handle linear shift register sequences, e.g.

- f equals the minimum polynomial f_x of the sequence x if and only if x^* and f are coprime, $\gcd(\mathrm{x}^*,\mathrm{f}) = 1$
- $x + y = \dfrac{\mathrm{x}^*}{\mathrm{f}} + \dfrac{\mathrm{y}^*}{\mathrm{g}} = \dfrac{\mathrm{z}^*}{\mathrm{lcm(f,g)}}$ implies that f_{x+y} divides lcm(f,g).

2. THE LINEAR COMPLEXITY CONCEPT

Given a periodic sequence x over a finite field GF(q) we can always write it as

$$x(t) = \frac{\mathrm{g}(t)}{1 - t^{\mathrm{per}\,x}},$$

i.e. a linear shift register sequence. The length of the shortest possible linear shift register being able to produce the sequence, i.e. the degree of the minimum polynomial f_x

$$\mathrm{L}(x) = \deg \mathrm{f}_x$$

is called the *linear complexity* of the sequence.

It is readily generalized by

$$\mathrm{L}(S) = \deg \mathrm{f}_S$$

to any finite set S of periodic sequences.

The problem of determining the linear complexity of a given sequence is completely solved in practice by the well-known Berlekamp-Massey algorithm (Berlekamp (1968), Massey (1969)). However, when the linear complexity becomes very large or when we want to derive some nice criteria on how to obtain maximal complexity, another technique is needed.

Any memoryless function of a number of linear shift register sequences over GF(q) can be implemented by means of a function F from $GF(q)^n$ to GF(q). Since GF(q) is finite, F has to be a polynomial function

$$F(x) = \sum_{\underline{a}} A_{\underline{a}} x^{\underline{a}}, \quad A_{\underline{a}} = A_{a_1 a_2 \ldots a_n}, \quad \underline{x}^{\underline{a}} = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$$

This is the algebraic normal form used by Müller (1954), Reed (1954) for q=2, and by Benjauthrit and Reed (1976) for general q.

Thus we have to study

1. $L(x+y)$ and $L(ax)$, $(x+y)_k = x_k + y_k$, $(ax)_k = ax_k$
2. $L(xy)$, $(xy)_k = x_k y_k$ (Hadamard product)
3. $L(x^a)$, $(x^a)_k = x_k^a$ (Hadamard power)

The simplest case is $L(ax)$. Defining the content

$$c(a)=0 \text{ when } a=0, =1 \text{ when } a \neq 0,$$

we find immediately

$$L(ax) = c(a)L(x).$$

For $x + y$ we have

Theorem 2.1: $L(x+y) \leq L(x)+L(y)$ with equality if and only if the minimum polynomials f_x and f_y are coprime i.e. $\gcd(f_x, f_y)=1$.

Corollary 2.2: $L(G(f) + G(g)) \leq L(G(f)) + L(G(g))$ with equality if and only if f and g are coprime i.e. $\gcd(f,g)=1$.

3. THE COMPLEXITY OF THE HADAMARD PRODUCT

The Hadamard product was first considered by Selmer (1966). When $f(t) = \prod_u (1 - \frac{t}{u})$, $g(t) = \prod_v (1 - \frac{t}{v})$ with mere simple zeroes, Selmer defined $f\S g = \prod_{u,v}(1 - \frac{t}{uv})$ and showed

Theorem 3.1: Assuming x belongs to $G(f)$, y to $G(g)$ then xy belongs to $G(f\S g)$. Further, if f and g are prime (irreducible) then $f\S g$ is prime too.

Corollary 3.2: If f and g are prime then $f_{xy} = f\S g$.

Note the analogy with Hadamard's well-known theorem for analytic functions:

If $\sum_{n=0}^{\infty} a_n z^n$, $\sum_{n=0}^{\infty} a_n z^n$ are analytic around the origin with singularities in the points $z_j(a)$, $1 \leq j \leq r$, $z_k(b)$, $1 \leq k \leq s$, then the Hadamard product $\sum_{n=0}^{\infty} a_n b_n z^n$ has all its singularities at the points $z_j(a)z_k(b)$, $1 \leq j \leq r$, $1 \leq k \leq s$.

Zierler and Mills (1973) defined f$\vee$g = f§g when f and g have mere simple zeroes and transferred it to the general case by means of an algebraic algorithm, utilizing the prime factorizations of f and g. No bounds on deg f$\vee$g or conditions for maximality were given.

