On the Linear and Nonlinear Complexity Profile of Nonlinear Pseudorandom Number Generators

Jaime Gutierrez, Igor E. Shparlinski, and Arne Winterhof

***Abstract*—We obtain lower bounds on the linear and nonlinear complexity profile of a general nonlinear pseudorandom number generator, of the inversive generator, and of a new nonlinear generator called quadratic exponential generator. The results are interesting for applications to cryptography and Monte Carlo methods.**

***Index Terms*—Inversive generator, linear and nonlinear complexity profile, nonlinear pseudorandom number generators, quadratic exponential generator.**

I. Introduction

We recall that the *linear complexity profile* $\mathcal{L}(\mathcal{S}, N)$ of an infinite sequence $\mathcal{S} := (s_n)_{n=0}^{\infty}$ of elements of the finite field $\mathbb{F}_q$ is the function which for every integer $N \geq 2$ is defined as the least order k of a linear recurrence relation

$$s_{n+k} = a_{k-1}s_{n+k-1} + \cdots + a_0 s_n, \qquad 0 \leq n \leq N-k-1$$

which is satisfied by this sequence (see [3], [18], [21], [33]). The largest value

$$\mathcal{L}(\mathcal{S}) := \sup_{N \geq 2} \mathcal{L}(\mathcal{S}, N)$$

is called the *linear complexity* of the sequence $\mathcal{S}$. Obviously, for some sequences the linear complexity can be equal to infinity. However, for the linear complexity of any periodic sequence of period t one easily verifies that

$$\mathcal{L}(\mathcal{S}) = \mathcal{L}(\mathcal{S}, 2t) \leq t.$$

The linear complexity and the linear complexity profile are important cryptographic characteristics of sequences. In particular, the well-known results about predictability (and thus unsuitability for cryptography) of sequences $\mathcal{Z} := (z_n)_{n=0}^{\infty}$ produced by the *linear generator*

$$z_n := az_{n-1} + b, \qquad n = 1, 2, \ldots$$

Manuscript received September 11, 2001; revised August 13, 2002. The work of I. E. Shparlinski and A. Winterhof was supported in part by the Institute for Mathematical Sciences of the National University of Singapore. The work of I. E. Shparlinski was also supported by the Australian Research Council. The work of J. Gutierrez was supported by Spain Grant Project BFM2001-1294.

J. Gutierrez is with the Faculty of Science, University of Cantabria, E-39071 Santander, Spain (e-mail: jaime@matesco.unican.es).

I. E. Shparlinski is with the Department of Computing, Macquarie University, NSW 2109, Australia (e-mail: igor@comp.mq.edu.au).

A. Winterhof is with the Department of Mathematics, National University of Singapore, 117543 Singapore, on leave from the Institute of Discrete Mathematics, Austrian Academy of Sciences, A-1010 Vienna, Austria (e-mail: arne.winterhof@oeaw.ac.at).

Communicated by N. I. Koblitz, Associate Editor for Complexity and Cryptography.

Digital Object Identifier 10.1109/TIT.2002.806144

with some $a \in \mathbb{F}_q^*$, $b, z_0 \in \mathbb{F}_q$, is based on the fact that $\mathcal{L}(\mathcal{Z}, N) \leq 2$ for such sequences. See [15], [16] for an outline of predictability results for such generators. In literature on pseudorandom number generators, this type of generator is usually defined over residue class rings and called linear congruential generator. In fact, the very low linear complexity of this generator has turned out to be undesirable for more traditional applications in Monte Carlo methods as well (see surveys given in [4], [19], [20], [22], [27]). A low linear complexity is equivalent to a coarse lattice structure which is considered an undesirable feature in many applications. Thus, both areas, cryptography and Monte Carlo methods, have stimulated studying *nonlinear generators*

