‘Good’ Pseudo-Random Binary Sequences from Elliptic Curves*

Zhixiong CHEN[1,2]†, Guozhen XIAO[1]

(1. National Key Lab. of ISN, Xidian Univ., Xi’an 710071, China
2. Depart. of Math., Putian Univ., Putian, Fujian 351100, China)

Abstract. Some families of binary sequences are constructed from elliptic curves. Such sequences are shown to be of strong pseudorandom properties with ‘small’ well-distribution measure and ‘small’ correlation measure of ‘small’ order, both of which were introduced by Mauduit and Sárközy to analyze the pseudo-randomness of binary sequences.
Keywords. pseudorandom sequences, elliptic curves, exponential sums, well-distribution, correlation.

1 Introduction

Mauduit and Sárközy [15] introduced several measures to evaluate the (local) pseudo-randomness of a finite binary sequence:

$$S_N = \{s_1, s_2, \cdots, s_N\} \in \{+1, -1\}^N.$$

The most two important measures are the well-distribution measure and the correlation measure of order k.

The *well-distribution measure* of S_N is defined as

$$W(S_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} s_{a+jb} \right|,$$

where the maximum is taken over all a, b, t such that $a, b, t \in \mathbb{N}$ and $1 \le a \le a + (t-1)b \le N$, while the *correlation measure of order* k (or *order* k *correlation measure*) of S_N is defined as

$$C_k(S_N) = \max_{M,D} \left| \sum_{n=1}^{M} s_{n+d_1} s_{n+d_2} \cdots s_{n+d_k} \right|,$$

where the maximum is taken over all $D = (d_1, \cdots, d_k)$ with non-negative integers $0 \le d_1 < \cdots < d_k$ and M such that $M + d_k \le N$.

S_N is considered as a “good” pseudo-random sequence, if both $W(S_N)$ and $C_k(S_N)$ (at least for small k) are “small” in terms of N (in particular, both are $o(N)$ as $N \to \infty$). It was shown

*Supported in part by the Science and Technology Foundation of Putian City (No. 2005S04).
†Corresponding author’s email: ptczx@126.com

in [2] that for a "truely" random sequence $S_N \in \{+1, -1\}^N$ (i.e., choosing $S_N \in \{+1, -1\}^N$ with probability $1/2^N$), both $W(S_N)$ and $C_k(S_N)$ (for some fixed k) are around $N^{1/2}$ with "near 1" probability.

For the Legendre sequence $S_p = \{s_1, s_2, \cdots, s_p\} \in \{+1, -1\}^p$ with

$$s_n = \begin{cases} \left(\frac{n}{p}\right), & \text{if } \gcd(n,p) = 1; \\ 1, & \text{if } p|n, \end{cases}$$

it was shown by Mauduit and Sárközy in [15] that

$$W(S_p) = O(p^{1/2}\log(p)) \quad \text{and} \quad C_k(S_p) = O(kp^{1/2}\log(p)),$$

which indicate that the Legendre sequence forms a "good" pseudo-random sequence. Many other "good" (but slightly inferior) binary sequences were designed in the literature, see for example [2, 3, 7, 8, 16, 18, 19] and references therein.

Recent developments point towards an interest in the elliptic curve analogues of pseudo-random number generators, see [1, 5, 6, 9, 10, 11, 12, 13, 14, 17, 20, 22] and references therein. Such number generators provide strong potential applications in cryptography for generating pseudo-random numbers and session keys.

Following the idea of Mauduit and Sárközy, we will apply elliptic curves to construct some families of binary sequences and analyze their pseudorandomness in the present paper.

We first introduce some notions and basic facts of elliptic curves over finite fields. Let $p > 3$ be a prime and $\mathbb{F}_p$ the finite field of p elements, which we identify with the set $\{0, 1, \cdots, p-1\}$. $\mathbb{F}_p^*$ is the set of non-zero elements of $\mathbb{F}_p$. Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$, given by an affine Weierstrass equation of the standard form

$$y^2 = x^3 + ax + b, \tag{1}$$

with coefficients $a, b \in \mathbb{F}_p$ and nonzero discriminant, see [4]. It is known that the set $\mathcal{E}(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points of $\mathcal{E}$ forms an Abelian group under an appropriate composition rule denoted by $\oplus$ and with the point at infinity $\mathcal{O}$ as the neutral element. We recall that

