Linear Recursive Sequences over Elliptic Curves

Guang Gong[1] and Charles C.Y. Lam[2]

[1] Department of Electrical and Computer Engineering
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
ggong@cacr.uwaterloo.ca

[2] Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
cy3lam@cacr.uwaterloo.ca

Abstract. In this paper, we introduce linear feedback shift register sequences (LFSR) over the group of the elliptic curve points, and a construction of binary sequences obtained from these LFSR sequences. The former is called *LFSR-EC sequences*. Properties on representation, period, and linear span of these two types of sequences are discussed. Also, the even case for the elliptic curve sequence proposed in [5] is analysed.

1 Introduction

Since Koblitz and Miller [11,15] proposed using elliptic curves over $\mathbb{F}_q$ to construct public-key cryptosystems, elliptic curve public-key cryptosystems over $\mathbb{F}_{2^l}$ or $\mathbb{F}_q$ have become widely used in applications such as smart cards which provide limited space for implementation of modular computations. Currently, the operations of points on elliptic curves over $\mathbb{F}_{2^l}$ or $\mathbb{F}_q$ have a well-developed technology in both hardware and software implementations.

Linear recursive sequences (or equivalently, linear feedback shift register sequences) over $\mathbb{F}_p$ have a significant influence in the development of communications and cryptography. In this work, we combine elliptic curves and linear feedback shift registers to generate pseudorandom sequences which provide strong potential applications in stream ciphers and pseudorandom number generators. The motivation for such a construction comes from constrained systems or devices, for example, wireless devices which employ an elliptic curve public-key cryptosystem, then such a construction automatically provide a pseudorandom sequence (or number) generator. If these sequences have good randomness, then it can be used for generating random numbers in the elliptic curve digital signature algorithm and session key in their encryption phases.

Elliptic curve sequences with strong cryptographic properties have been studied in the literature. Kaliski [10] used the randomness criteria based on the computational complexity of the discrete log problem over the elliptic curves to construct a class of elliptic curve pseudorandom sequences. Gong, Berson and Stinson [5] discussed the linear span, period and $0-1$ distribution of the one-stage LFSR over supersingular elliptic curves over finite fields of characteristic 2. Mahassni and Shparlinski [9] obtained a general bound for the $0-1$ distribution of the one-stage LFSR on elliptic curves over finite fields. Hallgren [8] discussed some heuristics with regard to the linear congruential generator over elliptic curves. Doumen and Beelen [1] has recently proposed a method on generating binary sequences using linear recurrence relations on elliptic curves.

The paper is organised as follows. In Section 2, we introduce a construction of linear recursive sequences over the group of points on an elliptic curve over finite fields, denoted by *EC sequences* for short, and discuss their representation, decomposition and period. In Section 3, we give a construction of binary sequences obtained from EC sequences and derive their randomness properties. In Section 4, we analyse a case for the supersingular elliptic curve sequences proposed in [5].

We conclude this section with the definition of elliptic curves over finite fields and linear recursive sequences.

A. Elliptic Curves over Finite Fields

Consider $\mathbb{F}_q$ where q is a power of a prime. If the characteristic of the field is 2, an elliptic curve E over $\mathbb{F}_q$ can be written in one of the following standard forms: [14]

$$E:\ y^2 + c_3 y = x^3 + c_4 x + c_6, c_i \in \mathbb{F}_q,\ \text{if } E \text{ is supersingular, or}$$
$$E:\ y^2 + xy = x^3 + c_2 x^2 + c_6, c_i \in \mathbb{F}_q,\ \text{if } E \text{ is non} - \text{supersingular.}$$

If the characteristic is greater than 3, E can be written in the following form

$$E : y^2 = x^3 + ax + b,\ a, b \in \mathbb{F}_q.$$

The points $P = (x, y),\ x, y \in \mathbb{F}_q$ that satisfy the equation, together with a "point at infinity" denoted by $\mathcal{O}$, form an abelian group $(E, +, \mathcal{O})$ with identity element $\mathcal{O}$ (for the case where the characteristic is 3, the reader is referred to [14].)

B. Linear Recursive Sequences over rings

Let r be a positive integer and let $\mathbb{Z}_r$ be the integer residue ring modulo r. Let $f(x) = x^n - \sum_{i=0}^{n-1} c_i x^i$, $c_i \in \mathbb{Z}_r$ be a monic polynomial over $\mathbb{Z}_r$, and $\underline{\mathbf{b}} = \{b_i\}$, $b_i \in \mathbb{Z}_r$. $\underline{\mathbf{b}}$ is called an n-th order linear recursive sequence or linear feedback shift register over $\mathbb{Z}_r$ (generated by $f(x)$) if for a given n-tuple $(b_0, b_1, \ldots, b_{n-1}) \in \mathbb{Z}_r^n$,

$$b_{k+n} = \sum_{i=0}^{n-1} c_i b_{k+i},\ k = 0, 1, \ldots$$

$f(x)$ is called a *characteristic polynomial* of $\underline{\mathbf{b}}$ over $\mathbb{Z}_r$ and $(b_0, b_1, \ldots, b_{n-1})$ is called an *initial state* of $\underline{\mathbf{b}}$. The characteristic polynomial of $\underline{\mathbf{b}}$ having the least degree is called the *minimal polynomial* of $\underline{\mathbf{b}}$ and the degree of the minimal polynomial of $\underline{\mathbf{b}}$ is called the *linear span* of $\underline{\mathbf{b}}$.

The period of $f(x)$ is defined as the smallest integer t such that $f(x) \mid x^t - 1$. Let $G_{\mathbb{Z}_r}(f)$ represent the set consisting of sequences with characteristic polynomial $f(x)$. It is easy to see that for any $\underline{\mathbf{b}} \in G_{\mathbb{Z}_r}(f)$, the period of $\underline{\mathbf{b}}$ is a factor of the period of $f(x)$.

Let $V(\mathbb{Z}_r) = \{(h_0, h_1, \ldots) \mid h_i \in \mathbb{Z}_r\}$. Then $V(\mathbb{Z}_r)$ is a linear space over $\mathbb{Z}_r$ and $G_{\mathbb{Z}_r}(f)$ is a subspace of $V(\mathbb{Z}_r)$.