$$x_n := f(x_{n-1}), \qquad n = 1, 2, \ldots \tag{1}$$

with some *initial value* $x_0 \in \mathbb{F}_q$, where f: $\mathbb{F}_q \to \mathbb{F}_q$ is some fixed function (which should admit an efficient evaluation algorithm). We prove a lower bound on the linear complexity profile of a general nonlinear sequence defined by (1) for certain nonlinear polynomials $f(X) \in \mathbb{F}_q[X]$. One of such frequently used generators of this type is the *power generator* which produces sequences $\mathcal{R} := (r_n)_{n=0}^{\infty}$ satisfying the relation

$$r_n := r_{n-1}^e, \qquad n = 1, 2, \ldots$$

with an initial value $r_0 := \vartheta \in \mathbb{F}_q^*$ and an *exponent* $e \geq 2$ (see [1], [3], [16], [35]). We remark that in cryptography this generator is used with *RSA moduli* which are products of two large primes. One can easily verify that

$$r_n = \vartheta^{e^n}, \qquad n = 0, 1, \ldots.$$

Lower bounds on the linear complexity and the linear complexity profile of the power generator have recently been obtained in [12], [34]. Results about the period can be found in [9] and results about the distribution of the power generator modulo a prime follow from the bounds of exponential sums [6], the results for RSA moduli are given in [10], finally, the results for prime power moduli are given in [7] and for arbitrary composite moduli in [8].

One more example of a frequently used nonlinear generator is given by the *inversive generator* which produces sequences $\mathcal{V} := (v_n)_{n=0}^{\infty}$ satisfying the relation

$$v_n := \psi(v_{n-1}), \qquad n = 1, 2, \ldots \tag{2}$$

where

$$\psi(v) := \begin{cases} av^{-1} + b, & \text{if } v \neq 0 \\ b, & \text{if } v = 0 \end{cases}$$

with some coefficients $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$. Recent results about the period and distribution of this (and related) generators can be found in the survey [27] (see also the original papers [11], [13], [14], [23]–[26], [28]–[31]). In particular, if q is a prime then the discrepancy of the fractional parts $\{v_n/q\}$, $n = 1, \ldots, N$ is $O(N^{-1/2}q^{1/4}\log q)$, see [26]. The results of [5], [32] imply that if the period t of the inversive generator takes its largest possible value $t = q$ then the linear complexity is at least $\mathcal{L}(\mathcal{V}) \geq \lceil q/2 \rceil$. On the other hand, neither the case of arbitrary period t nor the linear complexity profile of this generator has been studied. Here, we supplement lower bounds for the linear complexity profile for arbitrary period t.

Finally, we introduce one more nonlinear generator which we call *quadratic exponential generator* which has not been considered in literature known to the authors so far and which we believe deserves a more detailed study. Given an element $\vartheta \in \mathbb{F}_q^*$ we consider the sequence $\mathcal{U} := (u_n)_{n=0}^{\infty}$ where

$$u_n := \vartheta^{n^2}, \qquad n = 0, 1, \ldots. \tag{3}$$

The period of this sequence is at least $\tau/2$ where τ is the multiplicative order of ϑ. Also, the bound of exponential sums from [6] shows that the sequence $\mathcal{U}$ is asymptotically uniformly distributed. In particular, if q is prime then the discrepancy of the fractional parts $\{u_n/q\}$, $n = 1, \ldots, t$ is $O(\tau^{-1/4}q^{1/8+\varepsilon})$ for any $\varepsilon > 0$ (see [6, Theorem 6]). For the same generator defined modulo a composite integer one can use the corresponding results from [8]. In fact, expression (3) is convenient for studying the sequence $\mathcal{U}$ while for the actual generation of its elements one should probably use the recurrence formulas

$$w_n := \lambda w_{n-1}, \quad u_n := u_{n-1}w_{n-1}, \qquad n = 1, 2, \ldots$$

where $\lambda := \vartheta^2$, $u_0 := 1$, and $w_0 := \vartheta$.

