ACTA ARITHMETICA
140.2 (2009)

Large families of elliptic curve pseudorandom binary sequences

by

Huaning Liu, Tao Zhan and Xiaoyun Wang (Jinan)

1. Introduction. Elliptic curve public-key cryptosystems over $\mathbb{F}_q$ have become widely used in applications since N. Koblitz and V. Miller proposed using elliptic curves over $\mathbb{F}_q$ to construct public-key cryptosystems. Roughly speaking, the elliptic curve cryptosystems can be considered as pseudorandom sequence generators. If these sequences have good pseudorandomness, then they can be used for generating random numbers, which are very useful in cryptography and communications.

Many scholars have studied elliptic curve sequences with strong cryptographic properties. For example, B. S. Kaliski [12] first used elliptic curves to construct pseudorandom sequences by using randomness criteria based on the computational difficulty of the discrete logarithm over the elliptic curves. S. Hallgren [8] discussed some heuristics of the linear congruentia generator over elliptic curves. G. Gong, T. A. Berson and D. R. Stinson [4] constructed a class of binary sequences by applying trace functions to elliptic curves over $\mathbb{F}_{2^m}$, and discussed the least periods, linear complexities and 0-1 distributions of these sequences. E. E. Mahassni and I. Shparlinski [16] obtained a bound for the uniform distribution of the congruential generators over elliptic curves. Meanwhile, P. H. T. Beelen and J. M. Doumen [1] proved an upper bound for some exponential sums on algebraic curves over finite fields, and studied some sequences constructed from elliptic curves. G. Gong and C. C. Y. Lam [5] introduced linear recursive sequences over elliptic curves. Moreover, C. P. Xing et al. constructed some sequence families with both large linear complexity and low correlation in [22] and [23]. F. Hess and I. Shparlinski [9] studied the linear complexity and multidimensional distribution of the congruential generators over elliptic curves. Recently H. Hu, L. Hu and D. Feng [10] investigated a general method for

2010 *Mathematics Subject Classification*: Primary 11K45.
Key words and phrases: pseudorandom binary sequence, elliptic curve, pseudorandomness.

DOI: 10.4064/aa140-2-3

constructing families of pseudorandom sequences with low correlation and large linear complexity from elliptic curves.

It is of interest to further study the pseudorandom sequences from elliptic curves over finite fields. In this paper we shall give large families of elliptic curve pseudorandom binary sequences, and study their pseudorandomness: well-distribution and correlation. In Section 2 we introduce the construction methods, and present main results about the pseudorandomness of the constructions. We shall show some results on exponential sums for elliptic curves over finite fields in Section 3. Finally in Section 4 we prove the pseudorandomness of our constructions.

2. Constructions and pseudorandom properties. Throughout this paper, let $\mathbb{F}_q$ be a finite field with $q = p^m$, and let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_q$. We denote the set of $\mathbb{F}_q$-rational points of $\mathcal{E}$ by $\mathcal{E}(\mathbb{F}_q)$. Then $\mathcal{E}(\mathbb{F}_q)$ forms an abelian group with the point $\mathcal{O}$ at infinity as the identity. Suppose that

$$\mathcal{E}(\mathbb{F}_q) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z}$$

with $|\mathcal{E}(\mathbb{F}_q)| = NL$, $L \mid N$, and $L \mid (q-1)$. Let $P, Q \in \mathcal{E}(\mathbb{F}_q)$ be two points such that the order of P is N, and the order of Q is L. Let $\mathbb{F}_q(\mathcal{E})$ be the set of functions on $\mathcal{E}$ defined over $\mathbb{F}_q$. Now we give our large families of sequences.