Fact 1 *$G_{\mathbb{Z}_r}(f)$ is a linear space over $\mathbb{Z}_r$.*

C. Trace Representation

Let $\mathrm{Tr}_p^{p^k}(x) = x + x^p + \cdots + x^{p^{k-1}}$ be a trace function from $\mathbb{F}_{p^k}$ to $\mathbb{F}_p$.

Fact 2 *Let $f(x)$ be an irreducible polynomial over $\mathbb{F}_p$ of degree n and γ be a root of $f(x)$ in an extension field of $\mathbb{F}_p$. Then for any sequence $\underline{\mathbf{b}} = \{b_i\} \in G_{\mathbb{F}_p}(f)$, there exists some $\beta \in \mathbb{F}_{p^n}$ such that*

$$b_i = \mathrm{Tr}_p^{p^n}(\beta\gamma^i), \ i = 0, 1, \ldots$$

For the theory of linear recursive sequences over rings, the reader is referred to [4] and [20]. For the treatment of linear recursive sequences over finite fields the reader is referred to [6] and [12].

2 Construction and Basic Properties of LFSR Sequences over *E*

In this section, we will introduce a concept of linear (inhomogeneous) recurring sequences of points in the group of points on an elliptic curve over $\mathbb{F}_q$ and discuss some basic properties on the representation and period.

Definition 1 *Let E be an elliptic curve over $\mathbb{F}_q$ of order r, $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_1 x - c_0 \in \mathbb{Z}_r[x]$ be a monic polynomial over $\mathbb{Z}_r$ and $\underline{\mathbf{P}} = \{P_k\}$ where $P_k = (x_k, y_k) \in E$. For fixed $c_{-1} \in \mathbb{Z}_r$ and given $(n+1)$-tuple $(Q, P_0, \ldots, P_{n-1}) \in E^{n+1}$, if the sequence satisfies the following linear recursive relation:*

$$P_{n+k} = \sum_{i=0}^{n-1} c_i P_{i+k} + c_{-1} Q, \ k = 0, 1, \ldots,$$

then $\underline{\mathbf{P}}$ is called an nth-order linear recursive sequence over E (generated by $f(x)$)*, or traditionally, an* nth-order linear feedback shift register [6] (LFSR) sequence over the elliptic curve E (generated by $f(x)$)*, or simply* EC sequence *for short; $f(x)$ is called a* characteristic polynomial *of $\underline{\mathbf{P}}$ over $\mathbb{Z}_r$ and $(Q, P_0, P_1, \ldots, P_{n-1})$ is called an initial state of $\underline{\mathbf{P}}$.*

We denote $G_E(f)$ the set consisting of all EC sequences over E with characteristic polynomial $f(x)$.

Theorem 1 *For any* $\underline{\mathbf{P}} = \{P_k\} \in G_E(f)$ *with initial state* $(\mathcal{O}, P_0, P_1, \ldots, P_{n-1})$, *the elements of* $\underline{\mathbf{P}}$ *can be represented by*

$$P_k = \sum_{i=0}^{n-1} b_{k,i} P_i, \ \ k = 0, 1, \ldots$$

where for each j *with* $0 \leq j \leq n-1$, $\underline{\mathbf{b}}_j = \{b_{k,j}\} \in G_{\mathbb{Z}_r}(f)$ *with initial states given by* $b_{k,j} = \delta_{k,j}$ *for* $0 \leq k \leq n-1$.

Proof: We have

$$P_{n+k} = \sum_{i=0}^{n-1} c_i P_{i+k}, \ \ c_i \in \mathbb{Z}_r, \ \ k = 0, 1, \cdots$$

Suppose

$$P_k = \sum_{i=0}^{n-1} b_{k,i} P_i, \ \ b_{k,i} \in \mathbb{Z}_r, \ \ k = 0, 1, \ldots$$

Obviously, initial conditions are determined by the terms $b_{k,j}$ with $0 \leq k, j \leq n-1$, where

$$b_{k,j} = \delta_{k,j} \quad \text{for } 0 \leq k, j \leq n-1.$$

Then,

$$P_k = \sum_{i=0}^{n-1} c_i P_{k-n+i} = \sum_{i=0}^{n-1} c_i \sum_{j=0}^{n-1} b_{k-n+i,j} P_j = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{n-1} c_i b_{k-n+i,j} \right) P_j.$$

Therefore, by comparing coefficients, we can take

$$b_{k,j} = \sum_{i=0}^{n-1} c_i b_{k-n+i,j}.$$

Thus $\underline{\mathbf{b}}_j \in G_{\mathbb{Z}_r}(f)$. $\square$

From Theorem 1, if the initial state of $\underline{\mathbf{P}} = \{P_k\} \in G_E(f)$ is given as $(\mathcal{O}, s_0 P, s_1 P, \ldots, s_{n-1} P)$, $s_i \in \mathbb{Z}_r$, then

$$P_k = \sum_{j=0}^{n-1} b_{k,j}(s_j P) = \left(\sum_{j=0}^{n-1} b_{k,j} s_j \right) P = a_k P, \ \ k = 0, 1, \ldots \tag{1}$$

where

$$a_k = \sum_{j=0}^{n-1} b_{k,j} s_j, \ \ k = 0, 1, \ldots$$

Define $\underline{\mathbf{a}} = \{a_k\}$. This yields $\underline{\mathbf{a}} = \sum_{j=0}^{n-1} s_j \underline{\mathbf{b}}_j$. Since $\underline{\mathbf{b}}_j \in G_{\mathbb{Z}_r}(f)$ and from Fact 1, $G_{\mathbb{Z}_r}(f)$ is a linear space, therefore $\underline{\mathbf{a}} = \sum s_j \underline{\mathbf{b}}_j \in G_{\mathbb{Z}_r}(f)$. From (1), P_k is computed by multiplying P by $a_k \pmod t$, where t is the order of P. For this special initial state, we define

$$\underline{\mathbf{a}}P = \{a_i P\}_{i \geq 0} \tag{2}$$

and $G_P(f) = \{\underline{\mathbf{a}}P \mid \underline{\mathbf{a}} \in G_{\mathbb{Z}_r}(f)\}$. We call the EC sequence $\underline{\mathbf{a}}P$ as *a single point EC sequence.*

