Elliptic Curve Pseudorandom Sequence Generators

Guang Gong[1], Thomas A. Berson[2], and Douglas R. Stinson[3]

[1] Department of Combinatorics and Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, Canada
ggong@cacr.math.uwaterloo.ca
[2] Anagram Laboratories, P.O. Box 791
Palo Alto, CA 94301, USA
berson@anagram.com
[3] Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
dstinson@cacr.math.uwaterloo.ca

Abstract. In this paper, we introduce a new approach to the generation of binary sequences by applying trace functions to elliptic curves over $GF(2^m)$. We call these sequences *elliptic curve pseudorandom sequences* (EC-sequence). We determine their periods, distribution of zeros and ones, and linear spans for a class of EC-sequences generated from supersingular curves. We exhibit a class of EC-sequences which has half period as a lower bound for their linear spans. EC-sequences can be constructed algebraically and can be generated efficiently in software or hardware by the same methods that are used for implementation of elliptic curve public-key cryptosystems.

1 Introduction

It is a well-known result that any periodic binary sequence can be decomposed as a sum of linear feedback shift register (LFSR) sequences and can be considered as a sequence arising from operating a trace function on a Reed-Solomon codeword [22], [24]. More precisely, let α be a primitive element of a finite field $\mathbb{F}_{2^n}$ and let $C = \{r_1, \cdots, r_s\}, 0 < r_i < 2^n - 1$, be the null spectrum set of a Reed-Solomon code. If we want to transmit a message $m = (m_1, \cdots, m_s), m_i \in \mathbb{F}_{2^n}$, over a noisy channel, then first we form a polynomial $g(x) = \sum_{i=0}^{s} m_i x^{r_i}$ and then compute $c_j = g(\alpha^j)$. The codeword is $c = (c_0, c_1, \cdots, c_{2^n-2})$. Now we apply the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ to this codeword, i.e., we compute

$$a_i = Tr(c_i) = Tr(g(\alpha^i)), i = 0, 1, \cdots, 2^n - 2. \tag{1}$$

Then the resulting sequence $A = \{a_i\}$ is a binary sequence having period which is a factor of $2^n - 1$. All periodic binary sequences can be reduced to this model. Note that if $g(x) = x$, then A is an m-sequence of period $2^n - 1$. A lot of research

Howard Heys and Carlisle Adams (Eds.): SAC'99, LNCS 1758, pp. 34–48, 2000.

has been done concerning ways to choose the function $g(x)$ such that the resulting sequence has the good statistical properties. Examples include filter function generators [15], [11], [18], combinatorial function generators [14], [25], [23], and clock controlled generators and shrinking generators[1], [5]. Unfortunately, the trace function destroys the structure of Reed-Solomon code. It is difficult to get sequences satisfying cryptographic requirements from this approach. If one can specify the linear span, then there is no obvious method to determine the statistical properties of the resulting sequences. Examples include many conjectured sequences with two-level autocorrelation or lower level cross correlation [21], [27]. If one can fix the parameters for good statistical properties, then all known sequences have low linear spans in the sense that ratio of linear span to the period is much less than 1/2.

Note that if a binary sequence of period 2^n has the property that each n-tuple occurs exactly once in one period, then it is called a *de Bruijn sequence* [3]. Chan et al. proved that de Bruijn sequences have large linear spans [4]. From a de Bruijn sequence of period 2^n one can construct a binary sequence of period $2^n - 1$ by deleting one zero from the unique run of zeros of length n. The resulting sequence is called a *modified de Bruijn sequence*, see [10]. There is no theoretical result on the linear spans of such sequences except for m-sequences. Experimental computation on the linear spans of the modified sequences have only been done for the sequences with period 15, 31 and 63 [10]. Another problem that de Bruijn sequences have is that they are difficult to implement. All algorithms for constructing de Bruijn sequences (except for a class constructed from the m-sequences of period $2^n - 1$) require a huge memory space. It is infeasible to construct a de Bruijn sequence or a nonlinear modified de Bruijn sequence with period 2^n when $n > 30$ [6], [7], [9]. (It is a well known fact that in design of secure systems, if one sequence can be obtained by removing or inserting one bit from another sequence, and the resulting sequence has a large linear span, then it is not considered as secure. Consequently, the de Bruijn sequences of period 2^n constructed from m-sequences of period $2^n - 1$ by inserting one zero into the run of zeros of length $n - 1$ of the m-sequence are not considered to be good pseudorandom sequences.)

In this paper, we introduce a new method for generating binary sequences. We will replace a Reed-Solomon codeword in (1) by the points on an elliptic curve over $\mathbb{F}_{2^n}$. The resulting binary sequences are called *elliptic curve pseudorandom sequences*, or EC-sequences for short. We will discuss constructions and representation of EC-sequences, their statistical properties, their periods and linear spans. We exhibit a class of EC-sequences which may be suitable for use as a key generator in stream cipher cryptosystems. These EC-sequences have period equal to 2^{n+1}, the bias for unbalance is $\lfloor 2^{n/2} \rfloor$ and lower bound and upper bounds on their linear spans are 2^n and $2^{n+1} - 2$, respectively. It is worth pointing out that EC-sequences can be constructed algebraically and they can be generated efficiently in software or hardware by the same method that are used for implementation of elliptic curve public-key cryptosystems [20].

