Elliptic Curve Pseudorandom Sequence Generators

Guang Gong, Thomas A. Berson and Douglas R. Stinson*

Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Phones: (519) 888-4567 x6123
(519) 888-4567 x5590
Fax: (1-519) 725-5441
Emails: ggong@cacr.math.uwaterloo.ca
dstinson@cacr.math.uwaterloo.ca

*Anagram Laboratories
P.O. Box 791
Palo Alto, CA 94301, USA
Tel. (1-415) 324-0100
Email:berson@anagram.com

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 will show their periods, distribution of zeros and ones, and linear spans. This research has uncovered a class of EC-sequences, generated by super-singular curves, which has half period as a lower bound for their linear spans. In comparison to de Bruijn sequences with the same parameters, EC-sequences can be constructed algebraically and can be generated efficiently in software or hardware by means used for implementation of elliptic curve public-key cryptosystems.

Key Words Elliptic curves over $GF(2^n)$, pseudorandom sequences, stream ciphers.

1 Introduction and Preliminaries

In 1969, Massey[34] found that if a binary sequence of length p has linear span n, then the entire sequence can be reconstructed from $2n$ consecutive known bits by using the Berlekamp-Massey algorithm. Since then, stream cipher researchers have been working on how to construct binary sequences with large linear spans. It is a known result that any periodic binary sequence can be decomposed as a sum of linear feedback shift register (LFSR) sequences, which is a resulting sequence by operating a trace function on a Reed-Solomon codeword [42, 45]. More precisely,

let α be a primitive element of a finite field $GF(2^n)$ and $C = \{r_1, \cdots, r_s\}, 0 < r_i < 2^n - 1$, be the null spectrum set of a Read-Solomon code. If we want to transmit a message $m = (m_1, \cdots, m_s), m_i \in GF(2^n)$, over a noisy channel, then first we form a polynomial $g(x) = \sum_{i=0}^{s} m_i x^{r_i}$ and compute $c_j = g(\alpha^j)$. The codeword is $c = (c_0, c_1, \cdots, c_{2^n-2})$. Now we operate the trace function from $GF(2^n)$ to $GF(2)$ to this codeword, i.e., we do

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

Then the resulting sequence $A = \{a_i\}$ is a binary sequence where period of A 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 $2^n - 1$. So, a lot of research has been looking for a clever way to choose the function $g(x)$ such that the resulting sequence has a large linear span, a long period and good statistical properties. Examples include filter function generators [22, 26, 41, 24, 25, 3, 27, 44, 5, 47, 12, 46, 28, 19, 17, 18, 38, 32, 33], combinatorial function generators [22, 48, 43, 52, 8], and clock controlled generators and shrinking generators[1, 13, 30, 6]. 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 fix the linear span, then there is no proper method to determine the statistical properties of the resulting sequences. Examples include many conjectured sequences with two-level autocorrelation or lower level cross correlation [39, 40, 49]. If one can fix the parameters for good statistical properties, then all known sequences have low linear spans in the sense of that ratio of linear span over period is much less than 1/2. (See the references for filter generators and [21].) There is only one known exception: the so called de Bruijn sequences or modified de Bruijn sequences, which have large linear spans and satisfy $n-$tuple uniform distribution property [2, 4, 15]. But all algorithms for constructing de Bruijn sequences require a huge memory space. It is almost infeasible to construct a de Bruijn sequence with period 2^n when $n > 30$ [14, 9, 7, 10].

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 $GF(2^n)$. We will discuss the distribution of zeros and ones, the period and the linear span of the resulting binary sequences, which will be called *elliptic curve pseudorandom sequences*, EC-sequences for short. This research has uncovered a class of EC-sequences which are suitable for use as a key generator in stream cipher cryptosystems. For such a EC-sequence, its period is equal to 2^{n+1}, the bias for unbalance is $\lfloor 2^{n/2} \rfloor$ and a lower bound and an upper bound of linear span are 2^n and $2^{n+1} - 2$, respectively. Note that a de Bruijn sequence of period 2^{n+1} has $2^n + n + 1$ and $2^{n+1} - 1$ as its lower bound and upper bound on linear span. In comparison to de Bruijn sequences, we can construct EC-sequences algebraically and can generate EC-sequences efficiently in software or hardware by means used for implementation of elliptic curve public-key cryptosystems [36, 23, 51].

In the rest of this section, we will introduce some notation, concepts and preliminary results that will be used throughout this paper.

Let $q = 2^n$, F_q be a finite field $GF(q)$ and $F_q[x]$ be the ring of polynomials over F_q.

