Pseudorandom sequences constructed by the power generator

Katalin Gyarmati*

Abstract

We study the pseudorandom properties of the power generator (which includes as special cases the RSA generator and the Blum-Blum-Shub generator). In order to estimate the pseudorandom measures character sums with exponential functions are used.

1 Introduction

We will study the pseudorandom properties of the power generator by the following measures of pseudorandomness of finite binary sequences introduced by C. Mauduit and A. Sárközy [16, pp. 367-370].

For a binary sequence

$$E_N = \{e_1, \dots, e_N\} \in \{-1, +1\}^N,$$

**2000 Mathematics Subject Classification:* 11K45.

Key words and phrases: pseudorandom, power generator, Blum-Blum-Shub generator.

Research partially supported by Hungarian National Foundation for Scientific Research, Grants T043623, T043631 and T049693.

write

$$U(E_N, t, a, b) = \sum_{j=1}^{t} e_{a+jb}$$

and, for $D = (d_1, \ldots, d_\ell)$ with non-negative integers $0 \le d_1 < \cdots < d_\ell$,

$$V(E_N, M, D) = \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_\ell}.$$

Finally, for $X = \{x_1, \ldots, x_\ell\} \in \{-1, +1\}^\ell$ write

$$Z(E_N, M, X) = |\{n : 0 \le n < M,\ \{e_{n+1}, e_{n+2}, \ldots, e_{n+\ell}\} = X\}|.$$

Then the *well-distribution measure of* E_N is defined as

$$W(E_N) = \max_{a,b,t} |U(E_N, t, a, b)| = \max_{a,b,t} \left| \sum_{j=1}^{t} e_{a+jb} \right|,$$

where the maximum is taken over all a, b, t such that $a \in \mathbb{Z}$, $b, t \in \mathbb{N}$ and $1 \le a + b \le a + tb \le N$, while the *correlation measure of order* ℓ *of* E_N is defined as

$$C_\ell(E_N) = \max_{M,D} |V(E_N, M, D)| = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} \ldots e_{n+d_\ell} \right|,$$

where the maximum is taken over all $D = (d_1, \ldots, d_\ell)$ and M such that $0 \le d_1 < \cdots < d_\ell < M + d_\ell \le N$. The *normality measure of order* ℓ is defined as

$$N_\ell(E_N) = \max_{M,X} \left| Z(E_N, M, X) - M/2^\ell \right|,$$

where the maximum is taken over all $X = \{x_1, \ldots, x_\ell\} \in \{-1, +1\}^\ell$, and M such that $0 < M \le N - \ell + 1$.

The *power generator* is defined by the following:

Let $k \geq 2, m \geq 1$ and ϑ be integers such that $(\vartheta, m) = 1$. Define the sequence $\{u_n\}$ by the recurrence relation

$$u_n \equiv u_{n-1}^k \pmod{m}, \quad 0 \leq u_n \leq m-1, \quad n = 1, 2, \ldots \tag{1}$$

with the initial value $u_0 = \vartheta$.

The power generator has many applications in cryptography, see [1], [4], [14], [21]. In the two special cases $(k, \varphi(m)) = 1$ (where $\varphi(m)$ is the Euler function) and $k = 2$ this sequence is known as the *RSA generator* and as the *Blum-Blum-Shub generator*, respectively.

Although various properties of the power generator have been studied in a number of papers, see [1], [3], [5], [4], [6], [12], [13], [14], [17], [21], few unconditional results are known: Clearly, the sequence (1) becomes periodic, possible values of the period are studied in [10]. Cusick [5] proved that the rightmost bit of the Blum-Blum-Shub generator assumes values 0 and 1 almost equally often, provided that the period is large enough. Friedlander, Lieman and Shparlinski [8], proved that if the period of the RSA generator is large enough, then the elements of the sequence is uniformly distributed modulo m and a positive proportion of the rightmost and leftmost bits is uniformly distributed. Lower bounds on the linear complexity of the power generator have been given in [12], [20]. The results of this paper will be also unconditional.

Notation 1 *Let p be a prime, $\vartheta \in \mathbb{F}_p^*$ be an element. Define the sequence u_n by* (1) *with a prime modulus p in place of m (then the value of u_n is fixed in the interval $[0, p-1]$). Clearly the multiplicative order of $u_n \equiv \vartheta^{k^n} \pmod{p}$*

is non-increasing as $n \to \infty$. Let n_0 denote the smallest positive integer such that for $n \geq n_0$ the multiplicative order of

$$u_n \equiv \vartheta^{k^n} \pmod p$$

is the same number: t. Then

$$(k,t) = 1. \tag{2}$$

Denote by T the multiplicative order of k modulo t.

Throughout the paper we will use these notations: $p, \vartheta, t, k, T, n_0$ and the sequence $\{u_n\}$ will be as it described here. Clearly the sequence

$$u_{n_0}, u_{n_0+1}, u_{n_0+2}, \dots$$

is purely periodic with the period T.

We convert the sequence $\{u_n\}$ to a binary sequence by the parity of its last bit:

Construction 1 *Define the sequence $E_N = \{e_1, \dots, e_N\}$ by*

$$e_n = \begin{cases} +1 & \textit{if } u_n \textit{ is even,} \\ -1 & \textit{if } u_n \textit{ is odd.} \end{cases} \tag{3}$$

In this paper we will study the pseudorandom properties of the sequence E_N. First we will give upper bounds for the well-distribution measure and the normality measure of order ℓ. In Theorems 1 and 2 the length of the sequence is T (defined in Notation 1), which is the period of the power generator.

Theorem 1

$$W(E_T) \ll p^{7/8} (\log p)^2.$$

For the normality measure we have

Theorem 2 *For all $\varepsilon > 1/4$ we have*

$$N_\ell(E_T) \ll k^{\varepsilon(\ell-1)} p^{7/8} (\log p)^{\ell+1},$$

where the implied constant depends only on ε.

The proof of Theorems 1 and 2 will be based on extensions of theorems of Friedlander, Hansen and Shparlinski in [7] and [9].