The paper is organized as follows. In Section 2, we introduce some concepts and and preliminary results from sequence analysis and the definition of the elliptic curves over $\mathbb{F}_{2^n}$. In Section 3, we give a method for construction of EC-sequences and their representation by interleaved structure. In Section 4, we discuss statistical properties of EC-sequences constructed from supersingular elliptic curves. In Section 5, we determine the periods of EC-sequences constructed from supersingular elliptic curves. In Section 6, we derive a lower bound and an upper bound for EC-sequences constructed from a class of supersingular elliptic curves with order 2^n+1. Section 7 shows a class of EC-sequences which are suitable for use as a key generator in stream cipher cryptosystems. A comparison of this class of EC sequence generators with the other known pseudo-random sequence generators is also included in this section.

Remark. Kaliski discussed how to generate a pseudo-random sequence from elliptic curves in [16], where he used randomness criteria based on the computational difficulty of the discrete logarithm over the elliptic curves [26]. In this paper our approach is completely different. We use the unconditional randomness criteria to measure the EC-sequences and use the trace function to obtain binary sequences. A set of the unconditional randomness measurements for pseudorandom sequence generators is described as follows:

- Long period
- Balance property (Golomb Postulate 1 [9])
- Run property (Golomb Postulate 2)
- n-tuple distribution
- Two-level auto correlation (Golomb Postulate 3)
- Low-level cross correlation
- Large linear span and smooth increased linear span profiles

2 Preliminaries

In this section, we introduce some concepts and preliminary results on sequence analysis.

Let $q = 2^n$, let
F_q be a finite field and let $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$.

2.1 Trace Function from $\mathbb{F}_q$ to $\mathbb{F}_2$

$$Tr(x) = x + x^2 + \cdots + x^{2^{n-1}}, x \in F_q.$$

Property: $Tr(x^{2^k}) = Tr(x)$ for any positive integer k.

For $x \in \mathbb{F}_q$, this can be written as

$$x = x_0\alpha + x_1\alpha^2 + \cdots + x_{n-1}\alpha^{2^{n-1}}, x_i \in \{0, 1\}$$

where $\{\alpha, \alpha^2, \cdots, \alpha^{2^{n-1}}\}$ is a normal basis of $\mathbb{F}_{2^n}$. In this representation, $Tr(x)$ can be computed as follows

$$Tr(x) = x_0 + x_1 + \cdots + x_{n-1}.$$

2.2 Periods, Characteristic Polynomials, and Minimal Polynomials of Sequences

Let $A = \{a_i\}$ be a binary sequence. If v is a positive integer such that

$$a_i = a_{v+i},\ i = 0, 1, \cdots, \tag{2}$$

then v is called a length of A. We also write $A = (a_0, a_1, \cdots, a_{v-1})$, denote $v = length(A)$. Note the index is reduced modulo v. If p is the smallest positive integer satisfying (2), then we say p is the period of A, denoted as $per(A)$. It is easy to see that $p|v$.

Let $f(x) = x^l + c_{l-1}x^{l-1} + \cdots + c_1x + c_0 \in F_2[x]$. If $f(x)$ satisfies the following recursive relation:

$$a_{l+k} = \sum_{i=0}^{l-1} c_i a_{i+k} = c_{l-1}a_{l-1+k} + \cdots + c_1 a_{1+k} + c_0 a_k, k = 0, 1, \cdots$$

then we say $f(x)$ is a characteristic polynomial of A over $\mathbb{F}_2$.

The left shift operator L is defined as

$$L(A) = a_1, a_2, \cdots,$$

For any $i > 0$,

$$L^i(A) = a_i, a_{i+1}, \cdots,$$

We denote $L^0(A) = A$ for convention. If $f(x)$ is a characteristic polynomial of A over $\mathbb{F}_2$, then

$$f(L)A = \sum_{i=0}^{l} c_i L^i(A) = 0$$

where 0 represents a sequence consisting of all zeros. (Note 0 represents a number 0 or a sequence consisting of all zeros depending on the context.) Let

$$G(A) = \{f(x) \in F_2[x] | f(L)A = 0\}.$$

The polynomial in $G(A)$ with the smallest degree, say $m(x)$, is called the minimal polynomial of A over $\mathbb{F}_2$. Note that $G(A)$ is a principle ideal of $\mathbb{F}_2[x]$ and $G(A) =< m(x) >$. So, if $f(x)$ is a characteristic polynomial of A over $\mathbb{F}_2$, then $f(x) = m(x)h(x)$ where $h(x) \in F_2[x]$. The linear span of A over $\mathbb{F}_2$, denoted as $LS(S)$, is defined as $LS(A) = deg(m(x))$.

2.3 Interleaved Sequences

We can arrange the elements of the sequence A into a t by s array as follows:

$$\begin{pmatrix} a_0 & a_t & \cdots a_{(s-1)t} \\ a_1 & a_{t+1} & \cdots a_{(s-1)t+1} \\ a_2 & a_{t+2} & \cdots a_{(s-1)t+2} \\ \vdots & & \\ a_{t-1} & a_{t+t-1} & \cdots a_{(s-1)t+t-1} \end{pmatrix}$$

Let A_i denote the ith row of the above array. Then we also write the sequence $A = (A_0, A_1, \cdots, A_{t-1})^T$ where T is a transpose of a vector. In reference [12], A is called an *interleaved sequence* if A_i, $0 \leq i \leq t-1$, has the same minimal polynomial over $\mathbb{F}_2$. Here we generalize this concept to any structures of A_is. We still refer to A as a (t, s) interleaved sequence. By using the same approach as used in [12], we can have the following proposition.