A. Trace Function from F_q to 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 $x \in GF(2^n)$, 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 $GF(2^n)$. In this representation, $Tr(x)$ can be computed as follows

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

B. 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:

$$a_{l+k} = \sum_{i=0}^{l-1} c_{i+k}a_{i+k} = c_{l-1}a_{l-1+k} + \cdots + c_1a_{1+k} + c_0a_k, k = 0, 1, \cdots$$

then we say $f(x)$ is a characteristic polynomial of A over 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 F_2, then

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

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 F_2. Note that $G(A)$ is a principle ideal of $F_2[x]$ and $G(A) =< m(x) >$. So, if $f(x)$ is a characteristic polynomial of A over F_2, then $f(x) = m(x)h(x)$ where $h(x) \in F_2[x]$. The linear span of A over F_2, denoted as $LS(S)$, is defined as $LS(A) = deg(m(x))$.

C. Interleaved Sequences

We can depict 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 sequence $A = (A_0, A_1, \cdots, A_{t-1})^T$ where T is a transpose of a vector. In reference [20], A is called an interleaved sequence if A_i, $0 \leq i \leq t-1$, has the same minimal polynomial over 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 [20], 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*

$$m(x) | gcd\{m_0(x^t), m_1(x^t), \cdots, m_{t-1}(x^t)\}$$

D. Elliptic Curves over F_{2^n}

An elliptic curve E over $GF(2^n)$ can be written into the following standard form [35]

$$y^2 + y = x^3 + c_4 x + c_6, c_i \in GF(2^n) \tag{3}$$

if E is supersingular, or

$$y^2 + xy = x^3 + c_2 x^2 + c_6, c_i \in GF(2^n) \tag{4}$$

if E is non-supersingular. The points $P = (x, y)$, $x, y \in GF(2^n)$, 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 $2P = P + P = (x_3, y_3)$,

$$x_3 = x_1^4 + c_4^2 \quad (5)$$
$$y_3 = (x_1^2 + c_4)(x_1 + x_3) + y_1 + 1 \quad (6)$$

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

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

$$x_3 = \delta^2 + \delta + c_2$$
$$y_3 = (x_1 + x_3)\delta + x_3 + y_1$$

where $\delta = x_1 + y_1/x_1$. For $P+Q = (x_3, y_3)$, if $x_1 = x_2$, then $P+Q = O$. Otherwise,

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + c_2$$
$$y_3 = \lambda(x_1 + x_3) + x_3 + y_1$$

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 [14, 31, 37, 50, 35, 29].*

2 Constructions of Pseudorandom Sequences from Elliptic Curves over F_q

In this section, we give three types of constructions of binary sequences from an elliptic curve over F_q.

Let E be an elliptic curve over F_q. Let $P = (x_1, y_1)$ be a point of E with order $v+1|\#E(F_q)$. 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 and 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.

Construction I

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 $E(F_q)$ of type I*, an *EC-sequence* for short.

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 $v + 1 | \#E(F_q)$, and let $S = (S_0, S_1)^T$ be a EC-sequence generated by $E(F_q)$ of length $2v$ whose elements are given by (9).*

(i) *E is supersingular. Then*

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

(ii) *E is non-supersingular. Then*

$$S = \begin{pmatrix} A & 0 & \overleftarrow{A} \\ B & 0 & \overleftarrow{A} + \overleftarrow{B} \end{pmatrix} \text{ if } v = 2l + 1 \tag{11}$$

and

$$S = \begin{pmatrix} A & \overleftarrow{A} \\ B & \overleftarrow{A} + \overleftarrow{B} \end{pmatrix} \text{ if } v = 2l \tag{12}$$

Proof

Case 1 E is supersingular. Note that y and $y + 1$ are two roots of (3) in F_q under the condition $Tr(x^3 + c_4 x + c_6) = 0$. Since the order of P is $v + 1$, then

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

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

Case 2. E is non-supersingular. If v is odd, then

$$iP + (2l + 2 - i)P = O \Longrightarrow (l + 1)P = (0, 0), x_{l+1+i} = x_{l-i+1}, i = 1, \cdots, l.$$

Note that $x\alpha$ and $x\alpha + x$ are two roots of (4) in F_q under the condition $Tr(\beta) = 0$ where $\beta = x + a_6 x^{-1} + a_3$ and α is a root of the quadratic equation $z^2 + z = \beta$. So,

$$x_{l+1+i} = x_{l-i+1} \Longrightarrow y_{l+1+i} = y_{l-i+1} + x_{l-i+1}, i = 1, \cdots, l.$$

Thus $S_0 = (A, 0, \overleftarrow{A})$ and $S_1 = (B, 0, \overleftarrow{\overline{A}} + \overleftarrow{\overline{B}})$. If v is even, then $(0,0) \notin \Gamma$, then $S_0 = (A, \overleftarrow{A})$ and $S_1 = (B, \overleftarrow{\overline{A}} + \overleftarrow{\overline{B}})$.