Until very recently only the short-range correlation ($\sum_n e_{n+d_1} e_{n+d_2} \dots e_{n+d_\ell}$ for small d_i's) could be handled. By using Bourgain [2] new result, we will be able to handle the long-range correlation as well, which was out of reach until now. Thus here all the three pseudorandom measures of the power generator are studied, and this *unconditionally* proves that the pseudorandom generator has strong pseudorandom properties.

We will estimate the correlation measure E_N defined by (3) for some $N < T$, so the length of the sequence will be smaller than the period of the power generator following from certain technical conditions in Bourgain [2] theorem. The exact value of the length N is defined in Theorem 3.

Theorem 3 *Suppose that $\ell^2 < p$. Denote by $N = N(\vartheta, k, \delta)$ the largest positive integer such that for all $1 \le i < j \le 2N$ we have*

$$(k^j - k^i, t) \le t p^{-\delta}. \tag{4}$$

Then there exists a constant $\varepsilon(\ell, \delta) = \varepsilon > 0$ depending on ℓ and δ such that for the sequence E_N of length N defined by (4) we have

$$C_\ell(E_N) \le p^{1-\varepsilon}. \tag{5}$$

The proof will be based on a recent result of Bourgain [2]. The upper bound (5) for the correlation measure is non-trivial if N, the length of the sequence (defined by (4)) is large. The following corollary studies a simple case when N is indeed large.

Corollary 1 *Let $p-1=2q$, where p and q are odd primes, ϑ be primitive root modulo p, and k be primitive root modulo q. Then for the sequence $E_{(p-3)/4}$ of length $(p-3)/4$ defined by (3) we have*

$$C_\ell(E_{(p-3)/4}) \le p^{1-\varepsilon},$$

for an absolute constant $\varepsilon > 0$.

We remark that (3) is not the only way to define a binary sequence $\{e_n\}$ from the sequence $\{u_n\}$. For example, Theorems 1,2,3 also hold for the sequence $E_N = \{e_1, \dots, e_N\}$ defined by

$$e_n = \begin{cases} +1 & \text{if } 0 \le u_n < p/2, \\ -1 & \text{if } p/2 \le u_n < p. \end{cases}$$

In Section 2 we will estimate certain related exponential sums and the proofs of Theorems 1,2 and 3 will be completed in Section 3.

In this paper we study the prime modulus case, i.e., $u_n \equiv u_{n-1} \pmod p$, where p is a prime. These results can be extended for the composite modulus case by using exponential sums in [9]. Here I did not carry out the proof, since the computations will be similar but more difficult. However, it may happen that the power generator has stronger pseudorandom properties in the prime modulus case than in the composite modulus case. This situation indeed happens for the Legendre symbol sequence

$$E_m = \left\{ \left(\frac{p(1)}{m} \right), \left(\frac{p(2)}{m} \right), \dots, \left(\frac{p(m)}{m} \right) \right\}, \qquad f(x) \in \mathbb{Z}_m.$$

Goubin, Mauduit and Sárközy [11] proved that under certain conditions on the polynomial $p(x)$, this sequence has strong pseudorandom properties if m is a prime: $W(E_m), C_\ell(E_m) \ll m^{1/2} \log m$. If m is composite Rivat and Sárközy [18] proved that for all polynomial $p(x)$ we have $C_4(E_m) \gg m$.

Throughout the paper we write $e_p(a) = \exp(2\pi i \frac{a}{p})$.

2 Exponential sums

J. Friedlander, J. Hansen and I. Shparlinski gave an upper bound for the sum $\sum_{x=1}^{T} e_p(a\vartheta^{k^x})$. Later Friedlander and Shparlinski [9] extended this result to the sum $\sum_{x=1}^{T} e_p(a_1\vartheta^{k^x} + a_2\vartheta^{k^{x+1}} \cdots + a_r\vartheta^{k^{x+r-1}})$. Here we will study the extension this result to general powers and incomplete sums. First we will study the incomplete sum analog of the result in [9].

Lemma 1 *Let t, T be as in Notation 1. Let $\varepsilon_1 > 1/4$ and suppose that $t > p^{1/2+\delta}$ for a constant $\delta > 0$. Let $a_i \in \mathbb{F}_p$, $L, M \in \mathbb{N}$ with $L \le T$. Then*

$$\sum_{x=M+1}^{M+L} e_p(a_1\vartheta^{k^x} + a_2\vartheta^{k^{x+1}} + \cdots + a_r\vartheta^{k^{x+r-1}}) \ll k^{\varepsilon_1(r-1)} T^{1/4} t^{1/2} p^{1/8} \log p,$$

where the implied constant depends only on δ and ε_1. In the special case $r = 1$ we obtain

$$\sum_{x=M+1}^{M+L} e_p(a_1\vartheta^{k^x}) \ll T^{1/4} t^{1/2} p^{1/8} \log p,$$

where the implied constant depends only on δ.

Using J. Bourgain's result [2], we will prove:

Lemma 2 *For* $1 \le i \le r$ *let* $h_i \in \mathbb{Z}_{p-1}$, $\vartheta_i = \vartheta^{h_i}$ *and* $a_i \in \mathbb{F}_p^*$ *where* $(h_1, \dots, h_r, p-1) = 1$ *also holds. Then the sequence*

$$\{a_1 \vartheta_1^{k^x} + \cdots + a_r \vartheta_r^{k^x}\}$$

becomes periodic with period T *(where* T *is defined in Notation 1). Denote by*

$$N(\vartheta_1, \dots, \vartheta_r, k, \delta) = N$$

the largest positive integer N *such that* $N \le T$*, for all* $0 \le i \le N$, $1 \le j \le r$

$$(k^i h_j, t) \le t p^{-\delta}, \tag{6}$$

and for all pairs $\{i_1, j_1\}, \{i_2, j_2\}$ *with* $1 \le i_1, i_2 \le N$, $1 \le j_1 \le j_2 \le r$ *we have*

$$(k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t) \le t p^{-\delta} \quad \text{or} \quad (k^{i_1} h_{j_1} - k^{i_2} h_{j_2}, t) = t. \tag{7}$$

If there is no such N *define* $N(\vartheta_1, \dots, \vartheta_r, k, \delta) = N$ *by 1.*

Let $L, M \in \mathbb{N}$ *with* $L \le T$*. Then there exists a constant* $\varepsilon(r, \delta) = \varepsilon_2 \ge 0$ *depending on only* r *(the number of* ϑ_i*'s) and* δ *such that:*

$$\left| \sum_{x=M}^{M+L} e_p(a_1 \vartheta_1^{k^x} + \cdots + a_r \vartheta_r^{k^x}) \right| \ll (tT)^{1/2} \left(p^{-\varepsilon_2} + \frac{(r+1)^{r/2}}{N^{1/2}} \right) \log p.$$

Moreover, in the special case $(h_1, t) = 1$ *we may replace the term* $(r+1)^{r/2}$ *by* $(r+1)^{1/2}$*:*

$$\left| \sum_{x=M}^{M+L} e_p(a_1 \vartheta_1^{k^x} + \cdots + a_r \vartheta_r^{k^x}) \right| \ll (tT)^{1/2} \left(p^{-\varepsilon_2} + \frac{(r+1)^{1/2}}{N^{1/2}} \right) \log p.$$

where the implied constant factors are absolute.