Proposition 1 *Let v be a length of A and A be a (t, s) interleaved sequence where $v = ts$. Let $m_i(x) \in F_2[x]$ be the minimal polynomial of A_i, $1 \leq i \leq t$ and $m(x) \in F_2[x]$ be the minimal polynomial of A, then*

$$m(x) | m_j(x^t), 0 \leq j \leq t-1.$$

2.4 Elliptic Curves over $\mathbb{F}_{2^n}$

An elliptic curve E over $\mathbb{F}_{2^n}$ can be written in the following standard form (see [19]):

$$y^2 + y = x^3 + c_4 x + c_6, c_i \in \mathbb{F}_{2^n} \tag{3}$$

if E is supersingular, or

$$y^2 + xy = x^3 + c_2 x^2 + c_6, c_i \in \mathbb{F}_{2^n} \tag{4}$$

if E is non-supersingular. The points $P = (x, y)$, $x, y \in \mathbb{F}_{2^n}$, that satisfy this equation, together with a "point at infinity" denoted O, form an Abelian group $(E, +, O)$ whose identity element is O.

Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two different points in E and both P and Q are not equal to the infinity point.

Addition Law for *E* supersingular For $2P = P + P = (x_3, y_3)$,

$$x_3 = x_1^4 + c_4^2 \tag{5}$$

$$y_3 = (x_1^2 + c_4)(x_1 + x_3) + y_1 + 1 \tag{6}$$

For $P + Q = (x_3, y_3)$, if $x_1 = x_2$, then $P + Q = O$. Otherwise,

$$x_3 = \lambda^2 + x_1 + x_2$$
$$y_3 = \lambda(x_1 + x_3) + y_1 + 1$$

where $\lambda = (y_1 + y_2)/(x_1 + x_2)$.

Remark 1 *For a detailed treatment of sequence analysis and an introduction to elliptic curves, the reader is referred to [9], [19].*

3 Constructions of Pseudorandom Sequences from Elliptic Curves over $\mathbb{F}_q$

In this section, we give a construction of binary sequences from an elliptic curve over $\mathbb{F}_q$.

Let E be an elliptic curve over $\mathbb{F}_q$, denoted as $E(\mathbb{F}_q)$ or simply E if there is no confusion for the field that we work with, and let $|E|$ be the number of points of E over $\mathbb{F}_q$. Let $P = (x_1, y_1)$ be a point of E with order $v+1$. Note that $v+1||E|$. Let $\Gamma = (P, 2P, \cdots, vP)$ where $iP = (x_i, y_i)$, $1 \leq i \leq v$. Note that v is even if E is supersingular. v may be odd or even if E is non-supersingular. So, we can write $v = 2l$ if E is supersingular and $v = 2l + e, e \in F_2$ if E is non-supersingular.

3.1 Construction

Let

$$a_i = Tr(x_i) \text{ and } b_i = Tr(y_i), i = 1, 2, \cdots, v, \tag{7}$$

$$S_0 = (a_1, \cdots, a_v) \text{ and } S_1 = (b_1, \cdots, b_v). \tag{8}$$

Let $S = (S_0, S_1)^T$ be a $(2, v)$ interleaved sequence, i.e., the elements of $S = \{s_i\}_{i \geq 1}$ are given by

$$s_{2i-1} = a_i \text{ and } s_{2i} = b_i, i = 1, \cdots, v \tag{9}$$

where $length(S) = 2v$. For a convenient discussion in the following sections, we write S starting from 1, we denote 0 as $2v$ when the index is computed modulo $2v$. We call S a *binary elliptic curve pseudorandom sequence generated by* $E(\mathbb{F}_q)$ *of type I*, an *EC-sequence* for short.

Remark 2 *In the full paper [13], we discuss two other methods of constructing sequences from elliptic curves.*

Let $A = (a_1, a_2, \cdots, a_l)$ and $B = (b_1, b_2, \cdots, b_l)$. If $U = (u_1, u_2, \cdots, u_t)$, then we denote $\overleftarrow{U} = (u_t, u_{t-1}, \cdots, u_1)$, i.e., U written backwards.

Theorem 1 *With the above notation. Let $v+1||E|$, and let $S = (S_0, S_1)^T$ be a EC-sequence generated by $E(\mathbb{F}_q)$ of length $2v$ whose elements are given by (9). Let E be supersingular. Then*

$$S = \begin{pmatrix} A & \overleftarrow{A} \\ B & \overleftarrow{B} + 1 \end{pmatrix} \tag{10}$$

Proof. Let E be supersingular. Note that y and $y+1$ are two roots of (3) in $\mathbb{F}_q$ under the condition $Tr(x^3 + c_4 x + c_6) = 0$. Since the order of P is $v+1$, then

$$iP + (2l+1-i)P = O \Longrightarrow x_{l+i} = x_{l+1-i} \Longrightarrow y_{l+i} = y_{l+1-i} + 1, i = 1, \cdots, l.$$

Thus we have $S_0 = (A, \overleftarrow{A})$ and $S_1 = (B, \overleftarrow{B} + 1)$.