□

Construction II

Let $\{\alpha, \alpha^2, \cdots, \alpha^{2^{n-1}}\}$ be a normal basis of $GF(2^n)$ over F_2. Then its dual basis is also a normal basis of $GF(2^n)$ over F_2 [31]. Let it be $\{\eta, \eta^2, \cdots, \eta^{2^{n-1}}\}$. For each point $iP = (x_i, y_i) \in \Gamma$, the coordinates x_i and y_i can be represented as

$$\begin{aligned} x_i &= \sum_{j=0}^{n-1} x_{ij}\alpha^{2^j}, i = 0, 1, \cdots, x_{ij} \in F_2 \\ y_i &= \sum_{j=0}^{n-1} y_{ij}\alpha^{2^j}, i = 0, 1, \cdots, y_{ij} \in F_2 \end{aligned}$$

and the coefficients $x_{i,j}$ and $y_{i,j}$ are determined by

$$\begin{aligned} x_{i,j} &= Tr(\eta^{2^j} x_i), 0 \le j \le n-1, i = 0, 1, \cdots, \\ y_{i,j} &= Tr(\eta^{2^j} y_i), 0 \le j \le n-1, i = 0, 1, \cdots, \end{aligned}$$

For a fixed j: $0 \le j \le n-1$, let

$$S_0 = (x_{1,j}, x_{2,j}, \cdots, x_{v,j}) \text{ and } S_1 = (y_{1,j}, y_{2,j}, \cdots, y_{v,j}) \tag{13}$$

An *EC-sequence S of type II*, written into a form of a $(2, v)$ interleaved sequence, will be defined as $S = (S_0, S_1)^T$. Theorem 1 can be generalized to this type of EC-sequences.

Remark 2 *The row sequences S_0 and S_1 of the EC-sequence constructed by (9) are just the sum of n component sequences $\{x_{i,j}\}_{i=1}^{v}$,$0 \le j \le n-1$ and the sum of n component sequences $\{y_{i,j}\}_{i=1}^{v}$, $0 \le j \le n-1$, respectively.*

Theorem 2 *Let $S = (S_0, S_1)^T$ be an EC-sequence defined by (13). Let*

$$A_j = (x_{1,j}, \cdots, x_{l,j}) \text{ and } B_j = (y_{1,j}, \cdots, y_{l,j}).$$

(i) *E is supersingular. Then*

$$S = \begin{pmatrix} A_0 & \overleftarrow{A_0} \\ B_0 & \overleftarrow{B_0} + 1 \end{pmatrix} \text{ if } j = 0 \text{ or } S = \begin{pmatrix} A_j & \overleftarrow{A_j} \\ B_j & \overleftarrow{B_j} \end{pmatrix} \text{ if } j > 0 \tag{14}$$

(ii) *E is non-supersingular. In the following formula, $\triangle$ represents zero element if $v = 2l+1$ and no element occurs here if $v = 2l$.*

$$S = \begin{pmatrix} A_j & \triangle & \overleftarrow{A_j} \\ B_j & \triangle & \overleftarrow{A_j} + \overleftarrow{\overline{B_j}} \end{pmatrix} \tag{15}$$

Proof Note that the proof of Theorem 1 only depends on the property of the points on the curve. Let $\beta = \sum_{j=0}^{n-1} c_j \alpha^{2^j}, c_j \in F_2$ and $\zeta = \sum_{j=0}^{n-1} d_j \alpha^{2^j}, d_j \in F_2$ are two elements in F_q. Then $\beta = \zeta$ if and only if $c_j = d_j$ for each $j : 0 \leq j \leq n-1$. Together with this result, the results follow by following the same proof as we did for Theorem 1. □

Construction III

Let

$$S = \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{v,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{v,1} \\ \vdots & \vdots & & \vdots \\ x_{1,n-1} & x_{2,n-1} & \cdots & x_{v,n-1} \\ y_{1,0} & y_{2,0} & \cdots & y_{v,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{v,1} \\ \vdots & \vdots & & \vdots \\ y_{1,n-1} & y_{2,n-1} & \cdots & y_{v,n-1} \end{pmatrix} \tag{16}$$

which is a $(2n, v)$ interleaved sequence where the first n row sequences are $\{x_{i,j}\}_{i=1}^{v}$, $0 \leq j \leq n-1$ and the last n row sequences are $\{y_{i,j}\}_{i=1}^{v}$, $0 \leq j \leq n-1$. S is called an *EC-sequence of type III*. As a consequence of Theorem 2, we have the following theorem.

Theorem 3 *With the same S defined by (16).*

(i) *E is supersingular. Then*

$$S = \begin{pmatrix} A_0 & \overleftarrow{A_0} \\ A_1 & \overleftarrow{A_1} \\ \vdots & \vdots \\ A_{n-1} & \overleftarrow{A_{n-1}} \\ B_0 & \overleftarrow{B_0} + 1 \\ B_1 & \overleftarrow{B_1} \\ \vdots & \vdots \\ B_{n-1} & \overleftarrow{B_{n-1}} \end{pmatrix} \tag{17}$$

(ii) *E is non-supersingular. In the following formula, $\triangle$ represents zero element if*

$v = 2l+1$ *and no element occurs here if* $v = 2l$.