Construction 2.1. Let $f \in \mathbb{F}_q(\mathcal{E})$ be such that

$$f(R) = \infty \quad \text{if and only if} \quad R = \mathcal{O}.$$

Let B be a subset in $\mathbb{F}_q$ with

$$|B| = \frac{q-1}{2} \quad \text{and} \quad \sum_{r \in \mathbb{F}_q^*} \Big| \sum_{c \in B} \psi(rc) \Big| \ll q \log q$$

for any non-trivial additive character ψ on $\mathbb{F}_q$. Write $P_k = kP$. Then define $E'_{N-1} = (e'_1, \ldots, e'_{N-1})$, where

$$e'_k = \begin{cases} +1 & \text{if } f(P_k) \in B, \\ -1 & \text{if } f(P_k) \notin B. \end{cases}$$

Construction 2.2. Let $g \in \mathbb{F}_q(\mathcal{E})$ be such that

$$g(R) = 0 \quad \text{if and only if} \quad R = \mathcal{O}.$$

Let B be a subset in $\mathbb{F}_q$ with

$$|B| = \frac{q-1}{2} \quad \text{and} \quad \sum_{r \in \mathbb{F}_q^*} \Big| \sum_{c \in B} \psi(rc) \Big| \ll q \log q$$

for any non-trivial additive character ψ on $\mathbb{F}_q$. Write $P_k = kP$ and $\overline{\infty} = 0$, where $\overline{x}$ is the inverse of x. Then define $E''_{N-1} = \big(e''_1, \dots, e''_{N-1}\big)$, where

$$e''_k = \begin{cases} +1 & \text{if } \overline{g(P_k)} \in B, \\ -1 & \text{if } \overline{g(P_k)} \notin B. \end{cases}$$

EXAMPLE 2.1. A subset B in $\mathbb{F}_q$ as above does exist. For example, let p be an odd prime, $n \in \mathbb{N}$, $q = p^n$, and let $v_1, \dots, v_n$ be linearly independent elements of $\mathbb{F}_q$ over $\mathbb{F}_p$. Define $B_1^*, \dots, B_n^*$ by

$$B_1^* = \left\{ \sum_{i=1}^{n} u_i v_i : 0 \le u_1 \le \frac{p-3}{2}, u_2, \dots, u_n \in \mathbb{F}_p \right\},$$

$$B_j^* = \left\{ \sum_{i=1}^{n} u_i v_i : u_1 = \cdots = u_{j-1} = \frac{p-1}{2}, 0 \le u_j \le \frac{p-3}{2}, u_{j+1}, \dots, u_n \in \mathbb{F}_p \right\}$$

for $j = 2, \dots, n$, and write $B^* = \bigcup_{j=1}^{n} B_j^*$. Then B^* is a subset in $\mathbb{F}_q$. It is easy to show that $|B^*| = (q-1)/2$. On the other hand, from (3.21) of [21] we know that

$$\sum_{r \in \mathbb{F}_q^*} \Big| \sum_{c \in B^*} \psi(rc) \Big| \ll q \log q.$$

In a series of papers C. Mauduit, J. Rivat and A. Sárközy (partly with other coauthors) studied finite pseudorandom binary sequences

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

In particular, in [18] C. Mauduit and A. Sárközy first introduced the following measures of pseudorandomness: the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \Big| \sum_{j=0}^{t-1} e_{a+jb} \Big|,$$

where the maximum is taken over all $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le N$. The *correlation measure of order k* of E_N is denoted as

$$C_k(E_N) = \max_{M,D} \Big| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \cdots e_{n+d_k} \Big|,$$

where the maximum is taken over all $D = (d_1, \dots, d_k)$ and M with $0 \le d_1 < \cdots < d_k \le N - M$, and the *combined (well-distribution-correlation) PR-measure of order k*,

$$Q_k(E_N) = \max_{a,b,t,D} \Big| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \Big|,$$

is defined for all a, b, t, $D = (d_1, \dots, d_k)$ with $1 \le a + jb + d_i \le N$ $(i = 1, \dots, k)$.

The sequence is considered to be a "good" pseudorandom sequence if both $W(E_N)$ and $C_k(E_N)$ (at least for small k) are "small" in terms of N. J. Cassaigne, C. Mauduit and A. Sárközy [3] proved that this terminology is justified since for almost all $E_N \in \{-1, +1\}^N$, both $W(E_N)$ and $C_k(E_N)$ are less than $N^{1/2}(\log N)^c$. Later a few pseudorandom binary sequences were given and studied (see [2], [6], [7], [14], [15], [17], [19], [11], [20], [21]).