4 Statistical Properties of Supersingular EC-Sequences

In this section, we discuss the statistical properties of EC-sequences generated by supersingular curves over $\mathbb{F}_{2^n}$ where n is odd. Let $A = (a_0, \cdots, a_{p-1})$, $w(A)$ represent the Hamming weight of sequence A. i.e.,

$$w(A) = |\{i \mid a_i = 1, 0 \leq i < p\}|.$$

For convenience, we generalize the notation of Hamming weight of binary sequences to functions from $\mathbb{F}_q$ to $\mathbb{F}_2$. Let $g(x)$ be a function from $\mathbb{F}_q$ to $\mathbb{F}_2$, the weight of g is defined as $w(g) = |\{x \in \mathbb{F}_q | g(x) = 1\}|$. For two isomorphic curves $E(\mathbb{F}_q)$ and $T(\mathbb{F}_q)$, denote this by $E \cong T$. From [19], there are three different isomorphism classes for supersingular curves over $\mathbb{F}_q$ $(q = 2^n)$ for n odd.

1. $E_1 = \{E(\mathbb{F}_q) | E(\mathbb{F}_q) \cong y^2 + y = x^3\}$ and $|E_1| = 2^{2n-1}$ and for any $E(\mathbb{F}_q) \in E_1$, $|E| = q + 1$.
2. $E_2 = \{E(\mathbb{F}_q) | E(\mathbb{F}_q) \cong y^2 + y = x^3 + x\}$.
3. $E_3 = \{E(\mathbb{F}_q) | E(\mathbb{F}_q) \cong y^2 + y = x^3 + x + 1\}$.

Here $|E_2| = |E_3| = 2^{2n-2}$. For any $E(\mathbb{F}_q) \in E_2$ or E_3, $|E| = 2^n \pm 2^{(n+1)/2} + 1$. Let

$$E : y^2 + y = x^3 + c_4 x + c_6, c_4, c_6 \in F_q.$$

Theorem 2 *Let n be odd. Let $S = \begin{pmatrix} A & \overleftarrow{A} \\ B & \overleftarrow{B} + 1 \end{pmatrix}$ be an EC-sequence generated by a supersingular elliptic curve E where length$(S) = 2v$ and $v = |E| - 1$. Then $w(S_0) = 2w(A)$, $w(S_1) = v/2$ and $w(S) = 2w(A) + v/2$, where $w(A) = 2^{n-2} \pm 2^{(n-3)/2}$.*

In order to prove this result, we need the following lemma. If we denote $h(x) = x^3 + c_4 x + c_6$, then E can be written as $y^2 + y = h(x)$.

Lemma 1 *Let E and $h(x)$ be defined as above. Then we have*

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(h(x))} = |E| - 2^n - 1.$$

Proof.

$$\begin{aligned}\sum_{x \in \mathbb{F}_{2^n}} (-1)^{Tr(h(x))} &= |\{x \in \mathbb{F}_{2^n} : Tr(h(x)) = 0\}| - |\{x \in \mathbb{F}_{2^n} : Tr(h(x)) = 1\}| \\ &= 2|\{x \in \mathbb{F}_{2^n} : Tr(h(x)) = 0\}| - 2^n \\ &= (|E| - 1) - 2^n.\end{aligned}$$

For $i, j = 0, 1$, define

$$n_{i,j} = |\{x \in \mathbb{F}_{2^n} : Tr(x) = i, Tr(h(x)) = j\}|.$$

Next we determine $n_{1,0}$. Let F denote the elliptic curve $y^2 + y = h(x) + x$. Then the following equations hold:

$$\begin{aligned} n_{1,0} + n_{1,1} &= 2^{n-1} \\ n_{0,0} + n_{0,1} &= 2^{n-1} \\ n_{0,0} + n_{1,0} &= (|E| - 1)/2 \\ n_{0,0} + n_{1,1} - (n_{0,1} + n_{1,0}) &= |F| - 1 - 2^n. \end{aligned}$$

Note that the last equation follows easily from Lemma 1 since

$$\begin{aligned} n_{0,0} + n_{1,1} - (n_{0,1} + n_{1,0}) &= |\{x \in \mathbb{F}_{2^n} : Tr(x + h(x)) \\ &= 0\}| - |\{x \in \mathbb{F}_{2^n} : Tr(x + h(x)) = 1\}|. \end{aligned}$$

Now, this system of four equations in four unknowns is easily seen to have a unique solution. The value of $n_{1,0}$ is as stated in the following lemma:

Lemma 2 *Let E, F and $n_{1,0}$ be defined as above. Then we have*

$$n_{1,0} = 2^{n-2} + \frac{|E| - |F|}{4}.$$

It is known that $|E| - |F| = \pm 2^{(n+1)/2}$ for any values of c_4 and c_6 (This is shown in [8]; alternatively it follows easily from [19], p.40 and 47.) Thus we have the following corollary:

Corollary 1 *Let $n_{1,0}$ be defined as above; then $n_{1,0} = 2^{n-2} \pm 2^{(n-3)/2}$.*

Proof (Proof of Theorem 2). Since $length(S) = 2v$, from Theorem 1, we have $w(S_0) = 2w(A)$ and $w(S_1) = v/2$. So,

$$w(S) = 2w(A) + v/2. \tag{11}$$

According to the definition of $n_{i,j}$, we have $w(A) = n_{10}$. From Corollary 1, $w(A) = 2^{n-2} \pm 2^{(n-3)/2}$.