Thus, this sequence could be faster to generate than the sequences $\mathcal{V} := (v_n)_{n=0}^{\infty}$ produced by the inversive generator (2). We prove a lower bound on $\mathcal{L}(\mathcal{V}, N)$.

We recall that the *nonlinear complexity profile* $\mathcal{NL}_m(\mathcal{S}, N)$ of an infinite sequence $\mathcal{S} := (s_n)_{n=0}^{\infty}$ of elements of $\mathbb{F}_q$ is the function which for every integer $N \geq 2$ is defined as the least order k of a polynomial recurrence relation

$$s_{n+k} = \Psi(s_{n+k-1}, \ldots, s_n), \qquad 0 \leq n \leq N - k - 1$$

with a polynomial $\Psi(\lambda_1, \ldots, \lambda_k)$ over $\mathbb{F}_q$ of total degree at most m, which is satisfied by this sequence. Note that generally speaking $\mathcal{NL}_1(\mathcal{S}, N) \neq \mathcal{L}(\mathcal{S}, N)$ because in the definition of $\mathcal{L}(\mathcal{S}, N)$ one can use only homogeneous linear polynomials. Obviously, we have

$$\mathcal{L}(\mathcal{S}, N) \geq \mathcal{NL}_1(\mathcal{S}, N) \geq \mathcal{NL}_2(\mathcal{S}, N) \geq \cdots.$$

We present our results on the linear complexity profile of the above sequences in a more general form as lower bounds on the nonlinear complexity profile whenever possible.

In several cases, our lower bounds on the linear and nonlinear complexity profile are very tight and close to the best possible.

II. Preparations

We need the following result which extends [14, Lemma 1] and which could be of independent interest.

Let us consider the following sequence of rational functions over $\mathbb{F}_q$:

$$H_0(X) := X, \quad H_i(X) := H_{i-1}(aX^{-1} + b), \qquad i = 1, 2, \ldots \tag{4}$$

with some coefficients $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$. It is obvious that this sequence is purely periodic. Denote by T the smallest period. We observe that $H_i(X) = f_i(X)/g_i(X)$ are nonconstant rational functions where $f_i, g_i \in \mathbb{F}_q[X]$ with

$$\max\{\deg(f_i), \deg(g_i)\} = 1$$

that is, $\gcd(f_i, g_i) = 1$.

Lemma 1: For all integers i and k with $0 \leq i < k < T$ and all polynomials $\Psi \in \mathbb{F}_q[X_0, \ldots, X_i]$ and $G \in \mathbb{F}_q[X]$ with $\gcd(G, g_k) = 1$ we have

$$G(X)H_k(X) \neq \Psi(H_i(X), \ldots, H_0(X)).$$

Proof: By induction we see that if $g_i(X) := c_iX + d_i$ then

$$f_i(X) = (bc_i + d_i)X + ac_i. \tag{5}$$

In particular, if $c_i = 0$ then $H_i(X) = X$ and $i = 0$ or $i \geq T$. It also follows that for all integers j_1 and j_2 with $0 \leq j_1 < j_2 < T$, we have

$$\gcd(g_{j_1}, g_{j_2}) = 1.$$

If $\gcd(g_{j_1}, g_{j_2}) > 1$ for some $0 \leq j_1 < j_2 < T$ then

$$g_{j_1}(X) = kg_{j_2}(X), \qquad \text{with } k \in \mathbb{F}_q^*,$$

$f_{j_1}(X) = kf_{j_2}(X)$ by (5), and, thus, $H_{j_1}(X) = H_{j_2}(X)$. This implies

$$H_{j_1+1}(X) = H_{j_1}(aX^{-1}+b) = H_{j_2}(aX^{-1}+b) = H_{j_2+1}(X)$$

and iteratively

$$H_{j_1+T-j_2}(X) = H_T(X) = H_0(X)$$

in contradiction to $0 \leq j_1 + T - j_2 < T$.