The purpose of this paper is to study the well-distribution measure and correlation measure of sequences E'_{N-1} and E''_{N-1}. The main results are the following.

THEOREM 2.1. *Let E'_{N-1} be defined as in Construction* 2.1. *Then*

$$W(E'_{N-1}) \ll \deg(f) q^{1/2} \log q \log N,$$
$$C_k(E'_{N-1}) \ll k \deg(f) q^{1/2} (2 \log q)^k \log N,$$
$$Q_k(E'_{N-1}) \ll k \deg(f) q^{1/2} (2 \log q)^k \log N.$$

THEOREM 2.2. *Let E''_{N-1} be defined as in Construction* 2.2. *Then*

$$W(E''_{N-1}) \ll \deg(g) q^{1/2} \log q \log N,$$
$$C_k(E''_{N-1}) \ll q^{1/2} (2 \deg(g) \log q)^k \log N,$$
$$Q_k(E''_{N-1}) \ll q^{1/2} (2 \deg(g) \log q)^k \log N.$$

REMARKS. Let p be a prime, and let $Q \in \mathcal{E}(\mathbb{F}_p)$ with order N. For $k = 1, \dots, N-1$, write $Q_k = kQ$, and consider $Q_k = (x(Q_k), y(Q_k)) \in \mathcal{E}(\mathbb{F}_p)$. Define

$$\mathcal{A}_1 = \{n : p/2 < n \le p - 1\}, \quad \mathcal{A}_2 = \{n : 1 \le n \le p - 1,\ 2 \,|\, n\}.$$

For $i = 1, \dots, 5$, denote $E^{(i)}_{N-1} = (e^{(i)}_1, \dots, e^{(i)}_{N-1})$ by

$$e^{(1)}_k = \begin{cases} +1 & \text{if } y(Q_k) \in \mathcal{A}_1, \\ -1 & \text{if } y(Q_k) \notin \mathcal{A}_1, \end{cases} \quad e^{(2)}_k = \begin{cases} +1 & \text{if } x(Q_k) \in \mathcal{A}_1, \\ -1 & \text{if } x(Q_k) \notin \mathcal{A}_1, \end{cases}$$
$$e^{(3)}_k = \begin{cases} +1 & \text{if } y(Q_k) \in \mathcal{A}_2, \\ -1 & \text{if } y(Q_k) \notin \mathcal{A}_2, \end{cases} \quad e^{(4)}_k = \begin{cases} +1 & \text{if } x(Q_k) \in \mathcal{A}_2, \\ -1 & \text{if } x(Q_k) \notin \mathcal{A}_2, \end{cases}$$
$$e^{(5)}_k = \begin{cases} +1 & \text{if } x(Q_k) < y(Q_k), \\ -1 & \text{if } x(Q_k) \ge y(Q_k). \end{cases}$$

We point out that both $\mathcal{A}_1$ and $\mathcal{A}_2$ are special cases of B in our constructions, and $x(Q_k)$, $y(Q_k)$ are both rational functions in $\mathbb{F}_p(\mathcal{E})$ satisfying $x(R) = \infty$ if and only if $R = \mathcal{O}$, and $y(R) = \infty$ if and only if $R = \mathcal{O}$. Then from Theorem 2.1 we know that the above five binary sequences are good pseudorandom binary sequences.

3. Exponential sums for elliptic curves over finite fields. Since $\mathcal{E}(\mathbb{F}_q) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/L\mathbb{Z}$, the order of P is N, and the order of Q is L, it follows that any point in $\mathcal{E}(\mathbb{F}_q)$ can be written as $nP + lQ$ with $0 \le n < N$ and $0 \le l < L$. Define $\mathrm{e}(y) = e^{2\pi i y}$. Then any character ω on $\mathcal{E}(\mathbb{F}_q)$ is of the form

$$\omega(nP + lQ) = \mathrm{e}\left(\frac{an}{N}\right)\mathrm{e}\left(\frac{bl}{L}\right)$$

for some $0 \le a < N$ and $0 \le b < L$. Let $h \in \mathbb{F}_q(\mathcal{E})$ be a non-constant function. We write the divisor of poles of h as $(h)_\infty = \sum_{i=1}^{t} n_i \mathfrak{B}_i$, where $\deg(h) = \sum_{i=1}^{t} n_i \deg(\mathfrak{B}_i)$.