Proof of Lemma 1 and Lemma 2

We will use the following deep theorem of Bourgain [2]:

Lemma 3 *Let p be a prime. Given $r \in \mathbb{Z}^+$ and $\delta > 0$, there is an $\varepsilon = \varepsilon(r, \delta) > 0$ satisfying the following property: If*

$$f(x) = a_1 x^{k_1} + \cdots + a_r x^{k_r} \in \mathbb{Z}[x] \quad \textit{and } (a_i, p) = 1$$

where the exponents $1 \leq k_i \leq p-1$ satisfy

$$\begin{aligned} (k_i, p-1) &< p^{1-\delta} \textit{ for all } 1 \leq i \leq r \\ (k_i - k_j, p-1) &< p^{1-\delta} \textit{ for all } 1 \leq i \neq j \leq r \end{aligned} \tag{8}$$

then

$$\left| \sum_{x=1}^{p-1} e_p(f(x)) \right| < p^{1-\varepsilon}.$$

Proof of Lemma 3

See in [2].

In order to prove Lemma 1 and Lemma 2 first we need estimates for complete sums.

First we give an upper bound for n_0 defined in Notation 1. Let ord ϑ denote the multiplicative order of ϑ modulo p. n_0 is the smallest integer for which $(k^{n_0}, \text{ord } \vartheta)$ is maximal. From this

$$n_0 \leq \frac{\log \text{ord } \vartheta}{\log 2} < 1.45 \log p. \tag{9}$$

We will deduce the first two statements of Lemma 4 from Bourgain's theorem (Lemma 3), while the third part will be proved by extending an argument of Friedlander and Shparlinski [9].

Lemma 4 *Let $\vartheta_1, \ldots, \vartheta_r \in \mathbb{F}_p$ and $N(\vartheta_1, \ldots, \vartheta_r, k, \delta) = N$ as in Lemma 2, $j \in \mathbb{Z}_T$. Then there exists a constant $\varepsilon(r, \delta) = \varepsilon_2 \geq 0$ depending on only r and δ such that:*

$$\left| \sum_{x=n_0}^{n_0-1+T} e_p(a_1 \vartheta_1^{k^x} + \cdots + a_r \vartheta_r^{k^x}) e_T(jx) \right| \ll (tT)^{1/2} \left(p^{-\varepsilon_2} + \frac{(r+1)^{r/2}}{N^{1/2}} \right). \tag{10}$$

If $(h_1, t) = 1$ (where h_1 is defined by $\vartheta_1 \equiv \vartheta^{h_1} \pmod{p}$), then we may replace the term $(r+1)^{r/2}$ by $(r+1)^{1/2}$:

$$\left| \sum_{x=n_0}^{n_0-1+T} e_p(a_1 \vartheta_1^{k^x} + \cdots + a_r \vartheta_r^{k^x}) e_T(jx) \right| \ll (tT)^{1/2} \left(p^{-\varepsilon_2} + \frac{(r+1)^{1/2}}{N^{1/2}} \right), \tag{11}$$

where the implied constants are absolute.

If $\vartheta_i = \vartheta^{k^i}$ for $1 \leq i \leq r$ then there exists an upper bound, where the exponent of p is given: Suppose that $\varepsilon_1 > 1/4$ and $t > p^{1/2+\delta}$ for a constant $\delta > 0$, then

$$\left| \sum_{x=n_0}^{n_0-1+T} e_p(a_1 \vartheta^{k^x} + a_2 \vartheta^{k^{x+1}} + \cdots + a_r \vartheta^{k^{x+r-1}}) e_T(jx) \right| \ll k^{\varepsilon_1 (r-1)} T^{1/4} t^{1/2} p^{1/8}, \tag{12}$$

where the implied constant depends only on ε_1 and δ.

Proof of Lemma 4

The proof is similar to the proof of Theorem 8 in [7] in the special case $\nu = 1$, but in order to prove (10) and (11) we use Bourgain's theorem in place of Weil's theorem.

Let $S = \left|\sum_{x=n_0}^{n_0-1+T} e_p(a_1\vartheta_1^{k^x} + \cdots + a_r\vartheta_r^{k^x})e_T(jx)\right|$ and $\mathcal{K} \subseteq \{k^1, \ldots, k^T\}$. For $y = k^v \in \mathcal{K}$ denote v by $\mathrm{ind}_k y$. Clearly,

$$S = \frac{1}{|\mathcal{K}|}\left|\sum_{y\in\mathcal{K}}\sum_{x=n_0}^{n_0-1+T} e_p(a_1\vartheta_1^{yk^x} + \cdots + a_r\vartheta_r^{yk^x})e_T(j(x+\mathrm{ind}_k y))\right|.$$

By the Cauchy-Schwartz inequality we have

$$S \le \frac{T^{1/2}}{|\mathcal{K}|}\left(\sum_{x=n_0}^{n_0-1+T}\left|\sum_{y\in\mathcal{K}} e_p(a_1\vartheta_1^{yk^x} + \cdots + a_r\vartheta_r^{yk^x})e_T(j\mathrm{ind}_k y)\right|^2\right)^{1/2}.$$