For $i = 0$, an equation of the form

$$G(X)H_k(X) = \Psi(H_0(X)) = \Psi(X)$$

implies

$$G(X)f_k(X) = \Psi(X)g_k(X).$$

Since $\gcd(G, g_k) = 1$, the irreducible polynomial $g_k(X)$ divides $f_k(X)$. Since $H_k(X)$ is nonconstant and

$$\max\{\deg(f_k), \deg(g_k)\} = 1$$

we get $\deg(f_k) = 1$ and $\deg(g_k) = 0$ in contradiction to $c_k \neq 0$. For $i > 0$ we have an equation of the form

$$G(X)H_k(X) = \Psi(H_i(X), \ldots, H_0(X)).$$

Clearing the denominators, we get an equation of the form

$$g_i(X)^{s_i} \cdots g_1(X)^{s_1}G(X)f_k(X) = g_k(X)\Psi_0(X)$$

where $s_1, \ldots, s_i$ are nonnegative integers and $\Psi_0(X)$ is a nonzero univariate polynomial. The irreducible factor $g_k(X)$ on the right-hand side of the preceding equality does not appear on the left-hand side because

$$\gcd(f_k, g_k) = \gcd(G, g_k) = \gcd(g_j, g_k) = 1$$

for all $1 \le j \le i < k < T$. This contradiction finishes the proof. □

We also need the following result, which is [2, Theorem 10].

Lemma 2: Let $G(U, V) \in \mathbb{F}_q[U, V]$ be a polynomial of degree $n := \deg G$, not identically zero, such that

$$G(g^x, g^{x^2}) = 0, \qquad x \in S$$

for a set $S \subseteq \{0, \ldots, H-1\}$ and a primitive element g of $\mathbb{F}_q$. Then, there is an absolute constant $c > 0$ such that the bound

$$n \ge c|S|^{3/2}/H$$

holds.

III. Main Results

We start with a lower bound on the nonlinear complexity profile of the inversive generator.

Theorem 1: The nonlinear complexity profile of a sequence $\mathcal{V} := (v_n)_{n=0}^{\infty}$ produced by the inversive generator (2), which is purely periodic with period t, satisfies

$$\mathcal{NL}_m(\mathcal{V}, N) \ge \min\left\{\left\lceil\frac{N-1}{m+2}\right\rceil, \left\lceil\frac{t-1}{m+1}\right\rceil\right\}.$$

Proof: Let k be the least positive integer with

$$v_{n+k} = \Psi(v_{n+k-1}, \ldots, v_n), \qquad 0 \le n \le N-k-1$$

with a polynomial $\Psi(\lambda_1, \ldots, \lambda_k)$ over $\mathbb{F}_q$ of total degree at most m. Then

$$\psi^k(v_n) = \Psi(\psi^{k-1}(v_n), \ldots, \psi^0(v_n)),\ 0 \le n < N-k. \quad (6)$$

For $j \ge 0$, let denote by E_j the set of poles of the rational functions $H_0, \ldots, H_j$ defined by (4). Thus, $|E_j| \le j$. By induction we have

$$\psi^j(x) = H_j(x), \qquad \text{for all } x \in \mathbb{F}_q \setminus E_j. \quad (7)$$

Obviously, $T \ge t$, where as before T is the smallest period of the sequence (H_i). We may suppose that $k < t \le T$. Then, by Lemma 1

$$H(X) = -H_k(X) + \Psi(H_{k-1}(X), \ldots, H_0(X))$$

is a nonzero rational function. We see that

$$H_i(X) = f_i(X)/g_i(X)$$

are nonconstant rational functions, where

$$f_i(X), g_i(X) \in \mathbb{F}_q[X] \quad \text{with } \max\{\deg(f_i), \deg(g_i)\} = 1.$$

Hence, $H(X) = F(X)/G(X)$ with $F(X), G(X) \in \mathbb{F}_q[X]$ and $\deg(F) \le mk+1$. On the other hand, by (6) and (7), the polynomial $F(X)$ has at least $\min\{N-2k, t-k\}$ zeros, namely, all v_n, $0 \le n \le N-k-1$, with $v_n \notin E_k$, and, thus,

$$\deg(F) \ge \min\{N-2k, t-k\}.$$

Hence, we have $mk+1 \ge \min\{N-2k, t-k\}$ from which the result follows. □

Now we prove a lower bound on the linear complexity profile of the quadratic exponential generator.