Remark. Zierler and Mills used $\vee$ although it has nothing in common with the logical OR.

Herlestam (1977, 1982) defined f$\wedge$g as the minimum polynomial of

$$G(\mathrm{f})G(\mathrm{g}) = \{\ xy;\ x \text{ in } G(\mathrm{f}),\ y \text{ in } G(\mathrm{g})\ \}$$

and showed

Theorem 3.3: deg f$\wedge$g $\leq$ deg f $\cdot$ deg g with equality if and only if at least one of f and g has mere simple zeroes and all the zero products $z(\mathrm{f})z(\mathrm{g})$ are different.

Corollary 3.4: If f and g are prime and of coprime degrees then deg f$\wedge$g = deg f $\cdot$ deg g.

(Selmer (1966): in this case f$\wedge$g is prime.)

Corollary 3.5: $\mathrm{L}(xy) \leq \mathrm{L}(x)\mathrm{L}(y)$ with equality if and only if at least one of f_x and f_y has mere simple zeroes and all the zero products $z(\mathrm{f}_x)z(\mathrm{f}_y)$ are different.

Corollary 3.6: If f_x and f_y are prime and of coprime degrees then $\mathrm{L}(xy) = \mathrm{L}(x)\mathrm{L}(y)$.

(Selmer (1966): in this case f_{xy} is prime.)

Remark. Using the classical approach when q=2 and f_x and f_y prime and of coprime degrees, Key (1976) proved Corollary 3.6.

The period of a sequence $x \neq 0$ in $G(\mathrm{f})$ is trivially upperbounded

$$\text{per } x \leq \mathrm{q}^{\deg \mathrm{f}} - 1.$$

When equality is attained x is called a maximum length sequence (ML for short). The period of a feedback polynomial is defined by

$$\text{per f} = \min r \text{ for which } \mathrm{f}(t) \text{ divides } 1 - t^r.$$

Apparently per x = per f_x so if x is ML then all $x \neq 0$ in $G(\mathrm{f})$ are ML and

$$\text{per f} = \mathrm{q}^{\deg \mathrm{f}} - 1.$$

In this case f is called a maximum length polynomial (ML for short). Many authors use 'primitive polynomial' instead of ML-polynomial (but not 'primitive sequence' instead of ML-sequence !).

4. THE POWER FUNCTION

The power function x^a is of interest only when q>2 since $u^2=u$ holds in GF(2). If $a \geq$q it can be reduced by means of $u^q=u$ in GF(q). Thus we may assume $0 \leq a <$q.

Since q is a prime power, q=p^e, we can proceed by writing a in the p-ary number system

$$a = a_0 + a_1 p + a_2 p^2 + \ldots + a_{e-1} p^{e-1},$$

where the digits a_i are ≥ 0 and <p.

In order to handle a power of a shift register sequence we may use the well-known multinomial formula (see e.g. Tucker (1980))

$$(\sum_{j=1}^{n} X_j)^s = \sum_{\underline{u}} \frac{s!}{u_1! \ldots u_n!} X_1^{u_1} \ldots X_n^{u_n}$$

summed over all nonnegative solutions $\underline{u}$ of $\sum_i u_i = s$.

Note that $\frac{s!}{u_1! \ldots u_n!}$ should be interpreted by first considering it over the integers, then reducing it modulo the characteristic of the field.

Utilizing this multinomial formula Herlestam (1982 and later) derived the following results.

Theorem 4.1: If $0 \leq a <$q, $a = \sum_{i=0}^{e-1} a_i p^i$, $0 \leq a_i < p$, q=p^e, then

$$\mathrm{L}(x^a) \leq \prod_i \binom{\mathrm{L}(x) + a_i - 1}{a_i}$$

with equality if x is a ML-sequence. In particular, when p=2,

$$\mathrm{L}(x^a) \leq \mathrm{L}(x)^{H(a)},$$

where $H(a)$ is the Hamming weight of a and where equality holds if x is a ML-sequence.

(Brynielsson (1985): equality in the ML-case).

Now we have at our disposal all the components for handling any function of any finite number of shift register sequences. In the general case it may of course be quite hard to guarantee that maximal complexity be attained, but in many instances this can be achieved.