$$|\#\mathcal{E}(\mathbb{F}_p) - p - 1| \leq 2p^{1/2},$$

where $\#\mathcal{E}(\mathbb{F}_p)$ is the number of $\mathbb{F}_p$-rational points, including the point at infinity $\mathcal{O}$. Let $G \in \mathcal{E}(\mathbb{F}_p)$ be a point of order N, that is, N is the size of the cyclic group $\langle G \rangle$ generated by G. A multiple of a point P is taken by $nP = \oplus_{i=1}^{n} P$. We write $iG = (x_i, y_i) \in \mathbb{F}_p \times \mathbb{F}_p$ on $\mathcal{E}$ for all $1 \leq i \leq N-1$.

We build five types of finite binary sequences $S_{N-1} = \{s_1, \cdots, s_{N-1}\}$:

$$\text{Construction I}: \quad s_i := \begin{cases} 1, & y_i > \frac{p}{2}; \\ 0, & \text{otherwise.} \end{cases}$$

$$\text{Construction II}: \quad s_i := \begin{cases} 1, & x_i > \frac{p}{2}; \\ 0, & \text{otherwise.} \end{cases}$$

$$\text{Construction III}: \quad s_i := \begin{cases} 1, & y_i \text{ is even}; \\ 0, & \text{otherwise.} \end{cases}$$

$$\text{Construction IV}: \quad s_i := \begin{cases} 1, & x_i \text{ is even}; \\ 0, & \text{otherwise.} \end{cases}$$

$$\text{Construction V}: \quad s_i := \begin{cases} 1, & x_i < y_i; \\ 0, & \text{otherwise.} \end{cases}$$

In fact, Construction I has been proposed in [12] and the period and the linear complexity of this sequence has also been considered.

We will prove that these constructions indeed produce 'good' pseudo-random sequences. Namely, we show that both the well-distribution measure and the correlation measure of 'small' order of the above five sequences are 'small'. The proof is based on some bounds of character sums over subgroups of the point group of elliptic curves [11].

Throughout this paper, the implied constant in the symbol " $\ll$ " may sometimes depends on the integer $\deg(f)$, the degree of a rational function f, and is absolute otherwise.

2 Preparations

Let $\mathcal{E}$ be an elliptic curve over $\mathbb{F}_p$ defined as Eq.(1). Let $f \in \mathbb{F}_p(\mathcal{E})$ be a rational function. We denote by $\deg(f)$ the degree of the pole divisor of f. In particular, $\deg(f) = 2$ if $f = x$ and $\deg(f) = 3$ if $f = y$. The translation map by $W \in \mathcal{E}(\mathbb{F}_p)$ on $\mathcal{E}(\mathbb{F}_p)$ is defined as follows:

$$\tau_W : P \mapsto P \oplus W.$$

It is obvious that $(f \circ \tau_W)(P) = f(\tau_W(P)) = f(P \oplus W)$. We denote by $\ominus$ the inverse operation of $\oplus$ in the rational points group of $\mathcal{E}$. From Lemma 3.16, Theorem 3.17 and Lemma 3.14 of [4], we have the following statement.

Lemma 1 *Let $f \in \mathbb{F}_p(\mathcal{E})$ be a rational function. If f has a pole at $H \in \mathcal{E}(\overline{\mathbb{F}}_p)$ of multiplicity ρ, then $f \circ \tau_W$ has a pole at $H \ominus W$ of the same multiplicity ρ.*

Let $e_p(z) = \exp(2\pi i z/p)$ be an additive character of $\mathbb{F}_p$. For any positive m, an additive character of $\mathbb{Z}_m := \{0, 1, \cdots, m-1\}$, the residue ring modulo m, is defined as $e_m(z) = \exp(2\pi i z/m)$. We also need the following upper bound which is a special case of Corollary 1 of [11].

Lemma 2 *Let $f \in \mathbb{F}_p(\mathcal{E})$ be a nonconstant rational function and $G \in \mathcal{E}(\mathbb{F}_p)$ be a rational point of order N. Then the bound*

$$\left| \sum_{\substack{z=0 \\ f(zG)\neq\infty}}^{N-1} e_p(\lambda f(zG)) e_N(\eta z) \right| \leq 2\deg(f) p^{1/2}$$

holds for all $\lambda \in \mathbb{F}_p^*$ and $\eta \in \mathbb{Z}_N$.