Theorem 2: The linear complexity profile of a sequence $\mathcal{U} := (u_n)_{n=0}^{\infty}$ produced by the quadratic exponential generator (3), which is purely periodic with period t, satisfies the inequality

$$\mathcal{L}(\mathcal{U}, N) \ge \left\lceil\frac{\min\{N, t\}}{2}\right\rceil.$$

Proof: Let k be the least positive integer with

$$u_{n+k} = a_{k-1}u_{n+k-1} + \cdots + a_0 u_n, \qquad 0 \le n \le N-k-1$$

and verify that

$$u_{n+l} = \vartheta^{l^2} u_n \vartheta^{2nl}, \qquad l, n \ge 0. \quad (8)$$

Then with $a_k := -1$ and $b_l := \vartheta^{l^2} a_l$ for $0 \le l \le k$ we have

$$b_k \vartheta^{2nk} + \cdots + b_0 = 0, \qquad 0 \le n \le N-k-1.$$

Since for even values of τ the elements $1, \vartheta^2, \vartheta^4, \ldots, \vartheta^{\tau-2}$ and for odd values of τ the elements $1, \vartheta^2, \vartheta^4, \ldots, \vartheta^{2\tau-2}$ are distinct, the polynomial $F(X) := b_k X^k + \cdots + b_0$ of degree k has at least $\min\{N-k, \tau/2\}$ zeros if τ is even and at least $\min\{N-k, \tau\}$ zeros if τ is odd. Since $t \le \tau$, we get the result. □

Lemma 2 implies a lower bound on the nonlinear complexity of the quadratic exponential generator (3).

Theorem 3: The nonlinear complexity profile of a sequence $\mathcal{U} := (u_n)_{n=0}^{\infty}$ produced by the quadratic exponential generator (3), which is purely periodic with period t, satisfies the inequality

$$\mathcal{NL}_m(\mathcal{U}, N) \ge C\frac{\min\{N^{1/2}, t^{1/2}\}t}{m(q-1)}$$

with an absolute constant $C > 0$.

Proof: Let k be the least positive integer with

$$u_{n+k} = \Psi(u_{n+k-1}, \ldots, u_n), \qquad 0 \le n \le N-k-1$$

with a polynomial $\Psi(\lambda_1, \ldots, \lambda_k)$ over $\mathbb{F}_q$ of total degree at most m. By (8) we have

$$\vartheta^{k^2} u_n \vartheta^{2nk} = \Psi(\vartheta^{(k-1)^2} u_n \vartheta^{2n(k-1)}, \ldots, u_n)$$

$0 \le n \le N-k-1$, and the polynomial

$$F(X, Y) := -\vartheta^{k^2} Y X^{2k} + \Psi(\vartheta^{(k-1)^2} Y X^{2(k-1)}, \ldots, Y)$$

satisfies

$$F(\vartheta^n, \vartheta^{n^2}) = 0, \qquad 0 \le n \le \min\{N-k-1, t-1\}.$$

If $\deg(\Psi) \geq 2$, then the polynomial $F(X, Y)$ is nonzero since $\deg_Y(F) = \deg(\Psi)$. If $\deg(\Psi) = 1$, then the polynomial $F(X, Y)$ is nonzero since $\deg_X(F) = 2k$. As before, we denote by τ the multiplicative order of ϑ. Let $r := (q-1)/\tau$. Then $\vartheta = g^r$ for some primitive element g of $\mathbb{F}_q$ and we obtain