The following case is closely connected with the power function. Let $x_1, x_2, \ldots, x_s$ be a number of different shift register sequences with the same feedback polynominal f. The power function technique yields

$$\mathrm{L}(x_1, x_2, \ldots, x_s) \leq \binom{\deg \mathrm{f} + s - 1}{s},$$

a not particularly good estimate however. Instead, Herlestam (1983) derived the following

Theorem 4.2: Assume f prime over GF(q) and that $x_1, x_2, \ldots, x_s$, all $\neq 0$, be shift register sequences with f as feedback polynomial so that L(x_i)=L=deg f. Further, let $x_1, x_2, \ldots, x_s = y$. Then

1. $L(y) \le A_q(L,s) = \sum_{k=1}^{s} c_q(s,k)\binom{L}{k}$, where

$$c_q(s,k) = \sum_{r=0}^{k-1}(-1)^r\binom{k-1}{r}\binom{s-r(q-1)-1}{k-1}$$

so that $A_q(L,s) = \sum_{j=0}^{s-1}(-1)^j\binom{s-j(q-1)-1}{j}\binom{L+s-jq-1}{L-j-1}$

2. if g is a prime factor of f_y then deg g divides deg f_y.

In particular, when $s <$q, $A_q(L,s) = \binom{L+s-1}{s}$

and when q=2, $A_2(L,s) = \sum_{k=1}^{s}\binom{L}{k}$.

Remark. In the case of nonlinear feedforward, where q=2 and f a ML-polynomial, this result was stated without proof by Ristenbatt et al. (1973) and obtained later by Key (1976).

5. NONLINEAR FEEDFORWARD

The GF(2) case has been investigated by Groth (1971), Key (1976), Jennings (1980), Beker and Piper (1982), Rueppel (1984).

In the GF(q) case Herlestam (1983) derived

Theorem 5.1: Assume that f is prime over GF(q) and that x_i, $1 \le i \le s \le$ deg f, are sequences taken from different taps in a linear shift register with f as feedback polynomial. Let $y = x_1, x_2, \ldots, x_s$. Then

1. L(y) is independent of the starting state
2. if g is a prime factor of f_y then deg g divides deg f_y so if deg f_y is prime then f_y must be prime unless it has a first-degree factor
3. all zeroes of f_y are simple and belong to the set

$$S = \{\prod_i z_i^{w_i};\quad \sum_i w_i = s;\quad w_i \ge 0;\quad f(z_i) = 0\}.$$

Lower bounds on the linear complexity have been obtained by Rueppel (1984) in the GF(2) case for some special classes of feedforward functions.

6. SOME SKETCHES OF PROOFS

Th. 2.1: From $f_{x+y}|\mathrm{lcm}(f_x,f_y) \mid f_x f_y$ it follows that $L(x+y) \le L(x)+L(y)$. If gcd(f_x,f_y)=1 and $g \mid f_x f_y$, g prime, then $g \mid f_x$ or $g \mid f_y$ but not both so assume $g \mid f_x$. Should $L(x+y) < L(x)+L(y)$ then $g \mid (x^* f_y + y^* f_x)$ i.e. $g \mid x^* f_y$. Since gcd(g,f_y)=1 this implies $g \mid x^*$, against the minimality of f_x.

Conversely, if gcd(f_x,f_y)=h, deg h > 0, then h | ($x^* f_x + y^* f_y$), implying $L(x+y) < L(x)+L(y)$.

Th. 3.3: If f and g are feedback polynomials over GF(q) so that

$$f(t) = \prod (1 - \frac{t}{z_i(f)})^{m_i(f)}, \quad g(t) = \prod (1 - \frac{t}{z_j(g)})^{m_j(g)}$$

over a common splitting field GF(q^e), and if $x = x^*/f$, $y = y^*/g$, then the partial fractions expansions are

$$x = \sum_{i=0}^{n(f)-1} \sum_{r=0}^{m_i(f)-1} A_{ir}(1 - \frac{t}{z_i(f)})^{-r-1}, y = \sum_{j=0}^{n(g)-1} \sum_{s=0}^{m_j(g)-1} B_{js}(1 - \frac{t}{z_j(g)})^{-s-1}$$

By means of the binomial formal power series

$$(1-t)^{-a-1} = \sum_{k=0}^{\infty} \binom{a+k}{k} t^k$$

it follows that

$$x_k y_k = \sum_{i,r,j,s} A_{ir} B_{js} \binom{r+k}{k} \binom{s+k}{k} (z_i(f) z_j(g))^{-k},$$

As is easily shown

$$\binom{r+k}{k} \binom{s+k}{k} = \sum_m d_m(r,s) \binom{m+k}{k},$$

where $\max(r,s) \leq m \leq r+s$, and the integers $d_m(r,s)$ are independent of k. This shows that, over GF(q^e), xy is a partial fractions expansion of a rational form, the denominator of which has the zeroes $z_i(f) z_j(g)$ of multiplicity $\leq m_i(f) + m_j(g) - 1$.