We recall that $\vartheta_i \equiv \vartheta^{h_i} \pmod p$, where $(h_1, \ldots, h_r, p-1) = 1$. Let $d = (p-1)/t$. Since the order of ϑ^{k^x} is t for $n_0 \le x$, for each of these powers ϑ^{k^x}, there exist precisely d values of $z \in \mathbb{F}_p^*$ such that $\vartheta^{k^x} \equiv z^d \pmod p$. Thus

$$\begin{aligned} S &\le \frac{T^{1/2}}{|\mathcal{K}|\, d^{1/2}}\left(\sum_{z=1}^{p-1}\left|\sum_{y\in\mathcal{K}} e_p(a_1 z^{yh_1 d} + \cdots + a_r z^{yh_r d})e_T(j\mathrm{ind}_k y)\right|^2\right)^{1/2} \\ &\le \frac{T^{1/2}}{|\mathcal{K}|\, d^{1/2}}\Bigg(\sum_{y\in\mathcal{K}}\sum_{x\in\mathcal{K}}\Bigg|\sum_{z=1}^{p-1} e_p(a_1 z^{yh_1 d} + \cdots + a_r z^{yh_r d} - \\ &\quad - a_1 z^{xh_1 d} - \cdots - a_r z^{xh_r d})\Bigg|\Bigg)^{1/2}. \end{aligned}$$

For given $y, x \in \mathcal{K}$ define the polynomial $g_{y,x}(z) \in \mathbb{F}_p[z]$ by

$$g_{y,x}(z) \stackrel{\mathrm{def}}{=} a_1 z^{yh_1 d} + \cdots + a_r z^{yh_r d} - a_1 z^{xh_1 d} - \cdots - a_r z^{xh_r d}.$$

Denote by $g_{y,x}(z) \equiv c$ that the polynomial $g_{y,x}(z) \in \mathbb{F}_p[z]$ is identically constant. Then

$$\begin{aligned} S &\le \frac{T^{1/2}}{|\mathcal{K}|\, d^{1/2}}\left(\sum_{x\in\mathcal{K}}\sum_{y\in\mathcal{K}}\left|\sum_{z=1}^{p-1} e_p(g_{y,x}(z))\right|\right)^{1/2} \\ &\le \frac{T^{1/2}}{|\mathcal{K}|\, d^{1/2}}\left(\sum_{\substack{x,y\in\mathcal{K}\\ g_{y,x}(z)\not\equiv c}}\left|\sum_{z=1}^{p-1} e_p(g_{y,x}(z))\right| + \sum_{\substack{x,y\in\mathcal{K}\\ g_{y,x}(z)\equiv c}} p\right)^{1/2} \end{aligned} \tag{13}$$

Next we estimate the number of the pairs $y, x \in \mathcal{K}$ with $g_{y,x}(z) \equiv c$. Clearly, then apart from the multiplicity, the set $\{yh_1 d, \dots, yh_r d\} \setminus \{0\}$, contains the same residue classes modulo $p-1$ as the set $\{xh_1 d, \dots, xh_r d\} \setminus \{0\}$. So the set $\{yh_1, \dots, yh_r\} \setminus \{0\}$ contains the same residue classes modulo t as the set $\{xh_1, \dots, xh_r\} \setminus \{0\}$. We will use the following lemma.

Lemma 5 *For given $x \in \mathcal{K}$ at most $(r+1)^r$ pieces of $y \in \mathcal{K}$ exist such that the sets $\{xh_1, \dots, xh_r\} \setminus \{0\}$, $\{yh_1, \dots, yh_r\} \setminus \{0\}$ contain the same residue classes modulo t apart from the multiplicity. If $(h_1, t) = 1$ then at most $r+1$ pieces of $y \in \mathcal{K}$ exist with this property.*

Proof of Lemma 5 Define h_{r+1} by 0. Then for every $1 \le i \le r$ there exits a $1 \le j(i) \le r+1$ such that

$$yh_i \equiv xh_{j(i)} \pmod{t}. \tag{14}$$

This congruence determines y uniquely modulo $\frac{t}{(t,h_i)}$. As i runs through the numbers $1, 2, \dots, r$, by the Chinese Remainder Theorem we get that y is uniquely determined modulo $\frac{t}{(t,h_1,\dots,h_r)} = t$ (since $(h_1, \dots, h_r, p-1) = 1$). In the special case $(h_1, t) = 1$ the first congruence $yh_1 \equiv xh_{j(1)} \pmod{t}$ determines y uniquely. The elements of $\mathcal{K}$ are distinct modulo t, thus if the congruences in (14) are given, then at most one $y \in \mathcal{K}$ exists with the desired property. Since each $j(i)$ may take $r+1$ different values, from this follows the lemma.

We return to the proof of Lemma 4. Define the constant $c(r)$ by

$$c(r) = \begin{cases} r+1 & \text{if } (h_1, t) = 1, \\ (r+1)^r & \text{otherwise.} \end{cases} \tag{15}$$

By Lemma 5, for fixed $x \in \mathcal{K}$ at most $c(r)$ pieces of y exist with $g_{y,x}(z) \equiv c$. $x \in \mathcal{K}$ may take $|\mathcal{K}|$ different values, thus at most $c(r)\,|\mathcal{K}|$ pairs (y,x) exists such that $g_{y,x}(z) \equiv c$. By this and (13) we get

$$S \leq \frac{T^{1/2}}{|\mathcal{K}|\,d^{1/2}} \left(\sum_{\substack{x,y\in\mathcal{K} \\ g_{y,x}(z)\not\equiv c}} \left| \sum_{z=1}^{p-1} e_p(g_{y,x}(z)) \right| + c(r)\,|\mathcal{K}|\,p \right)^{1/2}.$$

Let Q

$$Q \stackrel{\text{def}}{=} \max_{\substack{x,y\in\mathcal{K} \\ g_{y,x}(z)\not\equiv c}} \left| \sum_{z=1}^{p-1} e_p(g_{y,x}(z)) \right|.$$

Then

$$S \leq \frac{T^{1/2}}{|\mathcal{K}|\,d^{1/2}} \left(|\mathcal{K}|^2\,Q + c(r)\,|\mathcal{K}|\,p \right)^{1/2} \leq \left(\frac{TQ}{d} \right)^{1/2} + \left(c(r)\frac{Tp}{|\mathcal{K}|\,d} \right)^{1/2}. \quad (16)$$