Let $V_E = \{(a_0, a_1, \ldots) | a_i \in E\}$, then $V(E)$ is a linear space over $\mathbb{Z}_r$. Let $\{\mathcal{O}, P_0, P_1, \ldots, P_{n-1}\}$ be the initial state of the sequence $\underline{\mathbf{P}}$. From Theorem 1 and equation (2), we have

$$\underline{\mathbf{P}} = \sum_{j=0}^{n-1} \underline{\mathbf{b}}_j P_j \text{ or } \underline{\mathbf{P}} = \sum_{j=0}^{n-1} \underline{\mathbf{P}}_j,$$

where $\underline{\mathbf{P}}_j = \{b_{k,j} P_j\}_{i \geq 0}$. That is, an n-th order linear recursive sequence over the points of E with characteristic polynomial $f(x)$ and initial state $(\mathcal{O}, P_0, P_1, \ldots, P_{n-1})$ can be decomposed into the sum of n initial state points, each multiplied by a scalar factor which comes from an n-th order LFSR sequence over $\mathbb{Z}_r$ with characteristic polynomial $f(x)$.

Corollary 1 *The period of $\{P_k\}$ is a factor of the period of $f(x)$.*

Proof: Let per(f) be the smallest integer t such that $f(x) | x^t - 1$. It is easy to see that per$(\underline{\mathbf{b}}_j) \mid$ per(f). Let $t =$ per(f), then $b_{k+t,j} = b_{k,j}$, hence

$$P_{k+t} = \sum_{j=0}^{n-1} b_{k+t,j} P_j = \sum_{j=0}^{n-1} b_{k,j} P_j = P_k.$$

Therefore t is a period of $\{P_i\}$. □

In the following, we restrict ourselves into special cases where either the elliptic curves has a prime order, that is, $|E| = r$ is a prime p, or that a given point $P \in E$ has a prime order p, with $f(x)$ being an irreducible polynomial over $\mathbb{F}_p$.

Lemma 1 *Let $f(x)$ be an irreducible polynomial of degree 2 over $\mathbb{F}_p$ and γ be a root of $f(x)$ in an extension field of $\mathbb{F}_p$.*

1. *The order of E over $\mathbb{F}_q$ is p. For any $\underline{\mathbf{P}} \in G_E(f)$, the elements of $\underline{\mathbf{P}}$ can be represented by*

$$P_k = \mathrm{Tr}_p^{p^2}(\alpha\gamma^k) P_1 + \mathrm{Tr}_p^{p^2}(\beta\gamma^k) P_0$$

where

$$\alpha = \frac{-1}{\gamma^p - \gamma} \text{ and } \beta = \frac{-\gamma}{\gamma^p - \gamma},$$

both as elements in the quadratic extension of $\mathbb{Z}_p$.

2. *Let $P \in E$ with order p and $P_1 = tP$ and $P_0 = sP$, $t, s \in \mathbb{Z}_p$, then*

$$P_k = \mathrm{Tr}_p^{p^2}((t\alpha + s\beta)\gamma^k)P, \ k = 0, 1, \ldots$$

Proof: Note that the two roots of $f(x)$ are γ and γ^p. From Theorem 1,

$$P_k = b_{k,0}P_0 + b_{k,1}P_1,$$

where $\underline{\mathbf{b}}_j = \{b_{k,j}\} \in G_{\mathbb{F}_p}(f)$, $j = 0, 1$. Since $f(x)$ is irreducible, according to Fact 2, $\underline{\mathbf{b}}_j$ has the following trace representation:

$$b_{k,0} = \mathrm{Tr}_p^{p^2}(\rho_0\gamma^k) = \rho_0\gamma^k + \rho_0^p\gamma^{pk}$$
$$b_{k,1} = \mathrm{Tr}_p^{p^2}(\rho_1\gamma^k) = \rho_1\gamma^k + \rho_1^p\gamma^{pk}, \ \rho_i \in \mathbb{F}_{p^2}, \ i = 0, 1$$

with initial conditions

$$\begin{pmatrix} b_{0,0} \\ b_{1,0} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ and } \begin{pmatrix} b_{0,1} \\ b_{1,1} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Solving, we have

$$\rho_0 = \frac{\gamma^p}{\gamma^p - \gamma} \text{ and } \rho_1 = \frac{-1}{\gamma^p - \gamma}.$$

Therefore

$$\begin{aligned} P_k &= b_{k,1}P_1 + b_{k,0}P_0 \\ &= (\frac{-\gamma^k}{\gamma^p - \gamma} + \frac{\gamma^{pk}}{\gamma^p - \gamma})P_1 + (\frac{\gamma^p}{\gamma^p - \gamma}\gamma^k + \frac{-\gamma}{\gamma^p - \gamma}\gamma^{pk})P_0 \\ &= \mathrm{Tr}_p^{p^2}(\alpha\gamma^k)P_1 + \mathrm{Tr}_p^{p^2}(\beta\gamma^k)P_0. \end{aligned}$$

□

In a more general case where $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_p$, we have the following results.

Theorem 2 *Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_p$ and γ be a root of $f(x)$ in an extension field of $\mathbb{F}_p$.*

1. *The order of E over $\mathbb{F}_q$ is p. For any $\underline{\mathbf{P}} \in G_E(f)$, with initial state $(\mathcal{O}, P_0, P_1, \ldots, P_{n-1})$, the elements of $\underline{\mathbf{P}}$ can be represented as*

$$P_k = \sum_{i=0}^{n-1} \mathrm{Tr}_p^{p^n}(\alpha_i\gamma^k)P_i,$$

where $\alpha_i \in \mathbb{F}_{p^n}$, $i = 0, 1, \ldots n-1$, with $(\alpha_0, \alpha_1, \ldots, \alpha_{n-1})$ given by the first row of B^{-1} where

$$B = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \gamma & \gamma^p & \cdots & \gamma^{p^{n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma^{n-1} & \gamma^{(n-1)p} & \cdots & \gamma^{(n-1)p^{n-1}} \end{bmatrix}. \quad (3)$$