Using the power sums of the roots to show that some polynomials over GF(q^e) are in fact polynomials over GF(q), it follows that deg $f_{xy} \leq$ deg f$\cdot$ deg g, and, after some further manipulations, the theorem follows.

Th. 4.1: When the characteristic coincides with the exponent the multinomial formula is particularly simple

$$(\sum X_j)^p = \sum X_j^p$$

since all multinomial coefficients $\neq 1$ are divisible by p.

By iteration

$$(\sum X_j)^{p^i} = \sum X_j^{p^i}$$

When $0 \leq a < p$,

$$(\sum X_j)^a = \sum_{\underline{u}} \frac{a!}{u_1! \ldots u_n!} X_1^{u_1} X_2^{u_2} \ldots X_n^{u_n}$$

where all the coefficients are $\neq 0$ since $a!$ cannot be divisible by p. Applied to an arbitrary element

$$x_k = \sum_{i,r} A_{ir} \binom{r+k}{k} z_i^{-k}$$

of a shift register sequence, one obtains for each term in the p-ary representation $a = \sum_i a_i p^i$ the inequality

$$\deg f_{x^{a_i p^i}} \le \binom{L(x) + a_i - 1}{a_i}$$

and finally, by Th. 3.3,

$$\deg f_{x^a} \le \prod \binom{L(x) + a_i - 1}{a_i}$$

The clause on equality follows from the facts that if x is a maximum length sequence, the zeroes of f_x can be written as

$$z^{q^i},\ 0 \le i < L(x),$$

where z is a primitive (q^n-1)-st root of unity, and that the q-ary representation of a number is unique.

Th. 4.2: Assume first that $x_1, x_2, \ldots, x_s$ are ML-sequences so that

$$x_i = x_i^*/f = \sum_{j=1}^{n} \frac{A_{ij}}{1 - t/z_j}$$

where all A_{ij}'s are nonzero. Thus

$$x_{ik} = \sum_{\underline{u}} A(\underline{u})(\underline{z}^{\underline{u}})^{-k}$$

where the summing interval is the set of all nonnegative solutions $\underline{u}$ of $\sum_j u_j = s$, and

$$A(\underline{u}) = \sum_{\underline{j}} \prod_{i=1}^{s} A_{ij_i}$$

summed over all permutations $\underline{j}$ of u_1 1's, u_2 2's,..., u_s s's. The minimum polynomial f_y cannot have any multiple zeroes, since the coefficients $A(\underline{u})$ are independent of k.

The zeroes of f can be written $z_j = z^{q^j}$ where z is a primitive (q^n-1)-st root of unity and

$$\underline{z}^{\underline{u}} = z^a\,, \quad 0 \le a < q^n - 1,$$

where $\sum_j u_j q^j = a \pmod{q^n - 1}$, $\underline{u}$ being a partition of $s = \sum_j u_j$, $u_j \ge 0$.

Let $A_q(n, s)$ denote the number of a's obtainable this way. It can also be described as the number of q-ary n-strings

$$a = \sum_{j=0}^{n-1} a_j q^j, \text{ not all } a_j = 0$$

such that $\sum_{j=0}^{n-1} a_j = s - k(q-1)$, $0 \le k < s/(q-1)$. This leads rather quickly to the form

$$A_q(n,s) = \sum_{k=1}^{s} c_q(s,k)\binom{n}{k}$$

where the integers $c_q(s,k)$ are independent of n and

$$c_q(s,k) = \sum_{j=1}^{q-1} c_q(s-j,k-1)\,, \quad c_q(s,1) = c_q(s,s) = 1.$$

When f is prime only, per f divides q^n-1 and z is a primitive root of unity of order per f. Hence the number of different $(\underline{z}^{\underline{u}})$'s must still be $\le A_q(n,s)$.