LEMMA 3.1. *Let ω be a character on $\mathcal{E}(\mathbb{F}_q)$, let ψ be a non-trivial additive character on $\mathbb{F}_q$, and let $h \in \mathbb{F}_q(\mathcal{E})$ be a non-constant function. Then $\psi \circ h$ determines a character of conductor $\sum_{i=1}^{t} m_i \mathfrak{B}_i$, where $m_i \le n_i + 1$ with equality if and only if $(n_i, q) = 1$. Moreover,*

$$\Big| \sum_{\substack{R \in \mathcal{H} \\ h(R) \neq \infty}} \omega(R)\psi(h(R)) \Big| \le 2 \deg(h) q^{1/2}.$$

Proof. This is Corollary 1 of [13]. ∎

Now we can give the following estimates for some special exponential sums.

LEMMA 3.2. *Let a, b, t be positive integers, and let $d_1, \dots, d_l$ be non-negative integers such that $1 \le a + jb + d_1 < \cdots < a + jb + d_l \le N - 1$. Let $r_1, \dots, r_l \in \mathbb{F}_q^*$. For a non-trivial additive character ψ on $\mathbb{F}_q$, define*

$$T_1 = \sum_{j=0}^{t} \psi(r_1 f(P_{a+jb+d_1}) + \cdots + r_l f(P_{a+jb+d_l})).$$

Then

$$T_1 \ll l \deg(f) q^{1/2} \log N.$$

Proof. It is not hard to show that

$$T_1 = \frac{1}{N} \sum_{\substack{n=0 \\ n+d_1, \dots, n+d_l \not\equiv 0 \pmod N}}^{N-1} \sum_{j=0}^{t} \psi(r_1 f(P_{n+d_1}) + \cdots + r_l f(P_{n+d_l})) \times \sum_{\lambda=0}^{N-1} \mathrm{e}(\lambda(n - (a + jb))/N)$$

$$\le \frac{1}{N}\sum_{\lambda=0}^{N-1}\Big|\sum_{j=0}^{t}\mathrm{e}(\lambda jb/N)\Big| \times \Big|\sum_{\substack{n=0\\ n+d_1,\dots,n+d_l\not\equiv 0 \,(\mathrm{mod}\, N)}}^{N-1}\mathrm{e}(\lambda n/N)\psi(r_1 f(P_{n+d_1})+\cdots+r_l f(P_{n+d_l}))\Big|.$$

Let ϕ be the character defined by $\phi(nP+lQ)=\mathrm{e}(\lambda n/N)$, and define

$$F(nP)=r_1 f(P_{n+d_1})+\cdots+r_l f(P_{n+d_l}).$$

Then

$$\sum_{\substack{n=0\\ n+d_1,\dots,n+d_l\not\equiv 0 \,(\mathrm{mod}\, N)}}^{N-1}\mathrm{e}(\lambda n/N)\psi(r_1 f(P_{n+d_1})+\cdots+r_l f(P_{n+d_l})) = \sum_{\substack{n=0\\ F(nP)\neq\infty}}^{N-1}\phi(nP)\psi(F(nP)).$$

Since $f(R)=\infty$ if and only if $R=\mathcal{O}$, we know that $F(nP)$ has l distinct poles at $n=N-d_1,\dots,N-d_l$. Thus F cannot be a constant function. So from Lemma 3.1 we have

$$\Big|\sum_{\substack{n=0\\ n+d_1,\dots,n+d_l\not\equiv 0 \,(\mathrm{mod}\, N)}}^{N-1}\mathrm{e}(\lambda n/N)\psi(r_1 f(P_{n+d_1})+\cdots+r_l f(P_{n+d_l}))\Big| \le 2l\deg(f)q^{1/2}.$$