2. *Let* $P \in E$ *with order* p *and* $P_i = s_i P$ *for* $i = 0, 1, \ldots n-1$ *and* $s_i \in \mathbb{Z}_p$, *then*

$$P_k = \mathrm{Tr}_p^{p^n}(\beta\gamma^k)P, \tag{4}$$

where

$$\beta = \sum_{i=0}^{n-1} s_i \mathrm{Tr}_p^{p^n}(\alpha_i).$$

Proof: Using the similar approach as in the proof of Lemma 1, we have for $0 \leq i \leq n-1$,

$$b_{k,i} = \mathrm{Tr}_p^{p^n}(\alpha_i\gamma^k),\ \ k = 0, 1, \ldots \tag{5}$$

with $0 \leq i \leq n-1$. From Theorem 1,

$$b_{k,i} = \delta_{k,i},\ \ 0 \leq i, k \leq n-1. \tag{6}$$

Let $M = (b_{ki})_{n\times n}$. From (5), we have $M = AB$ where

$$A = \begin{bmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{n-1} \\ \alpha_0^p & \alpha_1^p & \cdots & \alpha_{n-1}^p \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{p^{n-1}} & \alpha_1^{p^{n-1}} & \cdots & \alpha_{n-1}^{p^{n-1}} \end{bmatrix},$$

and B is given by (3). From (6), we have $M = I$ where I is the $n \times n$ identity matrix. Thus $AB = I$. The assertion is established. $\square$

Note : For a single point EC sequence associated with P, the representation in (4) requires the subgroup generated by the point P has prime order p, instead of requiring the order of E to be prime.

3 Binary Sequences Obtained from EC Sequences

In this section, we give the construction of a class of periodic binary sequences obtained from EC sequences, and derive the linear span for some special characteristic polynomials. We first introduce two operators on E which map the points of E to $\mathbb{F}_2^2$ and $\mathbb{F}_2$. Let

$$\tau : E \to \mathbb{F}_2,\ \text{ and }\ \delta : E \to \mathbb{F}_2^2$$

defined as follows: for $P \in E$, if $P = \mathcal{O}$, then

$$\tau(P) = 0 \text{ and } \delta(P) = (0, 0).$$

Otherwise, let $P = (x, y)$, if E is an elliptic curve over $\mathbb{F}_{2^l}$, then

$$\tau(P) = \mathrm{Tr}_2^{2^l}(y) \text{ and } \delta(P) = (\mathrm{Tr}_2^{2^l}(x), \mathrm{Tr}_2^{2^l}(y));$$

and if E is an elliptic curve over $\mathbb{F}_q$ where q is a prime > 3, then

$$\tau(P) = h(y) \text{ and } \delta(P) = (h(x), h(y)),$$

where $h(x)$ is a function which takes the *most significant bit* of an integer a modulo q:

$$h(a) = \begin{cases} 0, \; 0 \leq a \leq \frac{q-1}{2} \\ 1, \text{ otherwise.} \end{cases}$$

Let $|E| = r$, $f(x)$ be a monic polynomial over $\mathbb{Z}_r$ and $\underline{\mathbf{P}} \in G_E(f)$. Recall that $\underline{\mathbf{P}} = \{P_i\}_{i\geq 0}$ with $P_i = (x_i, y_i)$. Define *binary sequences* $\underline{\mathbf{u}} = \{u_i\}$ and $\underline{\mathbf{s}} = \{s_i\}$ as follows:

$$u_i = \tau(P_i), \; i = 0, 1, \ldots$$
$$(s_{2i}, s_{2i+1}) = \delta(P_i), \; i = 0, 1, \ldots$$

We call $\underline{\mathbf{u}}$ an EC bit sequence of y-coordinate (associated with $f(x)$) and $\underline{\mathbf{s}}$ an EC bit sequence (associated with $f(x)$) respectively.

Remark 1 *While $\underline{\mathbf{s}}$ seems to be more efficient over $\underline{\mathbf{u}}$ due to a higher output rate, $\underline{\mathbf{s}}$ is however not desirable for non-supersingular curves E over $\mathbb{F}_{2^l}$. For a non-supersingular curve E over $\mathbb{F}_{2^l}$,*

$$E : y^2 + xy = x^3 + c_2x^2 + c_6, \; c_2, c_6 \in \mathbb{F}_{2^l},$$

from [19, Proposition 91], we know that a point (x, y) on the curve is a double of another point, that is, $(x, y) = 2(z, w)$ for some $(z, w) \in E$ if an only if

$$\mathrm{Tr}_2^{2^l}(x) = \mathrm{Tr}_2^{2^l}(c_2).$$

Hence the subsequence $\{s_{2i}\}_{i\geq 0}$ would be $(0000\cdots)$, $(1111\cdots)$, $(1010\cdots)$, or $(0101\cdots)$.

Remark 2 *$\underline{\mathbf{s}}$ is the EC sequence studied in [5] with E being a supersingular curve over $\mathbb{F}_{2^l}$ where l is odd and $f(x) = x - 1$. We will study the $0 - 1$ distribution of $\underline{\mathbf{s}}$ when l is even in Section 4.*

Example 1 (curve defined on $\mathbb{F}_q$). Consider the curve $E_1 : y^2 = x^3 + x + 4$ over $\mathbb{F}_{23}$. This curve has order 29 and is cyclic. Here $q = 23$ and take $p = 29$. Let $P = (4, 7)$ be a point on E_1. The points, together with the map δ, is listed below.

Choose $f(x) = x^2 - 28x - 26 \in \mathbb{Z}_{29}[x]$. Taking an initial state $Q = \mathcal{O}$, $P_0 = P$ and $P_1 = 2P$, then

$$P_k = 28P_{k-1} + 26P_{k-2} = a_kP, \; k = 2, 3, \ldots \tag{7}$$

where

$$a_k = 28a_{k-1} + 26a_{k-2}, \; k = 2, 3, \ldots$$

i	iP	$\delta(iP)$	i	iP	$\delta(iP)$	i	iP	$\delta(iP)$	i	iP	$\delta(iP)$
1	$(4,7)$	$(0,0)$	9	$(9,12)$	$(0,1)$	16	$(0,21)$	$(0,1)$	23	$(1,12)$	$(0,1)$
2	$(10,18)$	$(0,1)$	10	$(11,9)$	$(0,0)$	17	$(14,5)$	$(1,0)$	24	$(8,15)$	$(0,1)$
3	$(13,11)$	$(1,0)$	11	$(17,9)$	$(1,0)$	18	$(17,14)$	$(1,1)$	25	$(15,17)$	$(1,1)$
4	$(15,6)$	$(1,0)$	12	$(14,18)$	$(1,1)$	19	$(11,14)$	$(0,1)$	26	$(13,12)$	$(1,1)$
5	$(8,8)$	$(0,0)$	13	$(0,2)$	$(0,0)$	20	$(9,11)$	$(0,0)$	27	$(10,5)$	$(0,0)$
6	$(1,11)$	$(0,0)$	14	$(22,5)$	$(1,0)$	21	$(18,14)$	$(1,1)$	28	$(4,16)$	$(0,1)$
7	$(7,20)$	$(0,1)$	15	$(22,18)$	$(1,1)$	22	$(7,3)$	$(0,0)$	29	$\mathcal{O}$	$(0,0)$
8	$(18,9)$	$(1,0)$									