$$S = \begin{pmatrix} A_0 & \triangle & \overleftarrow{A_0} \\ A_1 & \triangle & \overleftarrow{A_1} \\ \vdots & \vdots & \vdots \\ A_{n-1} & \triangle & \overleftarrow{A_{n-1}} \\ B_0 & \triangle & \overleftarrow{A_0} + \overleftarrow{B_0} \\ B_1 & \triangle & \overleftarrow{A_1} + \overleftarrow{B_1} \\ \cdots & \vdots & \vdots \\ B_{n-1} & \triangle & \overleftarrow{A_{n-1}} + \overleftarrow{B_{n-1}} \end{pmatrix} \tag{18}$$

Remark 3 *Construction III is the same method as used for constructing interleaved sequences in [20] and for mapping Reed-Solomon codes over* $GF(2^n)$ *to binary codes in [31].*

Starting with the next section, we restrict ourselves to discussing EC-sequences of type I. We will refer to these simply as *EC-sequences*. We will investigate the randomness properties of the other two types of EC-sequences in a separate paper.

3 Statistical Properties of Supersingular EC-Sequences

In this section, we discuss the statistical properties of EC-sequences generated by supersingular curves over 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 F_q to F_2. Let $g(x)$ be a function from F_q to F_2, the weight of g is defined as $w(g) = \{x \in F_q | g(x) = 1\}$. From [35], we have three different isomorphic classes for supersingular curves over F_q $(q = 2^n)$ for n odd. For two isomorphic curves $E(F_q)$ and $T(F_q)$, we denote as $E \cong T$.

Fact 1 *([33]) Let* $n = 2m+1$ *and* $q = 2^n$.

(i) *Let* $E_1 = \{E(F_q) | E(F_q) \cong y^2 + y = x^3\}$. *Then* $|E_1| = 2^{2n-1}$ *and for any* $E(F_q) \in E_1$, $\#E(F_q) = q+1$.

(ii) *Let* $E_2 = \{E(F_q) | E(F_q) \cong y^2 + y = x^3 + x\}$. *Then* $|E_1| = 2^{2n-2}$ *and* $\forall E(F_q) \in E_2$,

$$\#E(F_q) = \begin{cases} 2^n + 2^{m+1} + 1 & \text{if } n \equiv 1 \text{ or } 7 \bmod 8 \\ 2^n - 2^{m+1} + 1 & \text{if } n \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$$

(iii) *Let* $E_3 = \{E(F_q) | E(F_q) \cong y^2 + y = x^3 + x + 1\}$. *Then* $|E_1| = 2^{2n-2}$ *and* $\forall E(F_q) \in E_3$,

$$\#E(F_q) = \begin{cases} 2^n - 2^{m+1} + 1 & \text{if } n \equiv 1 \text{ or } 7 \bmod 8 \\ 2^n + 2^{m+1} + 1 & \text{if } n \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$$

From Fact 1, we have the following lemma.

Lemma 1 *Let* $q = 2^n$ *and* $n = 2m + 1$. *Let* $N = |\{x \in F_{2^n} | Tr(x^3 + x) = 0\}|$ *and* $\Delta = \sum_{x \in F_q} (-1)^{Tr(x^3+x)}$. *Then*

$$N = \begin{cases} 2^{n-1} + 2^m & \text{if } n \equiv 1 \text{ or } 7 \bmod 8 \\ 2^{n-1} - 2^m & \text{if } n \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$$

and

$$\Delta = \begin{cases} 2^{m+1} & \text{if } n \equiv 1 \text{ or } 7 \bmod 8 \\ -2^{m+1} & \text{if } n \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$$

Proof Since $\#E_2(F_q) = 2N + 1$, according to Fact 1, the first result follows. Note that

$$2^n - N = 2^{n-1} - \Delta/2 \Longrightarrow \Delta = 2N - 2^n.$$

So, the second result follows from the values of N.

□

Let

$$\Pi_1 = \{d \in F_q | 1 + d + x^2 + x^{n-1} = 0 \wedge Tr(dx + x^3) = 0 \text{ for some } x \in F_q\} \quad (19)$$

$$\Pi_2 = \{d \in F_q | 1 + d + x^2 + x^{n-1} = 0 \wedge Tr(dx + x^3) = 1 \text{ for some } x \in F_q\} \quad (20)$$

Theorem 4 *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* $E(F_{2^n})$ *where* $length(S) = 2v$ *and* $v = \#E(F_{2^n}) - 1$. *Then* $w(S_0) = 2w(A)$, $w(S_1) = v/2$ *and* $w(S) = 2w(A) + v/2$, *where* $w(A)$ *is determined as follows. Let* $c = (-1)^{Tr(c_6)}$.