Remark 3 *The value of $w(A)$ depends on the values of c_4 and c_6. For further results on this, we refer the reader to the full version of this work [13].*

5 Periods of Supersingular EC-Sequences

In this section, we discuss the periods of EC-sequences generated by supersingular curves.

Lemma 3 *Let $S = (S_0, S_1)^T$ be a EC-sequence generated by a supersingular elliptic curve $E(\mathbb{F}_q)$ where $S_0 = (a_1, a_2, \cdots, a_v)$ and $v = |E| - 1 = 2l$. Then*

$$a_{2i} = a_i + Tr(c_4), i = 1, 2, \cdots, l.$$

Proof. Recall that $a_i = Tr(x_i)$. From formula (5) in Section 1,

$$x_{2i} = x_i^4 + c_4^2, i = 1, \cdots, l. \tag{12}$$

$\Longrightarrow a_{2i} = Tr(x_{2i}) = Tr(x_i^4 + c_4^2) = Tr(x_i) + Tr(c_4) = a_i + Tr(c_4).$

Definition 1 *Let $U = (u_1, u_2, \cdots, u_{2k})$ be a binary sequence of length $2k$. Then U is called a coset fixed palindrome sequence of length $2k$, CFP-sequence of length $2k$ for short, if it satisfies the following two conditions.*

(i) *Palindrome Condition (P)*
$U = (U_0, \overleftarrow{U_0})$ where $U_0 = (u_1, u_2, \cdots, u_k)$.
(ii) *Coset Fixed Condition (CF)*
$u_{2i} = u_i + c$, for each $1 \leq i \leq k$ where c is a constant in $\mathbb{F}_2$.

Lemma 4 *Let U be a CFP sequence of length $2d$ and $0 < w(U) < 2d$. Then $per(U) = 2d$.*

Proof. We claim that $per(U) \neq 2$. Otherwise, from the coset fixed condition $u_{2i} = u_i$, $1 \leq i \leq d$, we get $w(U) = 0$ or $w(U) = 2d$, which is a contradiction with the given condition. Therefore we can write $per(U) = t$ where $2 < t$ and $t|2d$. If $t < 2d$, let $2d = ts$. Then

$$u_{t+i} = u_i, i = 1, 2, \cdots. \tag{13}$$

Since U is a CFP sequence, from condition (i) in Definition 1, we have

$$u_{d-i} = u_{d+1+i}, 0 \leq i \leq d - 1. \tag{14}$$

From (13) and (14), we get

$$u_{l-i} = u_{l+1+i}, 0 \leq i \leq l - 1 \tag{15}$$

where $l = t/2$ if t is even and

$$u_{l-i} = u_{l+i}, 1 \leq i \leq l - 1 \tag{16}$$

$l = (t + 1)/2$ if t is odd. From condition 2 in Definition 1,

$$u_{2i} = u_i + c, 1 \leq i \leq t. \tag{17}$$

Since $0 < w(U) < 2d$ and U satisfies the CF condition, there exists $k : 0 \leq k < l$ such that

$$(u_{t+2k+1}, u_{t+2k+2}) = (1, 0) \text{ or } (0, 1). \tag{18}$$

(For a detailed proof of existence of such k, please see the full version of this paper [13].)

Case 1 $t = 2l$. Applying the above identities,

$$u_{l+k+1} \overset{(17)}{=} u_{2l+2k+2} + c = u_{t+2k+2} + c. \tag{19}$$

On the other hand,

$$u_{l+k+1} \overset{(15)}{=} u_{l-k} \overset{(17)}{=} u_{2l-2k} + c = u_{t-2k} + c \overset{(14)}{=} u_{t+2k+1} + c \tag{20}$$

(19) and (20) $\Longrightarrow u_{t+2k+1} = u_{t+2k+2}$ which contradicts with (18). Thus $per(U) = 2d$.

Case 2 $t = 2l - 1$.

$$u_{l+k+1} \overset{(17)}{=} u_{2l+2k+2} + c = u_{t+2k+1} + c. \tag{21}$$

$$u_{l+k+1} \overset{(16)}{=} u_{l-k-1} \overset{(17)}{=} u_{2l-2k-2} + c = u_{t-2k-1} + c \overset{(14)}{=} u_{t+2k+2} + c \tag{22}$$

(21) and (22) $\Longrightarrow u_{t+2k+1} = u_{t+2k+2}$ which contradicts with (18). Thus $per(U) = 2d$.

Lemma 5 *Let $S = (S_0, S_1)^T$ be a EC-sequence of length $2v$, generated by a supersingular elliptic curve $E(\mathbb{F}_q)$, where $v|(|E| - 1)$ and $0 < w(S_0) < v$. Then $per(S_0) = v$.*

Proof. From Theorem 1, we have $S_0 = (A, \overleftarrow{A})$, where $length(A) = v/2$. Together with Lemma 3, S_0 is a CFP sequence of length v. Since $0 < w(S_0) < v$, applying Lemma 4, we get $per(S_0) = v$.