Table 1.

which is an LFSR sequence over $\mathbb{Z}_{29}$ with initial condition $(a_0, a_1) = (1, 2)$. Relation (7) gives the EC sequence

$$\underline{\mathbf{P}} = (P, 2P, 24P, 28P, 16P, 16P, 23P, 16P, 2P, 8P, 15P, 19P, 23P, 7P, \\ 11P, 26P, 28P, 10P, 22P, 6P, 15P, 25P, 17P, 24P, 12P, \ldots)$$

and the binary bit sequence $\underline{\mathbf{u}}$ obtained from $\underline{\mathbf{P}}$ by applying the map τ is

$$\underline{\mathbf{u}} = (0,1,1,1,1,1,1,1,1,0,1,1,1,1,0,1,1,0,0,0,1,1,0,1,1,\ldots).$$

One can obtain the elements of $\underline{\mathbf{u}}$ by looking up Table 1.

Example 2 (curve defined on $\mathbb{F}_{2^l}$). Let t be a root of the polynomial $g(x) = x^5 + x^2 + 1$ and $\mathbb{F}_{2^5}$ be the field generated by t. Consider the non-supersingular curve $E_2 : y^2 + xy = x^3 + t^9x^2 + t^{15}$ over $\mathbb{F}_{2^5}$. This curve has order 26. Let $P = (t, t^7)$ be a point on E_2. The points, together with the map δ, is listed below.

i	iP	$\delta(iP)$	i	iP	$\delta(iP)$	i	iP	$\delta(iP)$
1	(t, t^7)	$(0,0)$	10	(t^{24}, t^{17})	$(1,1)$	19	(t^{14}, t^{10})	$(0,1)$
2	(t^{21}, t)	$(1,0)$	11	(t^2, t^{18})	$(0,1)$	20	(t^9, t^{29})	$(1,0)$
3	(t^{30}, t^{29})	$(0,0)$	12	(t^{22}, t^5)	$(1,1)$	21	(t^{23}, t^{25})	$(0,0)$
4	$(t^{26}, 1)$	$(1,1)$	13	$(0, t^{23})$	$(0,0)$	22	(t^{26}, t^{28})	$(1,0)$
5	(t^{23}, t^{28})	$(0,0)$	14	(t^{22}, t^4)	$(1,0)$	23	$(t^{30}, t^{16}$	$(0,0)$
6	(t^9, t^{17})	$(1,1)$	15	(t^2, t^{11})	$(0,1)$	24	(t^{21}, t^9)	$(1,1)$
7	(t^{14}, t^{20})	$(0,1)$	16	(t^{24}, t^8)	$(1,0)$	25	(t, t^{28})	$(0,0)$
8	$(1, t^{27})$	$(1,0)$	17	(t^{28}, t^2)	$(0,0)$	26	$\mathcal{O}$	$(0,0)$
9	(t^{28}, t^{30})	$(0,0)$	18	$(1, t^6)$	$(1,1)$			

Table 2.

Take $R = 2P$, then R has order 13. Choose $f(x) = x^2 - 12x - 11 \in \mathbb{Z}_{13}[x]$. Taking an initial state $Q = \mathcal{O}$, $P_0 = R$ and $P_1 = 2R$, the single point EC sequence $\underline{\mathbf{P}} = \{P_k\}$ is given by

$$P_k = 12P_{k-1} + 11P_{k-2} = a_k R, \ \ k = 2, 3, \ldots \tag{8}$$

where

$$a_k = 12a_{k-1} + 11a_{k-2}, \ \ k = 2, 3, \ldots$$

and hence $\{\underline{\mathbf{a}}\} \in \mathbb{Z}_{13}(f)$. With the initial state $(a_0, a_1) = (1, 2)$, recurrence (8) gives the EC sequence

$$\underline{\mathbf{P}} = (R, 2R, 9R, \mathcal{O}, 8R, 5R, 5R, 11R, 5R, 12R, 4R, 11R, 7R, 10R, 2R,\\ 4R, 5R, \mathcal{O}, 3R, 10R, 10R, 9R, 10R, 11R, \ldots)$$

and the binary bit sequence $\underline{\mathbf{u}}$ obtained from $\underline{\mathbf{P}}$ by applying the map τ is

$$\underline{\mathbf{u}} = (0, 1, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 1, 0, 0, 1, 0, 0, \ldots).$$

by looking up from Table 2. Note that the mapping of the x-coordinate resulted in the subsequence $(1111\ldots)$.

For general E and f, the periods and linear spans of EC bit sequences are not easy to determine. However, by a result from Chan and Games [3], we can obtain the linear span of single point EC bit sequences under certain conditions.

Let E be an elliptic curve over $\mathbb{F}_q$, $P \in E$ with order p, $f(x)$ be a primitive polynomial of degree n over $\mathbb{F}_p$, and $\underline{\mathbf{P}} = \{P_i\} \in G_P(f)$ where $P_i = a_i P$ where $\underline{\mathbf{a}} = \{a_k\} \in G_{\mathbb{F}_p}(f)$ is an m-sequence over $\mathbb{F}_p$ generated by $f(x)$. Let $\underline{\mathbf{s}}$ and $\underline{\mathbf{u}}$ be the EC bit sequences formed by mappings τ and δ respectively. I.e.,

$$u_i = \tau(P_i) = \tau(a_i P), \ \ i = 0, 1, \ldots \tag{9}$$

Let $d = \frac{p^n - 1}{p-1}$ and $\underline{\mathbf{u}}_j = \{u_{id+j}\}_{i \geq 0}$, $0 \leq j < d$. Denote $\mathrm{LS}(\underline{\mathbf{w}})$ to be the linear span of a periodic sequence $\underline{\mathbf{w}}$.