In order to prove (10) and (11) we choose $\mathcal{K} = \{k^1, \dots, k^N\}$ with $N = N(\vartheta_1, \dots, \vartheta_r, k, \delta)$. Then $|\mathcal{K}| = N$. For $x, y \in \mathcal{K}$ and $\frac{p-1}{t} = d$ by (6) we have

$$(dxh_j, p-1) = d(xh_j, t) \leq dtp^{-\delta} < p^{1-\delta}. \quad (17)$$

Clearly (17) also holds with y in place of x. Similarly, by (7)

$$(dxh_{j_1} - dyh_{j_2}, p-1) = d(xh_{j_1} - yh_{j_2}, t) \begin{cases} \leq dtp^{-\delta} < p^{1-\delta} & \text{or} \\ = dt = p-1. \end{cases}$$

Thus (8) holds for the polynomial $g_{y,x}(z) \in \mathbb{F}_p[z]$ and we may use Lemma 3 since $g_{y,x}(z) \not\equiv c$. Then

$$Q \leq p^{1-\varepsilon_2}.$$

By this, (15), (16), $t = \frac{p-1}{d}$ and $|\mathcal{K}| = N$ we get:

$$S \ll \left(\frac{Tp^{1-\varepsilon_2}}{d} \right)^{1/2} + \left(c(r)\frac{Tp}{Nd} \right)^{1/2} \ll (Tt)^{1/2}(p^{-\varepsilon_2} + c(r)^{1/2}N^{-1/2})$$

which proves (10) and (11) in Lemma 4.

In order to get (12) we recall the proof of Friedlander and Shparlinski [9]. Consider the special case $h_i = k^{i-1}$ for $1 \le i \le r$. In order to estimate Q in this special case we need Weil's theorem for character sums, which we present in the following form:

Lemma 6 *For any prime p, and any polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $D \ge 1$ which is not identically constant, the bound*

$$\left| \sum_{x=1}^{p} e_p(f(x)) \right| \le Dp^{1/2}.$$

holds.

Proof of Lemma 6

This lemma can be deduced from Weil's theorem. See [22], an elementary proof can be found in [19].

We will also need the following lemma of Friedlander, Hansen and Shparlinski [7]:

Lemma 7 *For any set $\mathcal{W} \subseteq \mathbb{Z}_t^*$ of cardinality $|\mathcal{W}| = W$, any fixed $\delta > 0$ and any integer $h \ge t^{\delta}$, there exists an integer $a \in \mathbb{Z}_t^*$, such that the congruence*

$$ak \equiv b \pmod{t}, \quad k \in \mathcal{W},\ 0 \le b \le h-1 \tag{18}$$

has

$$L_a(h) \gg \frac{Wh}{t}$$

solutions.

Proof of Lemma 7

This is Lemma 2 in [7].

We return to the proof of (12) in Lemma 4. Let $\varepsilon_1 > 1/4$. If $k^{\varepsilon_1(r-1)} > \frac{T^{3/4}}{t^{1/2}p^{1/8}}$, then using the trivial estimate we obtain $S \le T \le k^{\varepsilon_1(r-1)}t^{1/2}T^{1/4}p^{7/8}$ which was to be proved. Thus we may suppose

$$k^{(r-1)/2} \le \frac{T^{3/(8\varepsilon_1)}}{t^{1/(4\varepsilon_1)}p^{1/(16\varepsilon_1)}}. \tag{19}$$

Set

$$h = \left[\frac{(r+1)^{1/2}t}{T^{1/2}k^{(r-1)/2}p^{1/4}}\right] \tag{20}$$

Then by (19), $T \le t$ and $t > p^{1/2+\delta}$ we have

$$\begin{aligned} h &\gg \frac{t}{T^{1/2}\frac{T^{3/(8\varepsilon_1)}}{t^{1/(4\varepsilon_1)}p^{1/(16\varepsilon_1)}}p^{1/4}} = \frac{t^{1+1/(4\varepsilon_1)}}{T^{1/2+3/(8\varepsilon_1)}p^{1/4-1/(16\varepsilon_1)}} \gg \frac{t^{1/2-1/(8\varepsilon_1)}}{p^{1/4-1/(16\varepsilon_1)}} \\ &= \left(\frac{t}{p^{1/2}}\right)^{1/2-1/(8\varepsilon_1)} \gg t^{\frac{2\delta}{1+2\delta}(1/2-1/(8\varepsilon_1))}, \end{aligned}$$

thus we may use Lemma 7. Let $\mathcal{W} = \{k^1, \ldots, k^T\}$. We select a as in Lemma 2. Let now $\mathcal{K}$ denote the subset of $\mathcal{W}$ which satisfies the corresponding congruence (18). Then the degree of the polynomial $g_{y,x}(z^a)$ is less than $hk^{r-1}d$. By this and Lemma 6 we have

$$Q = \max_{\substack{x,y\in\mathcal{K} \\ g_{y,x}(z)\equiv 0}} \left|\sum_{z=1}^{p-1} e_p(g_{x,y}(z))\right| = \max_{\substack{x,y\in\mathcal{K} \\ g_{y,x}(z)\equiv 0}} \left|\sum_{z=1}^{p-1} e_p(g_{x,y}(z^a))\right| \le hk^{r-1}dp^{1/2}. \tag{21}$$

By Lemma 7

$$|\mathcal{K}| \gg \frac{Th}{t}. \tag{22}$$

By (2) and (15) we have $c(r) = r + 1$. By this, (16), (20), (21), (22) and $t = \frac{p-1}{d}$ we get

$$\begin{aligned} S &\le \left(\frac{Thk^{r-1}dp^{1/2}}{d} \right)^{1/2} + \left(\frac{c(r)Tp}{|\mathcal{K}|\, d} \right)^{1/2} \\ &\le \left(Tk^{r-1}hp^{1/2} \right)^{1/2} + \left(\frac{(r+1)Tt}{|\mathcal{K}|} \right)^{1/2} \\ &\le \left(Tk^{r-1}hp^{1/2} \right)^{1/2} + \left(\frac{(r+1)t^2}{h} \right)^{1/2} \\ &\ll \left((r+1)k^{r-1}Tt^2p^{1/2} \right)^{1/4}, \end{aligned}$$

which was to be proved.