Lemma 3 *Let p be an odd prime number and $\lambda \in \mathbb{Z}$ with $0 \leq |\lambda| \leq \frac{p-1}{2}$. We define*

$$V(\lambda) := \sum_{r=0}^{(p-1)/2} e_p(-\lambda r) - \sum_{r=1}^{(p-1)/2} e_p(\lambda r), \tag{2}$$

$$U(\lambda) := \sum_{r=1}^{(p-1)/2} e_p(2\lambda r) - \sum_{r=0}^{(p-1)/2} e_p(-2\lambda r) \tag{3}$$

and

$$W(\lambda,u):=\sum_{r=0}^{u}e_p(-\lambda r)-\sum_{r=u+1}^{p-1}e_p(-\lambda r), \tag{4}$$

where $0\le u\le p-1$. *Then the following bounds hold:*

$$\sum_{|\lambda|\le(p-1)/2}|V(\lambda)|\le 2p(1+\log p)\ ;$$

$$\sum_{|\lambda|\le(p-1)/2}|U(\lambda)|\le 2p(1+\log p)\ ;$$

and

$$\sum_{|\lambda|\le(p-1)/2}|W(\lambda,u)|\le 2p(1+\log p).$$

Proof. Since $|V(\lambda)|\le\left|\sum_{r=0}^{(p-1)/2}e_p(-\lambda r)\right|+\left|\sum_{r=1}^{(p-1)/2}e_p(\lambda r)\right|$, the first desired result follows from Inequality (3.4) of [21]. The other two cases are similar. □

Lemma 4 *Let N be a positive integer, $1\le b\le N-1$ and $t\in\mathbb{N}$ with $(t-1)b\le N-1$. Then the following bound holds:*

$$\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{t-1}e_N(\lambda bx)\right|\ll N\log N.$$

Proof. Let $d=\gcd(b,N)$, $M=N/d$ and $b_1=b/d$. Since $(t-1)b\le N-1$, we have $d(t-1)\le(t-1)b<N$, and hence $t-1<M$. We derive

$$\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{t-1}e_N(\lambda bx)\right|=d\sum_{\lambda=0}^{M-1}\left|\sum_{x=0}^{t-1}e_N(\lambda bx)\right|=d\sum_{\lambda=0}^{M-1}\left|\sum_{x=0}^{t-1}e_M(\lambda b_1x)\right|\ll dM\log M.$$

Since $\gcd(M,b_1)=1$, the last inequality holds by Inequality (3.4) of [21]. □

Lemma 5 *Let $G\in\mathcal{E}(\mathbb{F}_p)$ be of order N and $f\in\mathbb{F}_p(\mathcal{E})$ a nonconstant rational function. Then for any fixed $a,b,t\in\mathbb{N}$ with $1\le a\le a+(t-1)b\le N-1$, the following bound holds:*

$$\left|\sum_{x=0}^{t-1}e_p(f((a+bx)G))\right|\ll p^{1/2}\log N.$$

Proof.

$$\begin{aligned}\left|\sum_{x=0}^{t-1}e_p(f((a+bx)G))\right| &= \left|\frac{1}{N}\sum_{n=0}^{N-1}\sum_{x=0}^{t-1}e_p(f(nG))\sum_{\lambda=0}^{N-1}e_N(\lambda(n-(a+bx)))\right|\\ &= \frac{1}{N}\left|\sum_{\lambda=0}^{N-1}\sum_{x=0}^{t-1}e_N(-\lambda(a+bx))\sum_{n=0}^{N-1}e_p(f(nG))e_N(\lambda n))\right|\\ &\le \frac{1}{N}\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{t-1}e_N(-\lambda(a+bx))\right|\cdot\left|\sum_{n=0}^{N-1}e_p(f(nG))e_N(\lambda n))\right|\\ &= \frac{1}{N}\sum_{\lambda=0}^{N-1}\left|\sum_{x=0}^{t-1}e_N(-\lambda bx)\right|\cdot\left|\sum_{n=0}^{N-1}e_p(f(nG))e_N(\lambda n))\right|.\end{aligned}$$

Now by Lemmas 2 and 4, we derive the desired result. We note that in the above formulae the poles of f must be ruled out. □

3 Pseudorandomness of Elliptic Curve Sequences

In this section we will present an upper bound respectively for the well-distribution measure $W(S_N)$ and the correlation measure $C_k(S_N)$ for binary sequences defined in Construction I-V.