$$G(g^n, g^{n^2}) = 0, \qquad 0 \leq n \leq \min\{N-k-1, t-1\}$$

where $G(X, Y) = F(X^r, Y^r)$. Now Lemma 2 implies

$$\deg(G) \geq c_0 \min\{N-k, t\}^{1/2}$$

with an absolute constant $c_0 > 0$. Since otherwise the result is trivial we may suppose $k \leq N/2$. Then

$$\deg(G) \leq r \max\{(2k-1)m, 2k+1\}$$

implies

$$c_0 \left(\frac{\min\{N,t\}}{2}\right)^{1/2} \leq c_0 \min\{N/2, t\}^{1/2} \leq (q-1)3km/\tau \leq (q-1)3km/t,$$

where we have used $t \leq \tau$. □

In particular, if ϑ is a primitive element (which is probably the most interesting case anyway) then

$$\mathcal{NL}_m(\mathcal{U}, N) \geq Cm^{-1} \min\{N^{1/2}, t^{1/2}\}.$$

In fact, the same method applies to nonlinear generators (1) with an arbitrary nonlinear polynomial $f \in \mathbb{F}_q[X]$ yielding much weaker results, however.

Theorem 4: The nonlinear complexity profile of a sequence $\mathcal{X} := (x_n)_{n=0}^{\infty}$ produced by a nonlinear generator (1) with a polynomial $f \in \mathbb{F}_q[X]$ of degree $d \geq 2$, which is purely periodic with period t, satisfies

$$\mathcal{NL}_{d-1}(\mathcal{X}, N) \geq \min\{\lceil \log_d (N - \lfloor \log_d N \rfloor) \rceil, \lceil \log_d t \rceil\}.$$

Proof: Let us consider the following sequence of polynomials over $\mathbb{F}_q$:

$$F_0(X) := X, \quad F_i(X) := F_{i-1}(f(X)), \quad i = 1, 2, \ldots .$$

It is clear that $\deg(F_i) = d^i$ for every $i = 1, 2, \ldots$. Then $x_{n+j} = F_j(x_n)$ for any integers $n, j \geq 0$. Let k be the least positive integer with

$$x_{n+k} = \Psi(x_{n+k-1}, \ldots, x_n), \qquad 0 \leq n \leq N-k-1$$

with a polynomial Ψ over $\mathbb{F}_q$ of total degree at most $d-1$ or equivalently

$$-F_k(x_n) + \Psi(F_{k-1}(x_n), \ldots, F_0(x_n)) = 0, \qquad 0 \leq n \leq N-k-1.$$

Hence, the polynomial

$$F(X) := -F_k(X) + \Psi(F_{k-1}(X), \ldots, F_0(X))$$

has degree d^k (we have $\deg(\Psi) < d$) and at least $\min\{N-k, t\}$ zeros. Thus, $d^k \geq \min\{N-k, t\}$. Since otherwise the result is trivial we may suppose $k \leq \lfloor \log_d N \rfloor$ and get

$$d^k \geq \min\{N - \lfloor \log_d N \rfloor, t\}$$

and the theorem follows. □

IV. Remarks

The dramatic difference in the strength of Theorems 1 and 4 is explained by the exponential growth of the degrees of the polynomials F_i, while H_i remains of the same shape for all $i = 1, 2, \ldots$. The same effect can be observed if one compares the results on the distribution of the inversive generator [14], [24]–[26], [28]–[31] and the polynomial generator [11], [13], [23]. On the other hand, there is no reason to expect that the polynomial generator exhibits less random behavior than the inversive generator and improving Theorem 4 as well as the results of [11], [13], [23] is an important open problem. However, in the particular case that q is a prime and $t = q$ a recent result of Meidl and the third author [17, Theorem 3] yields

$$\mathcal{L}(\mathcal{X}, N) \geq \min\left\{N - q + 1, \left\lceil \frac{q}{d} \right\rceil\right\}.$$

(Compare also [23, Theorem 5].) We also note that

$$\mathcal{NL}_m(\mathcal{X}, N) = 1, \qquad \text{for } m \geq d$$

thus, Theorem 4 covers all nontrivial cases (although the bound is rather weak). We should also remark that in Theorems 1 and 4, the same lower bounds hold also if Ψ belongs to the wider class of polynomials having degree at most m in each variable.