We return to the proof of Lemma 1 and Lemma 2. Let

$$S = \left| \sum_{x=M}^{M+L} e_p(a_1\vartheta_1^{k^x} + \cdots + a_r\vartheta_r^{k^x}) \right|.$$

We will suppose $M \ge n_0$, since by (9) the contribution of the terms of $M \le x \le n_0$ in S is small, at most $n_0 \le 1.45 \log p$. Using

$$\sum_{j=1}^{T} e_T(nj) = \begin{cases} T & \text{if } T \mid n, \\ 0 & \text{otherwise,} \end{cases}$$

we get

$$\begin{aligned} S &= \frac{1}{T} \left| \sum_{y=n_0}^{n_0-1+T} e_p(a_1\vartheta_1^{k^y} + \cdots + a_r\vartheta_r^{k^y}) \sum_{x=M}^{M+L} \sum_{j=1}^{T} e_T((y-x)j) \right| \\ &= \frac{1}{T} \sum_{j=1}^{T} \left| \sum_{x=M}^{M+L} e_T(-jx) \right| \left| \sum_{y=n_0}^{n_0-1+T} e_p(a_1\vartheta_1^{k^y} + \cdots + a_r\vartheta_r^{k^y}) e_T(jy) \right|. \end{aligned} \tag{23}$$

Let

$$Q = \max_j \left| \sum_{y=n_0}^{n_0-1+T} e_p(a_1\vartheta_1^{k^y} + \cdots + a_r\vartheta_r^{k^y}) e_T(jy) \right|.$$

By (23) we have

$$S \leq \frac{1}{T} \sum_{j=1}^{T} \left| \sum_{x=M}^{M+L} e_T(-jx) \right| Q. \tag{24}$$

By Lemma 4 there exits a constant $\varepsilon_2 > 0$ depending only on r and δ such that

$$Q \ll (tT)^{1/2}(p^{-\varepsilon_2} + (c(r))^{1/2} N^{-1/2}), \tag{25}$$

where the constant $c(r)$ is defined by (15). Moreover in the special case $\vartheta_i = \vartheta^{k^{i-1}}$ for $1 \leq i \leq r$ we get that for every $\varepsilon_1 > 1/4$

$$Q \ll k^{\varepsilon_1 (r-1)} t^{1/2} T^{1/4} p^{1/8} \tag{26}$$

also holds.

By the sum of geometric progression, the triangle-inequality and $|1 - e(x)| \geq 4 \parallel x \parallel$ we have

$$\sum_{j=1}^{T} \left| \sum_{x=0}^{L} e_T(-jx) \right| \leq \sum_{j=1}^{T} \frac{2}{|1 - e(j/T)|} \leq \frac{1}{2} \sum_{j=1}^{T} \frac{1}{\parallel j/T \parallel} \leq \sum_{j=1}^{[(T+1)/2]} \frac{1}{\parallel j/T \parallel}$$
$$= \sum_{j=1}^{[(T+1)/2]} \frac{j}{T} \ll T \log T. \tag{27}$$

By (24), (25), (26) and (27) we get the statements of Lemma 1 and Lemma 2.

Remark 1 *In fact, using the results of Friedlander, Hansen and Shparlinski [7], the following can be proved: if $t > p^{1/2+\delta}$ for all integer $\nu \geq 1$ we have:*

$$\left| \sum_{x=M}^{M+L} e_p(a_1 \vartheta^{k^x} + a_2 \vartheta^{k^{x+1}} + \cdots + a_r \vartheta^{k^{x+r-1}}) \right| \ll T^{1 - \frac{2\nu+1}{2\nu(\nu+1)}} t^{\frac{1}{2\nu}} p^{\frac{1}{4(\nu+1)}} \log T.$$

Here, we presented the proof only in the special case $\nu = 1$.

3 Proofs of Theorem 1-3

In order to express the terms of the sequence E_N we will use additive characters as in [15]. We will use the following representation:

Lemma 8 *For $n \in \mathbb{N}$ $r_p(n)$ denotes the unique $r \in \{0, \ldots, p-1\}$ for which $n \equiv r \pmod p$. Then for odd integer p, there exists a function $\nu_p(a, x) : \mathbb{Z} \times \mathbb{Z} \to \mathbb{C}$ such that*

$$\frac{1}{p} \sum_{|a|<p/2} \nu_p(a, x) e_p(an) = \begin{cases} +1 & \textit{if } r_p(n) \equiv x \pmod 2, \\ 0 & \textit{if } r_p(n) \not\equiv x \pmod 2, \end{cases}$$

and the function $\nu_p(a, x)$ satisfies

$$\nu_p(0, x) = \begin{cases} \frac{p+1}{2} & \textit{if } x \equiv 0 \pmod 2, \\ \frac{p-1}{2} & \textit{if } x \equiv 1 \pmod 2. \end{cases} \tag{28}$$

Furthermore, for $1 \le |a| < p/2$ we have

$$|\nu_p(a, x)| \ll \frac{p}{\min\{a, p-2a\}}. \tag{29}$$

Proof of Lemma 8

Since for $r \in \mathbb{Z}$, we have

$$\frac{1}{p} \sum_{|a|<p/2} e_p(a(n-r)) = \begin{cases} 1 & \text{if } n \equiv r \pmod p, \\ 0 & \text{otherwise}, \end{cases}$$

for $0 \le n \le p-1$ we have

$$\frac{1}{p} \sum_{|a|<p/2} \left(\sum_{\substack{r \equiv x \pmod 2, \\ 0 \le r \le p-1}} e_p(-ar) \right) e_p(an) = \begin{cases} 1 & \text{if } n \equiv x \pmod 2, \\ 0 & \text{otherwise}. \end{cases}$$

Thus we may define $\nu_p(a,x)$ by

$$\nu_p(a,x) \stackrel{\text{def}}{=} \sum_{\substack{r\equiv x \pmod 2,\\ 0\le r\le p-1}} e_p(-ar).$$

From this immediately follows (28). By computing the geometric sum above, using the triangle inequality and $|1-e(x)| \ge 4 \parallel x \parallel$ we get (29).