Assume that f is a rational function and $f = x$ or $f = y$ in the following context. We remark that $x(iG) = x_i$ and $y(iG) = y_i$ for $iG = (x_i, y_i) \in \mathcal{E}(\mathbb{F}_p)$. For Construction I and II, for any $1 \le i \le N-1$, we have

$$\frac{1}{p}\sum_{r=1}^{(p-1)/2}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda(f(iG)+r)) = \begin{cases} 1, & p > f(iG) \ge (p+1)/2, \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

$$\frac{1}{p}\sum_{r=0}^{(p-1)/2}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda(f(iG)-r)) = \begin{cases} 0, & p > f(iG) \ge (p+1)/2, \\ 1, & \text{otherwise.} \end{cases} \tag{6}$$

Subtracting (5) from (6) yields

$$\frac{1}{p}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda f(iG))V(\lambda) = \begin{cases} -1, & p > f(iG) \ge (p+1)/2, \\ 1, & \text{otherwise.} \end{cases}$$

where $V(\lambda)$ is defined as (2) in Lemma 3. It is easy to see that

$$(-1)^{s_i} = \frac{1}{p}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda f(iG))V(\lambda), \tag{7}$$

where $f = y$ for Construction I and $f = x$ for Construction II.

While for Construction III and IV, for any $1 \le i \le N-1$, we have

$$\frac{1}{p}\sum_{r=0}^{(p-1)/2}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda(f(iG)-2r)) = \begin{cases} 1, & f(iG) \text{ is even,} \\ 0, & \text{otherwise.} \end{cases} \tag{8}$$

$$\frac{1}{p}\sum_{r=1}^{(p-1)/2}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda(f(iG)+2r)) = \begin{cases} 0, & f(iG) \text{ is even,} \\ 1, & \text{otherwise.} \end{cases} \tag{9}$$

(9)$-$(8), we get

$$\frac{1}{p}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda f(iG))U(\lambda) = \begin{cases} -1, & f(iG) \text{ is even,} \\ 1, & \text{otherwise.} \end{cases}$$

where $U(\lambda)$ is defined as (3) in Lemma 3. Similar to (7), we obtain

$$(-1)^{s_i} = \frac{1}{p}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda f(iG))U(\lambda), \tag{10}$$

where $f = y$ for Construction III and $f = x$ for Construction IV.

For Construction V, the following two formulae hold for all x_i with $0 \le x_i \le p-1$:

$$\frac{1}{p}\sum_{r=x_i+1}^{p-1}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda(y_i-r)) = \begin{cases} 1, & x_i < y_i, \\ 0, & \text{otherwise.} \end{cases} \tag{11}$$

$$\frac{1}{p}\sum_{r=0}^{x_i}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda(y_i-r)) = \begin{cases} 0, & x_i < y_i, \\ 1, & \text{otherwise.} \end{cases} \tag{12}$$

(12)−(11), we get

$$\frac{1}{p}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda y_i)W(\lambda, x_i) = \begin{cases} -1, & x_i < y_i, \\ 1, & \text{otherwise.} \end{cases}$$

where $W(\lambda, x_i)$ is defined as (4) in Lemma 3. Hence we obtain

$$(-1)^{s_i} = \frac{1}{p}\sum_{|\lambda|\le(p-1)/2} e_p(\lambda y_i)W(\lambda, x_i). \tag{13}$$

Theorem 1 *Assume that $G \in \mathcal{E}(\mathbb{F}_p)$ is a point of order N and S_{N-1} is one of binary sequences obtained from Construction $\mathrm{I}-\mathrm{V}$. Then the well-distribution measure of S_{N-1} holds:*

$$W(S_{N-1}) \ll p^{1/2}\log p \log N.$$

Proof. We only prove the statement for S_{N-1} obtained from Construction I and II. Combining with (10), (13) and Lemma 3, one can prove the other three cases in a similar way. For any $a, b, t \in \mathbb{N}$ with $1 \le a \le a+(t-1)b \le N-1$, from (7) we have