On the other hand, we easily have

$$\sum_{\lambda=0}^{N-1}\Big|\sum_{j=0}^{t}\mathrm{e}(\lambda jb/N)\Big| \ll N\log N,$$

therefore

$$T_1 \ll l\deg(f)q^{1/2}\log N. \ \blacksquare$$

LEMMA 3.3. *Let a,b,t be positive integers, and let $d_1,\dots,d_l$ be non-negative integers such that $1\le a+jb+d_1<\cdots<a+jb+d_l\le N-1$. Let $r_1,\dots,r_l\in\mathbb{F}_q^*$. For non-trivial additive character ψ on $\mathbb{F}_q$, define*

$$T_2=\sum_{j=0}^{t}\psi(r_1\overline{g(P_{a+jb+d_1})}+\cdots+r_l\overline{g(P_{a+jb+d_l})}).$$

Then

$$T_2 \ll (\deg(g))^l q^{1/2}\log N.$$

Proof. It is easy to show that

$$T_1 = \frac{1}{N} \sum_{\substack{n=0 \\ n+d_1,\dots,n+d_l \not\equiv 0 \,(\mathrm{mod}\, N)}}^{N-1} \sum_{j=0}^{t} \psi(r_1\overline{g(P_{n+d_1})} + \cdots + r_l\overline{g(P_{n+d_l})})$$
$$\times \sum_{\lambda=0}^{N-1} \mathrm{e}(\lambda(n-(a+jb))/N)$$
$$\le \frac{1}{N} \sum_{\lambda=0}^{N-1} \Big| \sum_{j=0}^{t} \mathrm{e}(\lambda jb/N) \Big|$$
$$\times \Big| \sum_{\substack{n=0 \\ n+d_1,\dots,n+d_l \not\equiv 0 \,(\mathrm{mod}\, N)}}^{N-1} \mathrm{e}(\lambda n/N)\psi(r_1\overline{g(P_{n+d_1})} + \cdots + r_l\overline{g(P_{n+d_l})}) \Big|.$$

Let ϕ be the character defined by $\phi(nP + lQ) = \mathrm{e}(\lambda n/N)$, and define

$$G(nP) = \frac{\sum_{i=1}^{l} r_i \prod_{j=1,\, j\ne i}^{l} g(P_{n+d_j})}{\prod_{j=1}^{l} g(P_{n+d_j})}.$$

Since $g(R) = 0$ if and only if $R = \mathcal{O}$, we know that $G(nP)$ has l distinct poles at $n = N - d_1, \dots, N - d_l$. Thus G cannot be a constant function. So from Lemma 3.1 we have

$$\Big| \sum_{\substack{n=0 \\ n+d_1,\dots,n+d_l \not\equiv 0 \,(\mathrm{mod}\, N)}}^{N-1} \mathrm{e}(\lambda n/N)\psi(r_1\overline{g(P_{n+d_1})} + \cdots + r_l\overline{g(P_{n+d_l})}) \Big|$$
$$= \Big| \sum_{\substack{n=0 \\ G(nP)\ne\infty}}^{N-1} \phi(nP)\psi(G(nP)) \Big| \le 2(\deg(g))^l q^{1/2}.$$

Therefore $T_2 \ll (\deg(g))^l q^{1/2} \log N$. ∎

4. Proof of the pseudorandom properties. First we prove Theorem 2.1. Let ψ_1 be the canonical additive character of $\mathbb{F}_q$. Noting that

$$2\Big(\frac{1}{q} \sum_{c\in B} \sum_{r\in\mathbb{F}_q} \psi_1(r(x-c)) - \frac{1}{2}\Big) = \begin{cases} +1 & \text{if } x \in B, \\ -1 & \text{if } x \notin B, \end{cases}$$

we have

$$\sum_{j=0}^{t} e'_{a+jb+d_1} \cdots e'_{a+jb+d_k}$$
$$= 2^k \sum_{j=0}^{t} \prod_{i=1}^{k} \Big(\frac{1}{q} \sum_{c\in B} \sum_{r\in\mathbb{F}_q} \psi_1(r(f(P_{a+jb+d_i}) - c)) - \frac{1}{2}\Big).$$