Writing $\nu(a) = \nu(a,0) - \nu(a,1)$ from Lemma 8 we get immediately:

Lemma 9 *For $0 \le n \le p-1$ and an odd integer p, we have*

$$\frac{1}{p}\sum_{|a|<p/2} \nu_p(a)e_p(an) = \begin{cases} +1 & \text{if } r_p(n) \equiv 0 \pmod 2, \\ -1 & \text{if } r_p(n) \equiv 1 \pmod 2, \end{cases}$$

where the function $\nu_p(a)$ satisfies

$$\nu_p(0) = 1, \quad |\nu_p(a)| \ll \frac{p}{\min\{a, p-2a\}} \quad (1 \le |a| < p/2).$$

Proof of Theorem 1

If $t \le p^{7/8}$ Theorem 1 and 2 are trivial, since all pseudorandom measures of E_T are less or equal than $T \le t \le p^{7/8}$. Thus we may suppose that

$$t > p^{7/8}. \tag{30}$$

We have to prove that for any $0 \le b < p$, $0 \le c < b$, $1 \le M < T$, we have the estimate

$$\left| \sum_{\substack{j\\ c+jb\le M}} e_{c+jb} \right| \ll p^{7/8}(\log p)^2.$$

By Lemma 9 we have

$$\left| \sum_{\substack{j\\ c+jb\le M}} e_{c+jb} \right| = \frac{1}{p}\sum_{|a|<p/2} \nu_p(a) \sum_{\substack{j\\ c+jb\le M}} e_p(au_{c+jb})$$

Since $u_{c+jb} \equiv \left(\vartheta^{(k^c)}\right)^{(k^b)^j} \pmod p$, the multiplicative order of k^b modulo t is larger or equal than T/b and by (30) we may use Lemma 1 and obtain

$$\left|\sum_{\substack{j\\c+jb}} e_p(au_{c+jb})\right| \ll T^{1/4}t^{1/2}p^{1/8} \ll p^{7/8}\log p.$$

Thus

$$\left|\sum_{\substack{x\\r+xm\leq M}} e_{r+xm}\right| \ll \frac{1}{p}\left(\sum_{1\leq|a|<p/2}|\nu_a(p)|\right)p^{7/8}\log p + |\nu_p(0)|\,, \tag{31}$$

By Lemma 9 $\nu_p(0)=1$ and $\sum_{1\leq|a|<p/2}|\nu_a(p)| \ll \sum_{1\leq|a|<p/4+1}\frac{p}{a} \ll p\log p$, so the theorem follows from this and (31).

Proof of Theorem 2

By Lemma 8 for $M\leq T-\ell+1$ we have

$$Z(E_T,M,X) = \frac{1}{p^\ell}\sum_{|a_1|<p/2}\cdots\sum_{|a_\ell|<p/2}\nu_p(a_1,u_{n+1})\cdots\nu_p(a_\ell,u_{n+\ell})$$
$$\sum_{n<M} e_p(a_1u_{n+1}+\cdots+a_\ell u_{n+\ell}). \tag{32}$$

If $(a_1,\ldots,a_\ell)=(0,\ldots,0)$ then trivially

$$\left|\sum_{n<M} e_p(a_1u_{n+1}+\cdots+a_\ell u_{n+\ell})\right| = M-1. \tag{33}$$

By Lemma 8 we have

$$\frac{(p-1)^\ell}{2^\ell} \leq |\nu_p(0,u_{n+1})\cdots\nu_p(0,u_{n+\ell})| \leq \frac{(p+1)^\ell}{2^\ell}. \tag{34}$$

By (30) we may use Lemma 1 and for all $\varepsilon_1>1/4$ we have that if $(a_1,\ldots,a_\ell)\neq(0,\ldots,0)$ then

$$\left|\sum_{n<M} e_p(a_1u_{n+1}+\cdots+a_\ell u_{n+\ell})\right| = \left|\sum_{n<M} e_p(a_1\vartheta^{k^{n+1}}+\cdots+a_\ell\vartheta^{k^{n+\ell}})\right|$$
$$\ll k^{\varepsilon_1(r-1)}T^{1/4}t^{1/2}p^{1/8\log p} \ll k^{\varepsilon_1(r-1)}p^{7/8}\log p, \tag{35}$$

where the implied constant depends only on ε_1. By (32), (33), (35) and the triangle inequality we have

$$\left|Z(E_T, M, X) - M/2^\ell\right| \le \frac{1}{p^\ell}\left|\sum_{\substack{(a_1,\dots,a_\ell)\neq(0,\dots,0),\\ |a_i|<p/2\ (1\le i\le \ell)}} \nu_p(a_1, u_{n+1})\cdots\nu_p(a_\ell, u_{n+\ell})\right.$$

$$\left.\sum_{n<M} e_p(a_1u_{n+1}+\cdots+a_\ell u_{n+\ell})\right| + \frac{1}{p^\ell}\left|\frac{(p+1)^\ell}{2^\ell}(M-1) - \frac{M}{2^\ell}\right|.$$

Since $\ell < p$ we have

$$\frac{1}{p^\ell}\left|\frac{(p+1)^\ell}{2^\ell}(M-1)-\frac{M}{2^\ell}\right| \le \left(\frac{(p+1)^\ell}{p^\ell}-1\right)\frac{M}{2^\ell} \le \frac{e\ell M}{p2^\ell} \le \frac{e\ell}{2^\ell} < 1.5.$$

If $(a,p)=1$ let $\mu_p(a) = \frac{p}{\min\{a,p-2a\}}$ and let $\mu_p(0) = \frac{p+1}{2}$. Then by Lemma 8 $\nu_p(a, u_{n+i}) \le \mu(a)$. By this and (34) we have

$$\left|Z(E_T, M, X) - M/2^\ell\right| \ll \frac{1}{p^\ell}\left(\left|\sum_{|a|<p/2}\mu_p(a)\right|^\ell k^{\varepsilon_1(r-1)}p^{7/8}\log p\right) + 1.5.$$

Using $\left|\sum_{|a|<p/2}\mu_p(a)\right| \ll \sum_{1\le|a|\le p/4+1}\frac{p}{a} \ll \log p$, we get the theorem.