Theorem 3 *With the above notations and assumptions, the linear span of* $\underline{\mathbf{u}}$ *is given by*

$$\mathrm{LS}(\underline{\mathbf{u}}) = d \cdot \mathrm{LS}(\underline{\mathbf{u}}_j)$$

for any j *with* $\underline{\mathbf{u}}_j \neq 0$. *It is noted that all non-zero* $\underline{\mathbf{u}}_j$*'s are cyclic shifts of each other.*

In order to prove Theorem 3, we need a lemma from [3].

Lemma 2 (Chan and Games [3]) *With the notations above. let* $\rho : \mathbb{F}_p \to \mathbb{F}_2$ *be a function from* $\mathbb{F}_p$ *to* $\mathbb{F}_2$, *and a binary sequence* $\underline{\mathbf{u}} = \{b_i\}$ *obtained by* $b_i = \rho(a_i)$, $i = 0, 1, \ldots$.

Then, the linear span of $\underline{\mathbf{b}}$, $\mathrm{LS}(\underline{\mathbf{b}})$, *is given by*

$$\mathrm{LS}(\underline{\mathbf{b}}) = d \cdot \mathrm{LS}(\underline{\mathbf{b}}_j)$$

for any j *such that* $\underline{\mathbf{b}}_j = \{b_{id+j}\}_{i \geq 0} \neq \underline{0}$, $0 \leq j < d$. *It is noted that all non-zero* $\underline{\mathbf{b}}_j$*'s are shift equivalent.*

Proof: (of Theorem 3) We construct ρ as follows. Let η be a map from $\mathbb{F}_p$ to E defined by

$$\eta : c \to cP(\in E), \ \forall c \in \mathbb{F}_p, \tag{10}$$

and ρ be the composite of η and τ:

$$\rho = \tau \circ \eta : c \to \tau(\eta(c)) = \tau(cP), \ \forall c \in \mathbb{F}_p. \tag{11}$$

Thus ρ is a map from $\mathbb{F}_p$ to $\mathbb{F}_2$. Combining with (9), we have

$$u_i = \tau(a_i P) = \tau(\eta(a_i)) = \rho(a_i), \ i = 0, 1, \ldots$$

Applying Lemma 2, the assertion is established. □

Corollary 2 *The linear span of* $\underline{\mathbf{s}}$*,* $\mathrm{LS}(\underline{\mathbf{s}})$ *is bounded by*

$$\mathrm{LS}(\underline{\mathbf{s}}) \geq \frac{\mathrm{LS}(\underline{\mathbf{u}})}{2}.$$

Proof: Let $m(x)$ and $t(x)$ be the minimal polynomial of $\underline{\mathbf{s}}$ and $\underline{\mathbf{u}}$ respectively. Then $m(x^2)$ is a characteristic polynomial of $\underline{\mathbf{u}}$. Thus $t(x) \mid m(x^2)$. Hence

$$\mathrm{LS}(\underline{\mathbf{u}}) \leq 2\mathrm{LS}(\underline{\mathbf{s}}).$$

The result follows. □

Corollary 3 *The period of* $\underline{\mathbf{u}}$*,* $\mathrm{per}(\underline{\mathbf{u}})$*, is given by*

$$\mathrm{per}(\underline{\mathbf{u}}) = d \cdot \mathrm{per}(\underline{\mathbf{u}}_j)$$

for any $0 \leq j < d$ *such that* $\underline{\mathbf{u}}_j \neq 0$*.*

Proof: Note that $\underline{\mathbf{u}}$ can be considered as a binary sequence obtained from and m-sequence $\{a_i\}$ through the map $\rho = \tau \circ \eta$ defined by (10) and (11). According to the proof of Lemma 2 in [5], the result is immediate. □

Remark 3 *Theorem 3 and Corollary 3 show that the linear span and period of* $\underline{\mathbf{u}}$ *are determined by a shorter sequence* $\underline{\mathbf{u}}_j \neq 0$*. The results only depend on the order of the point* P *and the characteristic polynomial* $f(x)$ *and do not depend on* $\mathbb{F}_q$ *from which the coordinates of the points are taken. We will use the sequences obtained from equations (10) and (11) to explain this remarkable result. The study of linear span and period of* $\underline{\mathbf{u}}_j$ *is in progress.*

Example 3 (curve defined on $\mathbb{F}_{23}$*).* With the sequences in example 1, note that $f(x) = x^2 - 28x - 26$ is primitive in $\mathbb{Z}_{29}$. Let $d = \frac{29^2-1}{29-1} = 30$. Let

$\{\underline{\mathbf{a}}_j\} = \{a_{id+j}\}_{i\geq 0}$, and $\underline{\mathbf{P}}_j = \{P_{id+j}\}_{i\geq 0}$ for $0 \leq j < d$. Then we have

$$\begin{aligned}
\underline{\mathbf{a}}_0 &= (1, 3, 9, 27, 23, 11, 4, 12, 7, 21, 5, 15, 16, 19, 28, 26, 20, 2, 6, 18, 25,\\
&\quad 17, 22, 8, 24, 14, 13, 10, 1, 3, 9, \ldots),\\
\underline{\mathbf{P}}_0 &= (P, 3P, 9P, 27P, 23P, 11P, 4P, 12P, 7P, 21P, 5P, 15P, 16P, 19P,\\
&\quad 28P, 26P, 20P, 2P, 6P, 18P, 25P, 17P, 22P, 8P, 24P, 14P, 13P, 10P,\\
&\quad P, 3P, 9P, \ldots),\\
\underline{\mathbf{u}}_0 &= (0, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0,\\
&\quad 0, 0, 1, 0, \ldots).
\end{aligned}$$

Using the Berlekamp-Massey algorithm [2,13], the linear span of $\underline{\mathbf{u}}_0$ is 15, and by directly checking, the period of $\underline{\mathbf{u}}_0$ is 28. Thus, by Theorem 3 and Corollary 3,

$$\mathrm{LS}(\underline{\mathbf{u}}) = d \cdot \mathrm{LS}(\underline{\mathbf{u}}_0) = 30 \cdot \mathrm{LS}(\underline{\mathbf{u}}_0) = 450 \text{ and } \mathrm{per}(\underline{\mathbf{u}}) = 840.$$