(i) $E \in E_1 \Longrightarrow Tr(c_4) = 0$. *Then*

$$w(A) = \begin{cases} 2^{n-2} - \Delta/4 & \Longleftrightarrow 1 + c_4 \in \Pi_1 \\ 2^{n-2} + \Delta/4 & \Longleftrightarrow 1 + c_4 \in \Pi_2 \end{cases} \quad (21)$$

(ii) $E \in E_2 \Longrightarrow Tr(c_4) = 1$. *Then*

$$w(A) = \begin{cases} 2^{n-2} + c\Delta/4 & \Longleftrightarrow c_4 \in \Pi_1 \\ 2^{n-2} - c\Delta/4 & \Longleftrightarrow c_4 \in \Pi_2 \end{cases} \quad (22)$$

(iii) $E \in E_3 \Longrightarrow Tr(c_4) = 1$. *Then*

$$w(A) = \begin{cases} 2^{n-2} - c\Delta/4 & \Longleftrightarrow c_4 \in \Pi_1 \\ 2^{n-2} + c\Delta/4 & \Longleftrightarrow c_4 \in \Pi_2 \end{cases} \tag{23}$$

The proof of Theorem 4 uses the result on Gold pair sequences in [11]. Here we list this result with a slight modification.

Lemma 2 (Gold, 1968) *With the same* Δ, $\Pi_i, i = 1, 2$ *as the above. Let*

$$\sigma(d) = \sum_{x \in F_q} (-1)^{Tr(x^3 + dx + e)}, d, e \in F_q$$

and let $c = (-1)^{Tr(e)}$. *Then*

$$w(Tr(x^3 + dx + e)) = 2^{n-1} - \sigma(d)/2.$$

and the following two formulae are equivalent.

$$\sigma(d) = \begin{cases} 0 & \Longleftrightarrow Tr(d) = 0 \\ c\Delta & \Longleftrightarrow Tr(d) = 1 \wedge d \in \Pi_1 \\ -c\Delta & \Longleftrightarrow Tr(d) = 1 \wedge d \in \Pi_2 \end{cases}$$

Or equivalently,

$$w(Tr(x^3 + dx + e)) = \begin{cases} 2^{n-1} & \Longleftrightarrow Tr(d) = 0 \\ 2^{n-1} + c\Delta/2 & \Longleftrightarrow Tr(d) = 1 \wedge d \in \Pi_1 \\ 2^{n-1} - c\Delta/2 & \Longleftrightarrow Tr(d) = 1 \wedge d \in \Pi_2 \end{cases}$$

□

Proof of Theorem 4 Since $length(S) = 2v$, from Theorem 1, we have $w(S_0) = 2w(A)$ and $w(S_1) = v/2$. So, $w(S) = 2w(A) + v/2$. Let $g(x) = Tr(x^3 + c_4 x + c_6)$, $c_4, c_6 \in F_q$. Let

$$n_{i,j} = |\{x \in F_q | Tr(x) = i \wedge g(x) = j\}|, i, j \in F_2.$$

Then $w(A) = n_{10}$. For the rest of part of the proof, we will show how to compute n_{10}. Let $f(x) = Tr(x) + g(x)$. Then

$$w(f(x)) = w(Tr(x)) + w(g) - 2w(Tr(x)g). \tag{24}$$

Hence

$$w(f(x)) = n_{10} + n_{01} = 2^{n-1} + w(g) - 2n_{11}. \tag{25}$$

Let $\Lambda(c_4) = \sum_{x \in F_q} (-1)^{f(x)}$. Recalling that $c = (-1)^{Tr(c_6)}$. Then $\Lambda(c_4) = \sigma(1 + c_4)$. According to Lemma 2

$$\Lambda(c_4) = \begin{cases} 0 & \Longleftrightarrow & Tr(c_4) = 1 \\ c\Delta & \Longleftrightarrow & Tr(c_4) = 0 \wedge 1 + c_4 \in \Pi_1 \\ -c\Delta & \Longleftrightarrow & Tr(c_4) = 0 \wedge 1 + c_4 \in \Pi_2 \end{cases} \tag{26}$$

We also have

$$\Lambda(c_4) = n_{00} + n_{11} - (n_{10} + n_{01}). \tag{27}$$

(i) $E \in E_1 \Longrightarrow Tr(c_4) = 0$. According to Lemma 2 $\Longrightarrow w(g) = 2^{n-1} \Longrightarrow n_{00} = n_{11}$ and $n_{10} = n_{01}$. Therefore $n_{10} = 2^{n-1} - n_{11}$. Substituting it into (27), we get

$$n_{10} = 2^{n-2} - \Lambda(c_4)/4. \tag{28}$$

Substituting (26) into (28), the identity (21) follows.

(ii) $E \in E_2 \Longrightarrow Tr(c_4) = 1$. According to Lemma 2,

$$w(f) = 2^{n-1}. \tag{29}$$

Substituting (30) into (25), we have

$$n_{11} = w(g)/2. \tag{30}$$

From $w(Tr(x)) = 2^{n-1}$, we have

$$n_{10} + n_{11} = 2^{n-1} \Longrightarrow n_{10} = 2^{n-1} - n_{11}. \tag{31}$$

Again using Lemma 2, we have

$$w(g) = \begin{cases} 2^{n-1} - c\Delta/2 \Longleftrightarrow c_4 \in \Pi_1 \\ 2^{n-1} + c\Delta/2 \Longleftrightarrow c_4 \in \Pi_2 \end{cases} \tag{32}$$

Substituting (30), then (31), we get (22).