Since $|B| = (q-1)/2$, we get

$$\frac{1}{q}\sum_{c\in B} 1 - \frac{1}{2} = -\frac{1}{2q},$$

therefore

$$\begin{aligned}
&\sum_{j=0}^{t} e'_{a+jb+d_1}\cdots e'_{a+jb+d_k}\\
&= \frac{2^k}{q^k}\sum_{j=0}^{t}\prod_{i=1}^{k}\Big(\sum_{c\in B}\sum_{r\in\mathbb{F}_q^*}\psi_1\big(r(f(P_{a+jb+d_i})-c)\big)-\frac{1}{2}\Big)\\
&= \frac{2^k}{q^k}\sum_{j=0}^{t}\sum_{l=0}^{k}\Big(-\frac{1}{2}\Big)^{k-l}\sum_{(c_1,\dots,c_l)\in B^l}\ \sum_{(r_1,\dots,r_l)\in(\mathbb{F}_q^*)^l}\\
&\qquad\sum_{1\le i_1<\cdots<i_l\le k}\psi_1\big(r_1(f(P_{a+jb+d_{i_1}})-c_1)+\cdots+r_l(f(P_{a+jb+d_{i_l}})-c_l)\big)\\
&= \frac{1}{q^k}\sum_{l=0}^{k}(-1)^{k-l}2^l\\
&\qquad\times\sum_{(r_1,\dots,r_l)\in(\mathbb{F}_q^*)^l}\ \sum_{1\le i_1<\cdots<i_l\le k}\ \sum_{j=0}^{t}\psi_1\big(r_1f(P_{a+jb+d_{i_1}})+\cdots+r_lf(P_{a+jb+d_{i_l}})\big)\\
&\qquad\times\sum_{(c_1,\dots,c_l)\in B^l}\psi_1(-r_1c_1-\cdots-r_lc_l).
\end{aligned}$$

Noting that

$$\sum_{r\in\mathbb{F}_q^*}\Big|\sum_{c\in B}\psi_1(rc)\Big| \ll q\log q,$$

from Lemma 3.2 we have

$$\begin{aligned}
&\sum_{j=0}^{t} e'_{a+jb+d_1}\cdots e'_{a+jb+d_k}\\
&\qquad\ll \frac{1}{q^k}\sum_{l=0}^{k}2^l\binom{k}{l}l\deg(f)q^{1/2}\log N\Big(\sum_{r\in\mathbb{F}_q^*}\Big|\sum_{c\in B}\psi_1(rc)\Big|\Big)^l\\
&\qquad\ll \frac{1}{q^k}\,k\deg(f)q^{1/2}\log N\sum_{l=0}^{k}\binom{k}{l}2^l(q\log q)^l\\
&\qquad= \frac{1}{q^k}\,k\deg(f)q^{1/2}\log N(2q\log q+1)^k\\
&\qquad\ll k\deg(f)q^{1/2}(2\log q)^k\log N.
\end{aligned}$$

Therefore

$$Q_k(E'_{N-1}) = \max_{a,b,t,D}\Big|\sum_{j=0}^{t} e'_{a+jb+d_1}\cdots e'_{a+jb+d_k}\Big| \ll k\deg(f)q^{1/2}(2\log q)^k\log N. \tag{4.1}$$

Taking $k=1$ and $d_1=0$ in (4.1), we immediately get

$$W(E'_{N-1}) = \max_{a,b,t}\Big|\sum_{j=0}^{t-1} e'_{a+jb}\Big| \ll \deg(f)q^{1/2}\log q\log N.$$

Taking $a=0$, $b=1$, $j=n-1$ and $t=M-1$ in (4.1), we have

$$C_k(E'_{N-1}) = \max_{M,D}\Big|\sum_{n=1}^{M} e'_{n+d_1}\cdots e'_{n+d_k}\Big| \ll k\deg(f)q^{1/2}(2\log q)^k\log N.$$

This proves Theorem 2.1. Using the same methods and Lemma 3.3 we can complete the proof of Theorem 2.2.

Acknowledgments. The authors express their gratitude to the referee for his detailed comments.