$$\begin{aligned}
\left|\sum_{j=0}^{t-1}(-1)^{s_{a+jb}}\right| &= \frac{1}{p}\left|\sum_{j=0}^{t-1}\sum_{|\lambda|\le(p-1)/2} V(\lambda)e_p(\lambda f((a+jb)G))\right| \\
&= \frac{1}{p}\left|\sum_{|\lambda|\le(p-1)/2} V(\lambda)\sum_{j=0}^{t-1} e_p(\lambda f((a+jb)G))\right| \\
&\le \frac{1}{p}\sum_{|\lambda|\le(p-1)/2} |V(\lambda)|\cdot\left|\sum_{j=0}^{t-1} e_p(\lambda f((a+jb)G))\right| \\
&\le \frac{1}{p}\left(\sum_{|\lambda|=1}^{(p-1)/2} |V(\lambda)|\cdot\left|\sum_{j=0}^{t-1} e_p(\lambda f((a+jb)G))\right| + t\right).
\end{aligned}$$

Now by Lemmas 3 and 5, we obtain the desired result. □

Theorem 2 *Assume that $G \in \mathcal{E}(\mathbb{F}_p)$ is a point of order N and S_{N-1} is one of binary sequences obtained from Construction $\mathrm{I}-\mathrm{V}$. Then the correlation measure of order k ($k < p$) holds:*

$$C_k(S_{N-1}) \ll k2^k p^{1/2}(\log p)^k \log N.$$

Proof. Similar to Theorem 1, we only prove the statement for S_{N-1} obtained from Construction I and II. For $D = (d_1, \cdots, d_k)$ and M with $0 \le d_1 < \cdots < d_k \le N-1-M$, we have

$$\begin{aligned}
&\left|\sum_{n=1}^{M}(-1)^{s_{n+d_1}+\cdots+s_{n+d_k}}\right| \\
= &\left|\sum_{n=1}^{M}\prod_{i=1}^{k}\left(\frac{1}{p}\sum_{|\lambda_i|\le(p-1)/2}V(\lambda_i)e_p(\lambda_i f((n+d_i)G))\right)\right| \\
= &\frac{1}{p^k}\left|\sum_{|\lambda_1|\le(p-1)/2}\cdots\sum_{|\lambda_k|\le(p-1)/2}V(\lambda_1)\cdots V(\lambda_k)\sum_{n=1}^{M}e_p(\sum_{i=1}^{k}\lambda_i f((n+d_i)G))\right| \\
\le &\frac{1}{p^k}\left(2k\deg(f)p^{1/2}\log N\left(\sum_{|\lambda|\le(p-1)/2}|V(\lambda)|\right)^k + M\right).
\end{aligned}$$

The last inequality holds since the degree of the rational function $\sum_{i=1}^{k} f\circ\tau_{d_iG}$ is at most $k\deg(f)$ by Lemma 1. The desired result follows from Lemmas 3 and 5. □

Theorems 1 and 2 indicate that the five types binary sequences are "good" sequences. But it seems that they are slightly inferior to Legendre sequences.

There are a large family of elliptic curves over $\mathbb{F}_p$ with a rational point of large order N. In particular, if $\mathcal{E}(\mathbb{F}_p)$ is a cyclic group, then $N \sim p$. As indicated in [10], from Corollary 6.2 of [23], about 75% of the majority of (isomorphism classes of) elliptic curves have a cyclic point group. By Theorem 2.1 of [23], every cyclic group of order N satisfying $p-1-2p^{1/2} \le N \le p-1+2p^{1/2}$ can be realized as the point group of an elliptic curve over $\mathbb{F}_p$ $(p > 5)$. An elliptic curve with a rational point of large prime order is necessary for elliptic curve cryptosystems. More information on elliptic curves with cyclic groups can be found in [23, 24].

4 Final Remarks

Indeed, Goubin et al. presented these constructions in an original version of their paper [7]. They only listed some examples there and proposed a conjecture that such binary sequences have 'small' well-distribution measure and 'small' correlation measure of order k (for some small value k). But in the version available these contents were dropped.

References

[1] P. H. T. Beelen and J. M. Doumen. Pseudorandom sequences from elliptic curves. Finite Fields with Applications to Coding Theory, Cryptography and Related Areas. Berlin: Springer-Verlag, 2002, pp.37-52.