(iii) $E \in E_3 \Longrightarrow Tr(c_4) = 1$. According to the isomorphism between E and $y^2 + y = x^3 + x + 1$, then n_{10} under the condition $Tr(c_6) = 0 (or 1)$ is equal to n_{10} for $E \in E_2$ under the condition $Tr(c_6) = 1 (or 0)$. So, (23) follows.

□

Remark 4 *According to Theorem 2 and substituting the values of* Δ *from Lemma 1, we have the following distribution for 0's and 1's for the EC-sequence* S *generated by the isomorphic representative elements.*

Table 1 $n \equiv 1$ *or 7 mod 8*

$E(F_q)$	$length(S)$	$w(A)$	$w(S)$
$y^2 + y = x^3$	2^{n+1}	$2^{n-2} - 2^{m-1}$	$2^n - 2^m$
$y^2 + y = x^3 + x$	$2^{n+1} + 2^{m+2}$	$2^{n-2} + 2^{m-1}$	$2^n + 2^{m+1}$
$y^2 + y = x^3 + x + 1$	$2^{n+1} - 2^{m+2}$	$2^{n-2} - 2^{m-1}$	$2^n - 2^{m+1}$

Table 2 $n \equiv 3$ *or 5 mod 8*

$E(F_q)$	$length(S)$	$w(A)$	$w(S)$
$y^2 + y = x^3$	2^{n+1}	$2^{n-2} + 2^{m-1}$	$2^n + 2^m$
$y^2 + y = x^3 + x$	$2^{n+1} - 2^{m+2}$	$2^{n-2} - 2^{m-1}$	$2^n - 2^{m+1}$
$y^2 + y = x^3 + x + 1$	$2^{n+1} + 2^{m+2}$	$2^{n-2} + 2^{m-1}$	$2^n + 2^{m+1}$

4 Periods of Supersingular EC-Sequences

In this section, we discussion 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 $E(F_q)$ where $S_0 = (a_1, a_2, \cdots, a_v)$ and $v = \#E(F_q) - 1 = 2l$. 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,

$$x_{2i} = x_i^4 + c_4^2, i = 1, \cdots, l. \tag{33}$$

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

□

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* F_2.

Lemma 4 *Let U be a CF 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

$$u_{t+i} = u_i, i = 1, 2, \cdots. \tag{34}$$

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

$$u_{d-i} = u_{d+1+i}, 0 \leq i \leq d-1. \tag{35}$$

From (34) and (35), we get

$$u_{l-i} = u_{l+1+i}, 0 \leq i \leq l-1 \tag{36}$$

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

$$u_{l-i} = u_{l+i}, 1 \leq i \leq l-1 \tag{37}$$

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

$$u_{2i} = u_i + c,\ 1 \le i \le t. \tag{38}$$

In the following, we will prove that there exists $k : 0 \le k < l$ such that

$$(u_{t+2k+1}, u_{t+2k+2}) = (1,0). \tag{39}$$

If t is odd, since $0 < w(U) < 2d$, from P condition of U, it is easy to see that. Assume that t is oven. If $c = 1$ in CF condition, then $u_1 = u_2 + 1$. So, there at least exists one $k = 0$ such that (39) is true. If $c = 0$ in CF condition and $(u_{t+2k+1}, u_{t+2k+2}) = (1,1)$ or $(0,0)$ for all $k : 0 \le k < l$, then for any $1 \le i \le t$ we can construct the following sequence:

$$\begin{aligned} j_0 &= i; \\ j_1 &= (j_0 + \delta_1)/2 \\ j_2 &= (j_1 + \delta_2)/2 \\ &\vdots \\ j_r &= (j_{r-1} + \delta_r)/2 \\ &\vdots \end{aligned}$$

where

$$\delta_k = \begin{cases} 0 & \text{if } j_{k-1} \text{ even} \\ 1 & \text{if } j_{k-1} \text{ odd} \end{cases}$$

Keep doing this construction, till we reach $j_s = 2$ for some s. From the CF condition and the assumption, we have $u_k = u_2 = u_1$ for all $k \in \{j_0, j_1, \cdots, j_s\} \Longrightarrow u_i = u_1$ for any $1 \le i \le t \Longrightarrow w(U) = 0$ if $u_1 = 0$ and $w(U) = 2d$ if $u_1 = 1$ which is a contratiction with $0 < w(U) < 2d$. So, (39) is true.

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

$$u_{l+k+1} \overset{(38)}{=} u_{2l+2k+2} + c = u_{t+2k+2} + c. \tag{40}$$

On the other hand,

$$u_{l+k+1} \overset{(36)}{=} u_{l-k} \overset{(38)}{=} u_{2l-2k} + c = u_{t-2k} + c \overset{(35)}{=} u_{t+2k+1} + c \tag{41}$$

(40) and (41) $\Longrightarrow u_{t+2k+1} = u_{t+2k+2}$ which contradicts with (39). Thus $per(U) = 2d$.