This research was supported by the National Grand Fundamental Research 973 Programs of China under Grant 2007CB807902 and 2007CB807903, the China Postdoctoral Science Foundation funded project under Grant 20070421084 and 200801410, and the Specialized Research Fund for the Post Doctorates of Shandong Province under Grant 200702036.

References

[1] P. H. T. Beelen and J. M. Doumen, *Pseudorandom sequences from elliptic curves*, in: Finite Fields with Applications to Coding Theory, Cryptography and Related Areas (Oaxaca, 2001), Springer, 2002, 37–52.

[2] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, *On finite pseudorandom binary sequences III: The Liouville function, I*, Acta Arith. 87 (1999), 367–390.

[3] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, ibid. 103 (2002), 97–118.

[4] G. Gong, T. A. Berson and D. R. Stinson, *Elliptic curve pseudorandom sequence generators*, in: Selected Areas in Cryptography (Kingston, ON, 1999), Springer, 2000, 34–48.

[5] G. Gong and C. C. Y. Lam, *Linear recursive sequences over elliptic curves*, in: Sequences and their Applications (Bergen, 2001), Springer, 2002, 182–196.

[6] L. Goubin, C. Mauduit and A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56–69.

[7] K. Gyarmati, *On a family of pseudorandom binary sequences*, Period. Math. Hungar. 49 (2004), 45–63.

[8] S. Hallgren, *Linear congruential generators over elliptic curves*, Technical Report CS94-143, Cornegie Mellon Univ., 1994.
[9] F. Hess and I. Shparlinski, *On the linear complexity and multidimensional distribution of congruential generators over elliptic curves*, Designs Codes Cryptogr. 35 (2005), 111–117.
[10] H. Hu, L. Hu and D. Feng, *On a class of pseudorandom sequences from elliptic curves over finite fields*, IEEE Trans. Inform. Theory 53 (2007), 2598–2605.
[11] P. Hubert, C. Mauduit and A. Sárközy, *On pseudorandom binary lattices*, Acta Arith. 125 (2006), 51–62.
[12] B. S. Kaliski, *A pseudorandom bit generator based on elliptic logarithms*, in: Lecture Notes in Comput. Sci. 263, Springer, 1986, 84–103.
[13] D. Kohel and I. Shparlinski, *On exponential sums and group generators for elliptic curves over finite fields*, in: Lecture Notes in Comput. Sci. 1838, Springer, 2000, 395–404.
[14] H. Liu, *New pseudorandom sequences constructed by quadratic residues and Lehmer numbers*, Proc. Amer. Math. Soc. 135 (2007), 1309–1318.
[15] —, *A family of pseudorandom binary sequences constructed by the multiplicative inverse*, Acta Arith. 130 (2007), 167–180.
[16] E. E. Mahassni and I. Shparlinski, *On the uniformity of distribution of congruential generators over elliptic curves*, in: Sequences and their Applications (Bergen, 2001), Springer, 2002, 257–264.
[17] C. Mauduit, J. Rivat and A. Sárközy, *Construction of pseudorandom binary sequences using additive characters*, Monatsh. Math. 141 (2004), 197–208.
[18] C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences I: Measure of pseudorandomness, the Legendre symbol*, Acta Arith. 82 (1997), 365–377.
[19] —, —, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239–252.
[20] —, —, *On large families of pseudorandom binary lattices*, Uniform Distribution Theory 2 (2007), 23–37.
[21] —, —, *Construction of pseudorandom binary lattices by using the multiplicative inverse*, Monatsh. Math. 153 (2008), 217–231.
[22] C. P. Xing, *Constructions of sequences from algebraic curves over finite fields*, in: Sequences and their Applications (Bergen, 2001), Springer, 2002, 88–100.
[23] C. P. Xing, P. V. Kumar and C. S. Ding, *Low correlation, large linear span sequences from function fields*, IEEE Trans. Inform. Theory 49 (2003), 1439–1446.

School of Mathematics and System Sciences
Shandong University
Jinan, Shandong, P.R. China
E-mail: hnliumath@hotmail.com
zhantao@sdu.edu.cn
xywang@sdu.edu.cn

Received on 30.5.2008
and in revised form on 11.6.2009 (5722)