Example 4 (curve defined on $\mathbb{F}_{2^5}$). With the sequences from example 2. Since $f(x) = x^2 - 12x - 11$ is primitive over $\mathbb{Z}_{13}$, therefore $d = \frac{13^2-1}{13-1} = 14$. We have

$$\begin{aligned}
\underline{\mathbf{a}}_0 &= (1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1, 2, 4, 8, \ldots),\\
\underline{\mathbf{P}}_0 &= (R, 2R, 4R, 8R, 3R, 6R, 12R, 11R, 9R, 5R, 10R, 7R, R, 2R, \ldots),\\
\underline{\mathbf{u}}_0 &= (0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0 \ldots).
\end{aligned}$$

Similarly, applying the Berlekamp-Massey algorithm, the linear span of $\underline{\mathbf{u}}_0$ is 7, by directly checking, the period of $\underline{\mathbf{u}}_0$ is 12. By Theorem 3 and Corollary 3, $\mathrm{LS}(\underline{\mathbf{u}}) = d \cdot \mathrm{LS}(\underline{\mathbf{u}}_0) = 98$ and $\mathrm{per}(\underline{\mathbf{u}}) = 168$.

Remark 4 *The proofs of Theorem 3 and Corollary 3 do not involve any properties of the map τ (from E to $\mathbb{F}_2$). Hence, the map τ can be replaced by any map from E to $\mathbb{F}_2$, and the results in Theorem 3 and Corollary 3 will still hold. Therefore, τ can be considered as a map from $\mathbb{F}_q$ to $\mathbb{F}_2$.*

Remark 5 *If $q = p$, that is, the curve defined over $\mathbb{F}_p$ has order p, in this case the discrete logarithm problem over such curves is solved by Samaev, Smart, and Satoh and Araki [17,18,16].*

4 Binary Sequences Obtained from Supersingular Elliptic Curves with $f(x) = x - 1$

For the case $n = 1$, we take $f(x) = x - 1, c_{-1} = 1$ and $Q = P_0$. Then we have

$$P_k = P_{k-1} + P_0,\ \ k = 1, 2, \ldots.$$

Thus

$$P_k = (k+1)P_0,\ \ k = 0, 1, \ldots \tag{12}$$

Let $\underline{\mathbf{u}}$ and $\underline{\mathbf{s}}$ be the sequences constructed as in Section 3 from $\underline{\mathbf{P}}$ given by (12). In [5], Gong, Berson and Stinson studied $\underline{\mathbf{s}}$ when E is a supersingular elliptic curve over $\mathbb{F}_{2^l}$ and $\underline{\mathbf{s}}$ is referred to as an elliptic curve pseudorandom sequence. The $0-1$ distribution, period and linear span of $\underline{\mathbf{s}}$ was also analysed in [5] when l is odd. The bound for the $0-1$ distribution of $\underline{\mathbf{s}}$ where E is an elliptic curve over $\mathbb{F}_{2^l}$ was discussed in [9]. We have proved that the linear span of $\underline{\mathbf{u}}$ in some cases is at least a quarter of the order of E, for which the proof is given in a separate paper [7].

In the following, we will discuss the $0-1$ distribution of $\underline{\mathbf{s}}$ when l is even. First we introduce some notations. Let $H(\underline{\mathbf{w}})$ represent the Hamming weight of a binary vector. Let $\underline{\mathbf{w}} = (w_0, w_1, \ldots, w_{k-1})$, then the reverse of $\underline{\mathbf{w}}$ is $\overleftarrow{\underline{\mathbf{w}}} = (w_{k-1}, \ldots w_1, w_0)$. We also denote a periodic sequence with period t (not necessarily be the smallest period) as a vector of dimension t. Given the field $\mathbb{F}_{2^l}$ where l is even. Define

$$\mathrm{Te}(\alpha) = \alpha + \alpha^{2^2} + \alpha^{2^4} + \cdots + \alpha^{2^{l-2}}.$$

Let δ, ω be such that $\mathrm{Te}(\delta) \neq 0$ and $\mathrm{Tr}(\omega) = 1$. When l is even, there are 7 isomorphism classes [14]. Three of the 7 isomorphic classes of curves are:

1. $y^2 + y = x^3 + \delta x$,
2. $y^2 + y = x^3$,
3. $y^2 + y = x^3 + \omega$.

Let the order of the curve be $2v + 1$, and let

$$A = (s_0, s_2, \ldots, s_{2(v-1)}),\ B = (s_1, s_3, \ldots, s_{2v-1}),$$

and $\underline{\mathbf{s}}' = (s_0, s_1, \ldots, s_{4v-1})$. Note that $s_{4v} = s_{4v+1} = 0$ since (s_{4v}, s_{4v+1}) is mapped from $\mathcal{O}$. We have $H(\underline{\mathbf{s}}') = H(\underline{\mathbf{s}})$. $\underline{\mathbf{s}}'$ is the exact sequence discussed in [5].

Theorem 4 $\underline{\mathbf{s}}$ *can be arranged into an array*

$$S = \begin{bmatrix} A & \overleftarrow{A} & 0 \\ B & \overleftarrow{B} & 0 \end{bmatrix}.$$

The weight of the $S_0 = (A, \overleftarrow{A})$ *in all three cases is one of the five possible values:* $2^{l-1} + \{0, \pm 2^{\frac{l}{2}+1},\ \text{or}\ \pm 2^{\frac{l}{2}}\}$.