Case 2 $t = 2l - 1$.

$$u_{l+k+1} \overset{(38)}{=} u_{2l+2k+2} + c = u_{t+2k+1} + c. \tag{42}$$

$$u_{l+k+1} \overset{(37)}{=} u_{l-k-1} \overset{(38)}{=} u_{2l-2k-2} + c = u_{t-2k-1} + c \overset{(35)}{=} u_{t+2k+2} + c \tag{43}$$

(42) and (43) $\Longrightarrow u_{t+2k+1} = u_{t+2k+2}$ which contradicts with (39). 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 $E(F_q)$, where $v|(\#E(F_q) - 1)$ 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 $E(F_q)$, where $v|(\#E(F_q) - 1)$. 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 5 *Let $S = (S_0, S_1)^T$ be a EC-sequence of length $2v$, generated by a supersingular elliptic curve $E(F_q)$, where $v|(\#E(F_q) - 1)$ 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 1 *Let n be odd. Let $S = (S_0, S_1)^T$ be a EC-sequence of length $2v$, generated by a supersingular elliptic curve $E(F_q)$, where $v|(\#E(F_q) - 1)$. Then $per(S) = 2v$.*

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

5 Linear Span of Supersingular EC-Sequences

In this section, we derive a lower bound and an upper bound for 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 rewrite 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,

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

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 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 $w(U) \equiv 0 \bmod 2$, let $p = 2^k$, we have

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

$\Longrightarrow g(x) = \sum_{i=0}^{p-1} x^i$ is a characteristic polynomial of U over 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 $F_2 \Longrightarrow$

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

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

□

Theorem 6 *Let n be odd. Let S be an EC-sequence of length $2v$, generated from a supersingular elliptic curve $E(F_q)$ which is isomorphic to $y^2 + y = x^3$, where $v = \#E(F_q) - 1$. Then*

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

Proof From Corollary 1, we have $per(S) = 2^{n+1}$. According to Theorem 4, $w(S) \equiv 0 \bmod 2$. 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 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,

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

□

6 Discussion

Now we have constructed a class of EC-sequences, generated by supersingular elliptic curves in E_1, which has large linear span and small bias unbalance. Precisely, let $n = 2m + 1$, and let

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

where $v = \#E(F_{2^n}) - 1$. We also denote $G(E_1)$ as an *elliptic curve pseudorandom sequence generator of type I (ECPSG I)*. According to Theorems 1 and Theorems 4-6, we have the following data for $S \in G(E_1)$.

- Structure:

$$S = \begin{pmatrix} A & \overleftarrow{A} \\ B & \overleftarrow{B} + 1 \end{pmatrix} \text{ where } A = (a_1, \cdots, a_{2^{n-1}}) \text{ and } B = (b_1, \cdots, b_{2^{n-1}})$$

  where $a_i = Tr(x_i)$, $b_i = Tr(y_i)$ and $\Gamma = \{P, 2P, \cdots, 2^nP\}$ where $iP = (x_i, y_i)$ and P is a point on an elliptic curve $E(F_{2^n}) : y^2 + y = x^3 + c_4x + c_6$ isomorphic to $y^2 + y = x^3$, which has order $\#E(F_{2^n}) = 2^n + 1$.

- Period: $per((A, \overleftarrow{A})) = 2^n$ and $per(S) = 2^{n+1}$.

- Distribution of 0's and 1's: $w(A) = 2^{n-2} \pm 2^{m-1}$ and $w(S) = 2^n \pm 2^m$. The bias of unbalance is equal to $\pm 2^m$ for S.

- Linear span: $2^{n-1} < LS(A) \leq 2^n - 1$ and $2^n < LS(S) \leq 2(2^n - 1)$.

In the following table 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. Since implementation of ECPSG relies only on implementation of elliptic curves over $GF(2^n)$, we can borrow software/hardware from elliptic curve public-key cryptosystems to implement ECPSG. We conclude that ECPSG I is suitable for use as a key generator in a stream cipher cryptosystem.

Table 3 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}	$2^n \pm 2^{(n-1)/2}$	$\pm 2^{(n-1)/2}$	$\geq 2^n$ $\leq 2^{n+1} - 2$

ACKNOWLEDGEMENT

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] N.G. de Bruijn, A combinatorial problem, *Kononklijke Nederlands Akademi van Wetenchappen, Proc.,* vol. 49, Pr. 2, 1946, pp. 758-764.

[3] L. Brynielsson, On the linear complexity of combined shift register sequences, *Advances in Cryptology-Eurocrypt'85*, Lecture Notes in Computer Science, vol. 219, Springer-Verlag, 1985, pp. 156-160.

[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] A. H. Chan. and R.A. Games, On the linear span of binary sequences from finite geometries, q odd, *Proceedings of Crypto'86,* pp. 405-417.

[6] 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.