We have applied Lemma 2 in a very special situation (and to a polynomial of a special form). It is possible that in this case a stronger version of Lemma 2 is possible which would immediately improve the result of Theorem 3.

We remark that the constant c in Lemma 2, and, thus, the constant C in Theorem 3 can easily be evaluated explicitly.

On the other hand, we remark that our method does not apply to generators of higher order

$$x_n := f(x_{n-1}, \ldots, x_{n-m}), \qquad n = m, m+1, \ldots$$

whose distribution has been considered in [11], [13]. Obtaining a lower bound on their linear complexity is an interesting question as well.

Finally, we remark that Lemma 1 holds for similar iterations of rational functions over any field. In fact, the sequence (H_i) need not be periodic. In this case, Lemma 1 holds for any $0 < i < k$.

Acknowledgment

Parts of this work were written while I. E. Shparlinski and A. Winterhof were visiting the National University of Singapore. They wish to thank the Institute for Mathematical Sciences for hospitality.

References

[1] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM J. Comput.*, vol. 15, pp. 364–383, 1986.

[2] D. Coppersmith and I. E. Shparlinski, "On polynomial approximation of the discrete logarithm and the Diffie–Hellman mapping," *J. Cryptol.*, vol. 13, pp. 339–360, 2000.

[3] T. W. Cusick, C. Ding, and A. Renvall, *Stream Ciphers and Number Theory*. Amsterdam, The Netherlands: North-Holland, 1998.

[4] J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl, "A survey of quadratic and inversive congruential pseudorandom numbers," in *Monte Carlo and Quasi-Monte Carlo Methods (Lecture Notes in Statistics)*. New York: Springer-Verlag, 1996, vol. 127, pp. 66–97.

[5] M. Flahive and H. Niederreiter, "On inversive congruential generators for pseudorandom numbers," in *Finite Fields, Coding Theory, and Advances in Communications and Computing (Lecture Notes in Pure and Appl. Math.)*. New York: Dekker, 1993, 141, pp. 75–80.

[6] J. B. Friedlander, J. Hansen, and I. E. Shparlinski, "On character sums with exponential functions," *Mathematika*, vol. vol. 47, pp. 75–85, 2000.

[7] ——, "On the distribution of the power generator modulo a prime power," in *Proc. DIMACS Workshop Unusual Applications of Number Theory*, 2000, to be published.

[8] J. B. Friedlander, S. V. Konyagin, and I. E. Shparlinski, "Some doubly exponential sums over $\mathbb{Z}_m$," Acta Arith., to be published.

[9] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, "Period of the power generator and small values of Carmichael's function," *Math. Comput.*, vol. 70, pp. 1591–1605, 2001.

[10] J. B. Friedlander and I. E. Shparlinski, "On the distribution of the power generator," *Math. Comput.*, vol. 70, pp. 1575–1589, 2001.

[11] F. Griffin, H. Niederreiter, and I. E. Shparlinski, "On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders," in *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1999, vol. 1719, pp. 87–93.

[12] F. Griffin and I. E. Shparlinski, "On the linear complexity profile of the power generator," *IEEE Trans. Inform. Theory*, vol. 46, pp. 2159–2162, Sept. 2000.