Proof: The negative of a point (x, y) on a supersingular curve is $(x, y + c_3)$. In all the three cases, $c_3 = 1$, hence $\mathrm{Tr}_2^{2^l}(y + c_3) = \mathrm{Tr}_2^{2^l}(y)$. Therefore we must have

$$S = \begin{bmatrix} A & \overleftarrow{A} & 0 \\ B & \overleftarrow{B} & 0 \end{bmatrix}.$$

For the second half of the statement, first consider the case $y^2+y=x^3+\delta x$. This curve has order 2^l+1. Let

$$n_{i,j}=|\{x\in\mathbb{F}_{2^l}:\mathrm{Tr}_2^{2^l}(x)=i,\mathrm{Tr}_2^{2^l}(x^3+\delta x)=j\}|.$$

We proceed to count the quantities of $n_{i,j}$ to find the weight distribution of the sequence. We have $n_{0,0}+n_{0,1}=|\{x\in\mathbb{F}_{2^l}:\mathrm{Tr}_2^{2^l}(x)=0\}|=2^{l-1}$. Similarly, $n_{1,0}+n_{1,1}=2^{l-1}$. Also,

$$\begin{aligned}n_{0,0}+n_{1,0}&=|\{x\in\mathbb{F}_{2^l}:\mathrm{Tr}_2^{2^l}(x^3+\delta x)=0\}|\\&=|\{x\in\mathbb{F}_{2^l}:y^2+y=x^3+\delta x\text{ has a solution}\}|\\&=(|E|-1)/2=2^{l-1}.\end{aligned}$$

and

$$\begin{aligned}&n_{0,0}+n_{1,1}-(n_{0,1}+n_{1,0})\\&=|\{x\in\mathbb{F}_{2^l}:\mathrm{Tr}_2^{2^l}(x+x^3+\delta x)=0\}|\\&\quad-|\{x\in\mathbb{F}_{2^l}:\mathrm{Tr}_2^{2^l}(x+x^3+\delta x)=1\}|\\&=2|\{x\in\mathbb{F}_{2^l}:\mathrm{Tr}_2^{2^l}(x+x^3+\delta x)=0\}|-|\{x\in\mathbb{F}_{2^l}\}|\\&=2|\{x\in\mathbb{F}_{2^l}:y^2+y=x^3+(\delta+1)x\text{ has a solution}\}|-2^l\\&=\begin{cases}0&\text{if }\mathrm{Te}(\delta+1)\neq 0,\\\pm 2^{\frac{l}{2}+1}&\text{otherwise.}\end{cases}\end{aligned}$$

When $\mathrm{Te}(\delta+1)\neq 0$, we have $(n_{0,0},n_{0,1},n_{1,0},n_{1,1})=(2^{l-2},2^{l-2},2^{l-2},2^{l-2})$, then $H(S_0)=2H(A)=2n_{1,0}=2^{l-1}$. If $\mathrm{Te}(\delta+1)=0$, then $H(S_0)=2H(A)=2n_{1,0}=2^{l-1}\pm 2^{\frac{l}{2}}$.

The cases for the curves $y^2+y=x^3$ and $y^2+y=x^3+\omega$ are similar, except now the curve orders are as follows:

$$\#E=\begin{cases}2^l+1-2^{\frac{l}{2}+1}\text{ if }m\equiv 0\pmod 4,\\2^l+1+2^{\frac{l}{2}+1}\text{ if }m\equiv 2\pmod 4.\end{cases}\quad\text{for }E:y^2+y=x^3,$$

$$\#E=\begin{cases}2^l+1+2^{\frac{l}{2}+1}\text{ if }m\equiv 0\pmod 4,\\2^l+1-2^{\frac{l}{2}+1}\text{ if }m\equiv 2\pmod 4.\end{cases}\quad\text{for }E:y^2+y=x^3+\omega.$$

Similarly, the weight of S_0 must be one of the five possible values $2^{l-1}+\{0,\pm 2^{\frac{l}{2}+1},\text{ or }\pm 2^{\frac{l}{2}}\}$. □

References

1. P.H.T. Beelen, J.M. Doumen, Generating pseudo-random sequences using linear recurrency relations on elliptic curves, *Sixth International Conference on Finite Fields and Applications*, abstract, `http://www.iztapalapa.uam.mx/fq6/`, May 2001.

2. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.
3. A.H. Chan and R.A. Games, On the Linear Span of Binary Sequences Obtained from Q-Ary M-Sequences, Q Odd, *IEEE Trans. Information Theory*, Vol 36, No. 3, 548-552, 1990.
4. Z. Dai, M. Huang, Linear Complexity and the Minimal Polynomial of Linear Recurring Sequences over $\mathbb{Z}_m$, *Systems Science and Mathematical Sciences*, Vol. 4, No. 1, 51-54, Feb. 1991.
5. G. Gong, T. Berson and D. Stinson, Elliptic Curve Pseudorandom Sequence Generator, *Proceedings of the Sixth Annual Workshop on Selected Areas in Cryptography*, LNCS 1758, Springer-Verlag, 34-48, 1999.
6. S.W. Golomb, *Shift Register Sequences,* Holden-Day, Inc., 1967. Revised edition, Aegean Park Press, 1982.
7. G. Gong, C. Lam, Randomness of Several Elliptic Curve Sequences, *preprint*, 2001.
8. S. Hallgren, Linear congruential generators over elliptic curves, CS 94-143, Dept. of Comp. Sci., Carnegie Mellon University, 1994.
9. E.E. Mahassni and I. Shparlinski, On the Uniformity of Distribution of Congruential Generators over Elliptic Curves, *preprint*, November 2000.
10. B. Kaliski, *A Pseudo-Random Bit Generator Based on Elliptic Logarithms*, Advances in Cryptology–Crypto '86, Lecture Notes in Computer Science, LNCS 263(1986), Springer-Verlag, 84-103.
11. N. Koblitz, Elliptic Curve Cryptosystems, *Mathematics of Computation (48)*, 203-209, 1987.
12. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Addison-Wesley, 1983, Theorem 3.35, 97-98.
13. J. L. Massey, *Shift-register synthesis and BCH decoding*, IEEE Trans. Information Theory, January 1969.
14. A. J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.
15. V. Miller, Uses of Elliptic Curves in Cryptography, *Advances in Cryptology – CRYPTO '85*, LNCS 218, Springer-Verlag, 417-426, 1986.
16. T. Satoh and K. Araki, Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, *Commentarii Mathematici Universitatis Sancti Paul*, 47 (1998), 81-92.
17. I. Samaev, Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p, *Mathematics of Computation*, 67 (1998), 353-356.
18. N. Smart, The discrete logarithm problem on elliptic curves of trace one, *Journal of Cryptology*, 12 (1999), 193-196.
19. J. Solinas, Improved Algorithms for Arithmetic on Anomalous Binary Curves, *CACR Technical Reports*, CORR 99-46, University of Waterloo, 1999.
20. M. Ward, The characteristic number of a sequence of integers satisfying a linear recursion relation, Trans. Amer. Math. Soc., 33 (1931), 153-165.