Lemma 6 *Let $S = (S_0, S_1)^T$ be a EC-sequence of length $2v$, generated by an elliptic curve $E(\mathbb{F}_q)$, where $v|(|E| - 1)$. Then $per(S)$ is an even number.*

Proof. Assume that $per(S) = 2t + 1$. Then we have $s_1 = s_{2t+2} = b_{t+1}$ and $b_{v-t+1} = s_{2v-2(t+1)} = s_1 \Longrightarrow b_{v-t+1} = b_{t+1}$. From Theorem 1, $b_{v-t+1} = b_{t+1} + 1$ which is a contradiction. So, $per(S)$ is even.

Theorem 3 *Let $S = (S_0, S_1)^T$ be a EC-sequence of length $2v$, generated by a supersingular elliptic curve $E(\mathbb{F}_q)$, where $v|(|E| - 1)$ and $0 < w(S_0) < v$. Then $per(S) = 2v$.*

Proof. Since $length(S) = 2v$, then $per(S)|2v$. According to Lemma 6, $per(S) = 2t$ where $t|v$. Assume that $t < v$. Then

$$a_{t+j} = s_{2(t+j)-1} = s_{2t+2j-1} = s_{2j-1} = a_j, j = 1, 2, \cdots.$$

Thus, t is a length of $S_0 \Longrightarrow per(S_0)|t$. According to Lemma 5, $per(S_0) = v$. Thus $t = per(S_0) = v \Longrightarrow per(S) = 2v$.

Corollary 2 *Let n be odd. Let $S = (S_0, S_1)^T$ be a EC-sequence of length $2v$, generated by a supersingular elliptic curve $E(\mathbb{F}_q)$, where $v|(|E|-1)$. Then $per(S) = 2v$.*

Proof. From Theorem 4, we have $0 < w(S_0) < v$. Applying Theorem 5, the result follows.

6 Linear Span of Supersingular EC-Sequences

In this section, we derive a lower bound and an upper bound on the linear span of the EC-sequences generated by supersingular elliptic curves in the isomorphic class E_1. For convenience in using Proposition 1, from now on we will write S, S_0 and S_1 with the starting index at 0, i.e., $S = (s_0, s_1, \cdots, s_{2^{n+1}-1})$, $S_0 = (a_0, a_1, \cdots, a_{2^n-1})$ and $S_1 = (b_0, b_1, \cdots, b_{2^n-1})$ ($v = 2^n$ in this case). So,

$$a_i = s_{2i}, i = 0, 1, \cdots,$$
$$b_i = s_{2i+1}, i = 0, 1, \cdots.$$

Lemma 7 *Let $U = (u_0, \cdots, u_{2^k-1})$ where $per(U) = 2^k$ and $w(U) \equiv 0 \bmod 2$. Then, the linear span of U, $LS(U)$, is bounded as follows:*

$$2^{k-1} < LS(U) \leq 2^k - 1$$

Proof. Let $h(x)$ be the minimal polynomial of U over $\mathbb{F}_2$. Let $f(x) = x^{2^k} + 1$, then $f(L)(S) = 0$. Thus $h(x)|f(x)$. Since

$$f(x) = x^{2^k} + 1 = (x+1)^{2^k},$$

we have $h(x) = (x+1)^t$ where t is in the range of $1 \leq t \leq 2^k$. Since $w(U) \equiv 0$ mod 2, let $p = 2^k$, we have

$$u_{p+j} = \sum_{i=0}^{p-1} u_{j+i}, j = 0, 1, \cdots.$$

$\Longrightarrow g(x) = \sum_{i=0}^{p-1} x^i$ is a characteristic polynomial of U over $\mathbb{F}_2$. So $h(x)|g(x) \Longrightarrow LS(U) \leq 2^k - 1$.

On the other hand, if $r < 2^{k-1}$, then $h(x)|(x+1)^{2^{k-1}} = x^{2^{k-1}} + 1 \Longrightarrow x^{2^{k-1}} + 1$ is a characteristic polynomial of U over $\mathbb{F}_2 \Longrightarrow$

$$(L^{2^{k-1}} + 1)U = u_{2^{k-1}+i} + u_i = 0, i = 0, 1, \cdots$$

$\Longrightarrow per(U)|2^{k-1}$. This contradicts $per(U) = 2^k$. So, $r = LS(U) > 2^{k-1}$.

Theorem 4 *Let n be odd. Let S be an EC-sequence of length $2v$, generated from a supersingular elliptic curve $E(\mathbb{F}_q)$ which is isomorphic to $y^2 + y = x^3$, where $v = |E| - 1$. Then*

$$2^n \leq LS(S) \leq 2(2^n - 1).$$

Proof. From Corollary 2, we have $per(S) = 2^{n+1}$. According to Theorem 2, $w(S) \equiv 0 \bmod 2$. So, S satisfies the conditions of Lemma 7. Applying Lemma 7,

$$2^n < LS(S) < 2^{n+1} - 1.$$

Now, we only need to prove that $LS(S) \leq 2(2^n - 1)$. Let $m(x)$ and $m_0(x)$ be the minimal polynomials of S and S_0 over $\mathbb{F}_2$, respectively, where $S = (S_0, S_1)^T$. According to Proposition 1, we have

$$m(x)|m_0(x^2) \Longrightarrow deg(m(x)) \leq 2deg(m_0(x)).$$

Since S_0 also satisfies the condition of Lemma 7, we get $deg(m_0(x)) = LS(S_0) \leq 2^n - 1$. So,

$$LS(S) = deg(m(x)) \leq 2deg(m_0(x)) \leq 2(2^n - 1).$$

7 Applications

In this section, using the theoretical results that we obtained in the previous sections, we construct a class of EC-sequences with large linear spans and small bias unbalance, point out its implementation and give a comparison of ECPSG I with other known pseudorandom sequence generators.