[13] J. Gutierrez and D. Gomez-Perez, "Iterations of multivariate polynomials and discrepancy of pseudorandom numbers," in *Proc. 14th Symp. Applied Algebra Algebraic Alg. Error-Correcting Codes (Lecture Notes in Computer Science)*. Berlin, Germany: Springer-Verlag, 2001, vol. 2227, pp. 192–199.

[14] J. Gutierrez, H. Niederreiter, and I. E. Shparlinski, "On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period," *Monatsh. Math.*, vol. 129, pp. 31–36, 2000.

[15] A. Joux and J. Stern, "Lattice reduction: A toolbox for the cryptanalyst," *J. Cryptol.*, vol. 11, pp. 161–185, 1998.

[16] J. C. Lagarias, "Pseudorandom number generators in cryptography and number theory," in *Cryptology and Computational Number Theory (Proc. Symp. Appl. Math.)*. Providence, RI: Amer. Math. Soc., 1989, pp. 115–143.

[17] W. Meidl and A. Winterhof, "On the linear complexity profile of explicit nonlinear pseudorandom numbers," *Inform. Processing Lett.*, to be published.

[18] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC, 1997.

[19] H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*. Philadelphia, PA: SIAM, 1992.

[20] ——, "New developments in uniform pseudorandom number and vector generation," in *Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing (Lecture Notes in Statistics)*. New York: Springer-Verlag, 1994, pp. 87–120.

[21] ——, "Some computable complexity measures for binary sequences," in *Proc. Int. Conf. Sequences and Their Applications (SETA'98), Singapore*. London: Springer, 1999, pp. 67–78.

[22] ——, "Design and analysis of nonlinear pseudorandom number generators," in *Monte Carlo Simulation*. Rotterdam, The Netherlands: A. A. Balkema, 2001, pp. 3–9.

[23] H. Niederreiter and I. E. Shparlinski, "On the distribution and lattice structure of nonlinear congruential pseudorandom numbers," *Finite Fields Their Appl.*, vol. 5, pp. 246–253, 1999.

[24] ——, "Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus," *Acta Arith.*, vol. 92, pp. 89–98, 2000.

[25] ——, "On the distribution of pseudorandom numbers and vectors generated by inversive methods," *Appl. Algebra Engrg. Comm. Comput.*, vol. 10, pp. 189–202, 2000.

[26] ——, "On the distribution of inversive congruential pseudorandom numbers in parts of the period," *Math. Comput.*, vol. 70, pp. 1569–1574, 2001.

[27] ——, "Recent advances in the theory of nonlinear pseudorandom number generators," in *Proc. Conf. Monte Carlo and Quasi-Monte Carlo Methods (2000)*. Berlin, Germany: Springer-Verlag, 2002, pp. 86–102.

[28] ——, "On the average distribution of inversive pseudorandom numbers," *Finite Fields and Their Appl.*, vol. 8, pp. 491–503, 2002.

[29] H. Niederreiter and A. Winterhof, "Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number," *Acta Arith.*, vol. 93, pp. 387–399, 2000.

[30] ——, "On the distribution of compound inversive congruential pseudorandom numbers," *Monatsh. Math.*, vol. 132, pp. 35–48, 2001.

[31] ——, "On a new class of inversive pseudorandom numbers for parallelized simulation methods," *Period. Math. Hungar.*, vol. 42, pp. 77–87, 2001.

[32] ——, "Lattice structure and linear complexity of nonlinear pseudorandom numbers," *Appl. Algebra in Eng. Commun. and Computing*, vol. 13, pp. 319–326, 2003.

[33] R. A. Rueppel, "Stream ciphers," in *Contemporary Cryptology: The Science of Information Integrity*. New York: IEEE, 1992, pp. 65–134.

[34] I. E. Shparlinski, "On the linear complexity of the power generator," *Des. Codes Cryptogr.*, vol. 23, pp. 5–10, 2001.

[35] D. R. Stinson, *Cryptography: Theory and Practice*. Boca Raton, FL: CRC, 1995.