The clause on a prime factor of f_y follows quite easily from the fact that per f_y divides per f.

Th. 5.1: Follows from

$$x_i^*(t) = t^{e_i} x^*(t) \qquad (\text{mod } f(t)),$$

where x^* is associated solely with the starting state and the exponent $e_i \ge 0$ with the position of the tap from which x_i is taken.

Acknowledgement

The author wants to express his deep gratitude to Prof J. L. Massey and Prof R. Johannesson for many fruitful discussions on the subject.

SOME SELECTED REFERENCES (in chronological order)

L. Fibonacci, *Liber Abaci*, 1202

E. Galois, "Sur la theorie des nombres", Bull. Sci. Math. de M. Ferussac, 1830; J. Math. Pures Appl., 1846

L. Kronecker, *Werke Bd. 2*, pp. 146-149, 1881

D. E. Müller, "Application of Boolean Algebra to Switching Circuit Design and to Error Detection", IRE Trans. on Electron, Comp., 1954

I. S, Reed, "A Class of Error Correcting Codes and the Decoding Scheme", IRE Trans. on Electron. Comp., 1954

N. Zierler, "Linear Recurring Sequences", J. SIAM, 1959; also in W. H. Kautz, *Linear Sequential Switching Circuits*, Holden-Day, San Francisco, 1965

E. S. Selmer, *Linear Recurrence Relations over Finite Fields*, Univ. of Bergen, Norway, 1966

B. L. van der Waerden, *Algebra I*, Springer, Berlin, 1966

S. W. Golomb, *Shift Register Sequences*, Holden-Day, San Francisco, 1967

E. R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968

J. L. Massey, "Shift-Register Synthesis and BCH Decoding", IEEE Trans on Inform. Th., 1969

E. J. Groth, "Generation of Binary Sequences with Controllable Complexity", IEEE Trans. on Inform. Th., 1971

N. Zierler and W. H. Mills, "Products of Linear Recurring Sequences", J. Algebra, 1973

M. P. Ristenbatt et al., "Crack-Resistant Sequences for Data Security", IEEE Nat. Telecomm. Conf., 1973

P. R. Geffe, "How to Protect Data with Ciphers That Are Really Hard to Break", Electronics, 1973

P. Nyffeler, *Binäre Automaten und ihren linearen Rekursionen*, Ph.D. Thesis, Bern, 1975

B. Benjauthrit and I. S. Reed, "Galois Switching Functions and Their Applications", IEEE Trans. on Comp., 1976

E. L. Key, "An Analysis of the Structure and Complexity of Nonlinear Binary Sequences Generators", IEEE Trans. on Inform. Th., 1976

K. P. Yiu and R. B. Ward, "A Method for Deciphering a Maximal-Length Sequence", Proc. IEEE, 1977

T. Herlestam, "On Linearization of Nonlinear Combinations of Linear Shift Register Sequences", IEEE ISIT, Ithaca, New York, 1977

H. Lüneburg, *Galoisfelder, Kreisteilungskörper und Schieberegisterfolgen*, Bibliogr. Inst., Zürich, 1979

A. Tucker, *Applied Combinatorics*, Wiley, New York, 1980

S. M. Jennings, *A Special Class of Binary Sequences*, Ph.D. Thesis, London, 1980

T. Herlestam, "On Using Prime Polynomials in Crypto Generators", in *Cryptography, Proc. Burg Feuerstein, 1982*, ed. by T. Beth, Springer, Berlin, 1983

T. Herlestam, "On the Complexity of Functions of Linear Shift Register Sequences", IEEE ISIT, Les Arcs, France, 1982

H. Beker and F. Piper, *Cipher Systems*, Northwood Publ., London, 1982

R. Lidl and H. Niederreiter, *Finite Fields*, Encycl. Math. and Its Appl. Vol. 20, Addison-Wesley, 1983

T. Herlestam, "On the Complexity of Certain Crypto Generators", in *security, IFIP/sec'83*, ed. by V. Fåk, North-Holland, 1983

R. Rueppel, *New Approaches to Stream Ciphers*, Ph.D. Thesis, Zürich, 1984

L. Brynielsson, "On the Linear Complexity of Combined Shift Register Sequences", Eurocrypt 85, Linz, Austria, 1985