7.1 ECPSG I

(a) Choose a finite field $K = \mathbb{F}_{2^n}$ where n is odd
(b) Randomly choose a super singular curve $E : y^2 + y = x^3 + c_4x + c_6$ over $\mathbb{F}_{2^n}$ in the isomorphism class E_1 of the curve $y^2 + y = x^3$. ($|E_1| = 2^{2n-1}$.)
(c) Randomly choose a point $P = (x, y)$ on the curve E such that the order of P is $2^n + 1$.
(d) Compute $iP = (x_i, y_i)$, $i = 1, \cdots, 2^n$.
(e) Map iP into a binary pair by using the trace function

$$a_i = Tr(x_i) \text{ and } b_i = Tr(y_i)$$

(f) Concatenate the pair (a_i, b_i) to construct the sequence $S = (a_1, b_1, a_2, b_2, \cdots, a_{2^n}, b_{2^n})$.

Let

$$G(E_1) = \{S = \{s_i\}|S \text{ generated by } E(F_{2^n}) \in E_1\}.$$

$G(E_1)$ is called an *elliptic curve pseudorandom sequence generator of type I (ECPSG I)*. Any sequence in $G(E_1)$ satisfies that $per(S) = 2^{n+1}$, $w(S) = 2^n \pm 2^m$ and $2^n < LS(S) \leq 2(2^n - 1)$.

Example Let $n = 5$.

(a) Construct a finite field $\mathbb{F}_{2^5}$ which is generated by a primitive polynomial $f(x) = x^5 + x^3 + 1$. Let α be a root of $f(x)$. We represent the elements in $\mathbb{F}_{2^5}$ as a power of α. For zero element, we write as $0 = \alpha^\infty$.

(b) Choose a curve $E : y^2 + y = x^3$.
(c) Choose $P = (\alpha, \alpha^{23})$ with order 33.
(d) Compute $iP = (x_i, y_i)$, $i = 1, \cdots, 32$, and the exponents of α for each point iP are listed in Table 1.

Table 1. $\{iP\}$

(1, 23)	(4, 13)	(18, 7)	(16, 27)	(13, 5)
(10, 2)	(26, 6)	(2, 22)	(5, 14)	(21, 12)
$(\infty, 0)$	(9, 19)	(22, 17)	(11, 9)	(20, 25)
(8, 29)	(8 , 26)	(20, 4)	(11, 24)	(22, 18)
(9, 8)	(∞, ∞)	(21, 20)	(5 , 1)	(2, 15)
(26, 10)	(10, 28)	(13, 3)	(16, 21)	(18, 16)
(4, 30)	(1, 11)			

(e) Map the point iP into two bits by the trace function:
x-coordinate sequence

$$\{a_i = Tr(x_i)\} = 00101110110111100111101101110100$$

and y-coordinate sequence

$$\{b_i = Tr(y_i)\} = 01101001101101101001001001101001$$

(f) Interleave (a_i, b_i):

$$S = (a_1, b_1, a_2, b_2, \cdots, a_{32}, b_{32})$$
$$= 0001110011101001111001111011110001101011100011100011111001100001$$

According to Theorems 3, 2 and 4, we have

- $per(S) = 64$.
- $w(S) = 2^5 + 2^2 = 36$. The bias of unbalance is equal to 4 for S.
- Linear span: $32 < LS(S) \leq 62$.

Remark 4 *1. The actual linear span of S is 62 and it has the minimal polynomial $m(x) = (x + 1)^{62}$.*
2. The linear span of a periodic sequence is invariant under the cyclic shift operation on the sequence. We computed the supersingular EC-sequences over $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$ for all phase shifts of the sequences. Experimental data shows that the profile of linear spans of any supersingular EC-sequence increases smoothly for each phase shift of the sequence.

7.2 Implementation of ECPSG I

Implementation of ECPSG relies only on implementation of elliptic curves over $\mathbb{F}_{2^n}$, we can borrow software/hardware from elliptic curve public-key cryptosystems to implement ECPSG.

7.3 A Table

In Table 2, we compare the period, frequency range of 1 occurrence, unbalance range, and linear span (LS) of ECPSG I with other sequence generators, such as filter function generators (FFG), combinatorial function generators (CFG), and clock controlled generators (CCG). We also include data for de Bruijn sequences. We conclude that ECPSG I may be suitable for use as a key generator in a stream cipher cryptosystem.

Table 2. Comparison of ECPSG I with Other Sequence Generators

Type of Generator	Period	Frequency Range of 1 occurrence	Unbalance Range	Linear Span
FFG	$2^n - 1$	$[1, 2^{n-1}]$	$[1, 2^{n-1}]$	unclear
CFG	$\leq 2^n - 1$	$[1, 2^{n-1}]$	$[1, 2^{n-1}]$	unclear
CCG	$(2^n - 1)^2$	$2^{n-1}(2^n - 1)$	$2^n - 1$	$n(2^n - 1)$
de Bruijn	2^{n+1}	2^n	0	$\geq 2^n + n + 1$ $\leq 2^{n+1} - 1$
ECPSG I	2^{n+1}	$2^n \pm 2^{(n-1)/2}$	$\pm 2^{(n-1)/2}$	$\geq 2^n$ $\leq 2^{n+1} - 2$

Acknowledgment

The authors would like to acknowledge useful discussions with Alfred Menezes.