[2] J. Cassaigne, C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences, VII: the measures of pseudorandomness. Acta Arithmetica 103 (2002) 97–118.

[3] Z. Chen, S. Li, G. Xiao, Construction of pseudo-random binary sequences from elliptic curves by using discrete logarithm, Proc. Intern. Conf. on Sequences and Their Applications-SETA'06, LNCS 4086, Berlin : Springer-Verlag, 2006, 285-294.

[4] A. Enge. Elliptic curves and their applications to cryptography: an introduction. Kluwer Academic Publishers, Dordrecht, 1999.

[5] G. Gong, T. Berson and D. Stinson. Elliptic curve pseudorandom sequence generator. Available at http://www.cacr.math.uwaterloo.ca, Technical Reports, CORR1998-53, 1998.

[6] G. Gong and C. Lam. Linear recursive sequences over elliptic curves. Proceedings of Sequences and Their Applications-SETA'01. DMTCS series. Berlin: Spring-Verlag, 2001, pp.182-196.

[7] L.Goubin, C. Mauduit and A. Sárközy. Construction of large families of pseudorandom binary sequences. J. Number Theory, 106(1) (2004) 56-69.

[8] K. Gyarmati, On a family of pseudorandom binary sequences, Periodica Mathematica Hungarica 49(2) (2004) 45–63.

[9] S. Hallgren. Linear congruential generators over elliptic curves. Technical Report CS-94-143, Cornegie Mellon University, 1994.

[10] F. Hess and I. E. Shparlinski. On the linear complexity and multidimensional distribution of congruential generators over elliptic curves. Designs, Codes and Cryptography 35(1) (2005) 111-117.

[11] D. Kohel and I. E. Shparlinski. Exponential sums and group generators for elliptic curves over finite fields. Proc. Algorithmic Number Theory Symposium, Leiden, 2000, LNCS 1838, Berlin: Springer-Verlag, pp.395-404.

[12] C. Y. Lam and G. Gong. Randomness of elliptic curve sequences. Available at http:// www.cacr.math.Uwaterloo.ca, Technical Reports, CORR 2002-18, 2002.

[13] T. Lange and I. E. Shparlinski. Certain exponential sums and random walks on elliptic curves. Canad. J. Math., 57(2) (2005) 338-350.

[14] L. Lee and K. Wong. An elliptic curve random number generator. In Communications and Multimedia Security Issues of the new Century, Fifth Joint Working Conference on Communications and Multimedia Security (CMS'01), 2001, pp.127-133.

[15] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences I: measures of pseudorandomness, the Legendre symbol, Acta Arithmetica 82 (1997) 365–377.

[16] C. Mauduit, J. Rivat and A. Sárközy. Construction of Pseudorandom Binary Sequences Using Additive Characters. Mh. Math. 141(3) (2004) 197-208.

[17] E. El Mahassni and I. E. Shparlinski. On the uniformity of distribution of congruential generators over elliptic curves. Proc. Intern. Conf. on Sequences and their Applications (SETA'01), Bergen, London: Springer-Verlag, 2002, pp.257-264.

[18] J. Rivit, A. Sárközy, Modular constructions of pseudorandom binary sequences with composite moduli, Periodica Math. Hungarica 51(2) (2005) 75–107.

[19] A. Sárközy, A finite pseudorandom binary sequence, Studia Sci. Math. Hungarica 38(1-4) (2001) 377–384.

[20] I. E. Shparlinski. On the Naor-Reingold pseudo-random number function from elliptic curves. Appl. Algebra Engng. Comm. Comput. 11(1) (2000) 27-34.

[21] I. E. Shparlinski. Cryptographic applications of analytic number theory: complexity lower bounds and pseudorandomness. Progress in Computer Science and Applied Logic, Vol.22, Birkhauser Verlag, Basel, 2003.

[22] I. E. Shparlinski and J. H. Silverman. On the linear complexity of the Naor-Reingold pseudo-random function from elliptic curves. Designs, Codes and Cryptography, 24(3) (2001) 279-289.

[23] S. G. Vlăduţ. Cyclicity statistics for elliptic curves over finite fields. Finite Fields and Their Applications, 5(1) (1999) 13-25.

[24] S. G. Vlăduţ. On the cyclicity of elliptic curves over finite field extensions. Finite Fields and Their Applications, 5 (1999) 354-363.