Proof of Theorem 3

Theorem 3 is trivial if $N \le p^{1/2}$. Thus we may suppose that

$$N > p^{1/2}. \tag{36}$$

By Lemma 9 for $M < p$ and $0 \le d_1 < \cdots < d_\ell \le p - M$ we have

$$\sum_{n\le M} e_{n+d_1}\dots e_{n+d_\ell} = \frac{1}{p^\ell}\sum_{|a_1|<p/2}\cdots\sum_{|a_\ell|<p/2}\nu_p(a_1)\cdots\nu_p(a_\ell)$$

$$\sum_{n<M} e_p(a_1u_{n+d_1}+\cdots+a_\ell u_{n+d_\ell})$$

If $(a_1,\dots,a_\ell)\neq(0,\dots,0)$ we may use Lemma 2 with $h_1=k^{d_1},\dots,h_\ell=k^{d_\ell}$. By (2) $(h_i,t)=(k,t)=1$, thus we obtain

$$\begin{aligned}&\left|\sum_{n<M} e_p(a_1u_{n+d_1}+\dots+a_\ell u_{n+d_\ell})\right|\\ &=\left|\sum_{n<M} e_p(a_1\left(\vartheta^{k^{d_1}}\right)^{k^n}+\dots+a_\ell\left(\vartheta^{k^{d_\ell}}\right)^{k^n})\right|\\ &\ll (tT)^{1/2}\left(p^{-\varepsilon_2}+\frac{(r+1)^{1/2}}{N^{1/2}}\right)\log p.\end{aligned}$$

By (36) and $r^2<p$ we have

$$\left|\sum_{n<M} e_p(a_1u_{n+d_1}+\dots+a_\ell u_{n+d_\ell})\right|\ll p^{1-\varepsilon_2/2},$$

where the implied constant depends only on ε_2. Thus

$$\left|\sum_{n\le M} e_{n+d_1}\dots e_{n+d_\ell}\right|=\frac{1}{p^\ell}\left(\left(\sum_{|a|<p/2}|\nu_p(a)|\right)^\ell p^{1-\varepsilon_2/2}+M\right).$$

Using $\left|\sum_{|a|<p/2}\nu_p(a)\right|\ll\left|\sum_{|a|<p/4+1}\frac{p}{a}\right|\ll\log p$, we get

$$C_\ell(E_N)\le c_1p^{1-\varepsilon_2/4},$$

where the constant c_1 depends only on ε_2. From this for large $p>p_0$ follows the theorem, while for small $p\le p_0$ the theorem is trivial with an $\varepsilon>0$ for which $N<p^{1-\varepsilon}$ if $p<p_0$. Such $\varepsilon>0$ exists, since $N<p$.

Proof of Corollary 1

Since q is a prime, $t=q$ or $t=2q$. k is a primitive root modulo q, thus for $1\le i<j\le q-1$ we have

$$(k^j-k^i,t)=1\quad\text{or}\quad(k^j-k^i,t)=2$$

which is less than $tp^{-\delta}$ for $\delta > 1/2$. Thus (4) holds with $N = (p-1)/3$ and using Theorem 3 we get the corollary.

We would like to thank Professor András Sárközy for the valuable discussions.

References

[1] L. Blum, M. Blum and M. Shub, *A simple unpredictable pseudorandom number generator*, SIAM J. Comp. 15 (1986), 364-383.

[2] J. Bourgain, *Mordell's exponential sum estimate revisited*, to appear.

[3] J. J. Brennan and B. Geist, *Analysis of iterated modular exponentiation: The orbit of x^α mod N*, Designs, Codes and Cryptography 13 (1998), 229-245.

[4] T. W. Cusick, C. Ding and A. Renvall, *Stream Ciphers and Number Theory*, Elsevier, North-Holland Publishing Co., Amsterdam 1998.

[5] T. W. Cusick, *Properties of the x^2 mod N pseudorandom number generator*, IEEE Trans. Inform. Theory 41 (1995), 1155-1159.

[6] R. Fischlin and C. P. Schnorr, *Stronger Security proofs for RSA and Rabin bits*, Lecture Notes in Comp. Sci., Springer-Verlag, Berlin, 1233 (1997), 267-279.

[7] J. B. Friedlander, J. Hansen and I. Shparlinski, *Character sums with exponential functions*, Mathematika, 47 (2000), 75-85.

[8] J. B. Friedlander, D. Lieman and I. E. Shparlinski, *On the distribution of the RSA generator*, Proc. Itern. Conf. on Sequences and Their Applications (SETA'98), Singapore, Springer-Verlag, London 1999, 205-212.

[9] J. B. Friedlander and I. E. Shparlinski, *On the distribution of the power generator*, Math Comp. 70 (2001), no. 236, 1575-1589.

[10] J. B. Friedlander, C. Pomerance, I. E. Shparlinski, *Period of the power generator and small values of the Carhmichael's function*, Math Comp. 70 (2001), no. 236, 1591-1605.

[11] L. Goubin, C. Mauduit, A. Sárközy, *Constuction of large families of pseudorandom binary sequences*, Journal of Number Theory 106 (2004), no.1, 56-69.

[12] F. Griffin and I. E. Shparlinski, *On the linear complexity profile of the power generator*, IEEE Trans. Inform. Theory 46 (2000), no. 6, 2159-2162.

[13] J. Håstad and M. Näslund, *The security of individual RSA bits*, Proc 39th IEEE Symp. on Foundations of Comp. Sci., 1998, 510-519.

[14] J. C. Lagarias, *Pseudorandom number generators in cryptography and number theory*, Proc. Symp. in Appl. Math., Amer. Math. Soc., Providence, RI, 42 (1990), 115-143.

[15] C. Mauduit, J. Rivat and A. Sárközy, *Construction of Pseudorandom Binary Sequences Using Additive Characters*, Monatsh. Math. 141, (2004), 197-208.

[16] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences, I. Measures of pseudorandomness, the Legendre symbol*, Acta Arithmetica 82 (1997), 365-377.

[17] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.

[18] J. Rivat, A. Sárközy, *Modular Constructions of pseudorandom binary sequences with composite moduli*, to appear.

[19] W. M. Schmidt, *Equation over Finite Fields*, Springer-Verlag, Berlin · Heidelberg · New York 1976.

[20] I. E. Shparlinski, *On the linear complexity of the power generator*, Designs, Codes and Cryptography 23 (2001) no. 1, 5-10.

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

[22] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.