References

1. T. Beth and F.Piper, The stop-and-go generator, *Advances in Cryptology, Proc. of EUROCRYPT'84*, vol. 209, Springer-Verlag, 1985, pp. 88-92.
2. M. Blum and S. Micali, How to generate cryptographically strong sequences of pseudo-random bits, *SIAM Journal of Computing* **13**(4), pp. 850-864, 1984.
3. N.G. de Bruijn, A combinatorial problem, *Kononklijke Nederlands Akademi van Wetenchappen, Proc.,* vol. 49, Pr. 2, 1946, pp. 758-764.
4. A.H. Chan, R.A. Games and E.L. Key, On the complexities of de Bruijn sequences, *J. Combin. Theory*, vol. 33, pp. 233-246, Nov. 1982.
5. D. Coppersmith, H. Krawczys and Y. Mansour, The shrinking generator, *Advances in Cryptology-Crypt'93*, Lecture Notes in Computer Science, vol. 773, Springer-Verlag, 1994, pp. 22-39.
6. H. Fredrickson, A survey of full length nonlinear shift register cycle algorithms, *SIAM Rev.*, Vol. 24, pp. 195-229, Apr. 1982.
7. R.A. Games, A generalized recursive construction for de Bruijn sequences, *IEEE Trans- on Inform. Theory* vol. IT-29, No. 6, Nov. 1983, pp. 843-850.
8. R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. on Inform. Theory*, January 1968, pp. 154-156.

9. S.W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982, pp. 39.
10. G.L. Mayhew and S.W. Golomb, Linear spans of modified de Bruijn sequences, *IEEE Trans. Inform. Theory*, vol. IT-36, No. 5, September 1990, pp. 1166-1167.
11. G. Gong, *An Analysis and Synthesis of Phases and Linear Complexity of Nonlinear Feed-forward Sequences*, Ph. D. dissertation, Institute of Information Systems, Univ. of Electronic Sci. & Tech. of China, Chengdu, Sichuan, China, 1990.
12. G. Gong, Theory and applications of $q-$ary interleaved sequences, *IEEE Trans. on Inform. Theory*, vol. IT-41, No. 2, March 1995, pp. 400-411.
13. G. Gong, T.A. Berson, and D.R. Stinson, Elliptic curve pseudorandom sequence generators, Technical Report, University of Waterloo, December 1998, `http://www.cacr.math.uwaterloo.ca`.
14. E.J. Groth, Generation of binary sequences with controllable complexity, *IEEE Trans. on Inform. Theory* vol. IT-17, No. 3, May 1971, pp. 288-296.
15. E.L. Key, An analysis of the structure and complexity of nonlinear binary sequence generators, *IEEE Trans. on Inform. Theory* vol. IT-22, No. 6, November 1976, pp. 732-736.
16. Jr. B. Kaliski, A pseudo-random bit generator based on elliptic logarithms, *Advances in Cryptology-Crypto'86*, Lecture Notes in Computer Science, vol. 263 , Springer-Verlag, Berlin, 1986. pp. 84-103.
17. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.
18. J.L. Massey and S. Serconek, The linear complexity of periodic sequences: a general theory, *Advances in Cryptology-Crypto'96*, Lecture Notes in Computer Science, vol. 1109 , Springer-Verlag, Berlin, 1996. pp. 358-372.
19. A.J. Menezes, *Elliptic Curve Public Key Cryptosystems*, Kluwer Academic Publishers, 1993.
20. A.J. Menezes and S.A. Vanstone, Elliptic curve cryptosystems and their implementation, *Journal of Cryptology,* **6**(1993), pp.209-224.
21. J.S. No, S.W. Golomb, G. Gong, H.K. Lee, and P. Gaal, New binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation, *IEEE Trans. on Inform. Theory*, vol. 44, No. 2, March 1998, pp.814-817.
22. I.R. Reed and G. Solomon, Polynomial codes over certain finite fields, *J. SIAM,* **8**(1960), pp. 300-304.
23. R.A. Rueppel, Products of linear recurring sequences with maximum complexity, *IEEE Trans. on Inform. Theory* vol. IT-33, No. 1, January 1987, pp. 124-131.
24. D.V. Sarwate, Optimum PN sequences for CDMA systems, *Proceedings of IEEE Third International Symposium on Spread Spectrum Techniques and Applications (IEEE ISSSTA'94)*, pp. 27-35.
25. T. Siegenthaler, Correlation-immunity of nonlinear combing functions for cryptographic applications, *IEEE Trans. Inform. Theory*, vol. IT-30, Sep. 1984, pp. 776-780.
26. Andrew C. Yao, Theory and applications of trapdoor functions , *23rd Annual Symposium of Foundations of Computer Science*, pp. 80-91.
27. D.V. Sarwate and M.B. Pursley, Cross correlation properties of pseudo-random and related sequences, *Proc. of the IEEE*, vol. 68, No. 5, May 1980.