[7] T. Etzion and A. Lempel, Construction of de Bruijn sequences of minimal complexity, *IEEE Trans. Inform. Theory*, Vol. IT-30, No. 5, September 1984, pp. 705-709.

[8] E. Filiol and C. Fontaine, Highly nonlinear balanced Boolean functions with a good correlation-immunity, *Advances in Cryptology-Eurocrypt'98*, Lecture Notes in Computer Science, vol. 1403, Springer-Verlag, Berlin, 1998, pp. 474-488.

[9] H. Fredrickson, A survey of full length nonlinear shift register cycle algorithms, *SIAM Rev.*, Vol. 24, pp. 195-229, Apr. 1982.

[10] 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.

[11] R. Gold, Maximal recursive sequences with 3-valued recursive cross-correlation functions, *IEEE Trans. on Inform. Theory*, January 1968, pp. 154-156.

[12] J.D. Golic,On the linear complexity of functions of periodic $GF(q)$ sequences, *IEEE Trans. on Inform. Theory* vol. IT-35, No. 1, January 1989, pp. 69-75.

[13] D. Gollman and W.G. Chambers, Clock-controlled shift registers: a review, *IEEE J. on Selected Areas in Comm.* vol. 7, No. 4, pp. 525-533, May 1989.

[14] S.W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982, pp. 39.

[15] 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.

[16] S. W. Golomb, On the classification of balanced binary sequences of period $2^n - 1$, *IEEE Trans. Inform. Theory*, vol. IT-26, pp. 730-732, Nov. 1980.

[17] G. Gong, On $q-$ary cascaded GMW sequences, *IEEE Trans. on Inform. Theory*, vol. 42, No. 1, January 1996, pp. 263-267.

[18] G. Gong, A new class of $q-$ary PN sequences, *IEEE Trans. on Inform. Theory*, May 1997.

[19] 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.

[20] 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.

[21] G. Gong and S.W. Golomb, Binary sequences with two-level autocorrelation, to appear in the March 1999 issue of *IEEE Trans. on Inform. Theory.*

[22] 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.

[23] J. Guajardo and C. Paar, Efficient algorithms for ellitic curve cryptosystems, *Advances in Cryptology-Crypto'97*, Lecture Notes in Computer Science, No. 1294, Springer-Verlag, 1997, pp. 342-356.

[24] T. Herlestam, On functions of linear shift register sequences, *Advances in Cryptology-Eurocrypt'85*, Lecture Notes in Computer Science, No. 219, Springer-Verlag, 1985, pp. 119-129.

[25] T. Herlestam, On the complexity of functions of linear shift register sequences, Preliminary version 8409.

[26] 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.

[27] N. Kalouptsidis and M. Manolarakes, Sequences of linear feedback shift registers with nonlinear feedforward logic, *IEE Proceedings,* vol. 130, Pt. E., No. 5, September 1983, pp.174-176.

[28] A. Klapper, A.H. Chan, and M. Goresky, Cascaded GMW sequences, *IEEE Trans. on Inform. Theory,* vol. IT-39, No. 1, pp. 177-183, January 1993.

[29] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1988.

[30] H. Krawczyk, The shrinking generator, *Fast Software Encryption: Cambridge Security Workshop*, Cambridge, UK., December 1993, Springer-Verlag LNCS 809 (1994).

[31] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, New York, 1977.

[32] J.L. Massey and S. Serconek, A Fourier transform approach to the linear complexity of nonlinearly filtered sequences, *Advances in Cryptology- Eurocrypt'94*, Lecture Notes in Computer Science, vol. 839, Springer-Verlag, Berlin, 1994, pp. 332-341.

[33] 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.

[34] J.L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. on Inform. Theory* vol. IT-15, January 1969.

[35] A.J. Menezes, *Elliptic Curve Public Key Cryptosystems,* Kluwer Academic Publishers, 1993.

[36] A.J. Menezes and S.A. Vanstone, Elliptic curve cryptosystems and their implementation, *Journal of Cryptology,* **6**(1993), pp.209-224.

[37] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Addison-Wesley, 1983.

[38] Jong-Seon No and P.V. Kumar, A new family of binary pseudo random sequences having optimal periodic correlation properties and large linear span, *IEEE Trans. on Inform. Theory,* vol. IT-35, No. 2, pp. 371-379, March 1989.

[39] 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.

[40] Y. Niho, *Multi-valued Cross-correlation Functions between Two Maximal Linear Recursive Sequences*, Ph. D. dissertation, Dept. Elec. Eng., Univ. Souththern California, 1972.

[41] J.D. Olsen, R.A. Scholtz, and L.R. Welch, Bent-function sequences, *IEEE Trans. on Inform. Theory*, vol. IT-28, No. 6, pp. 858-864, November 1982.

[42] I.R. Reed and G. Solomon, Polynomial codes over certain finite fields, *J. SIAM,* **8**(1960), pp. 300-304.

[43] 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.

[44] R.A. Rueppel, *Analysis and Design of Stream Ciphers,* Springer-Verlag, 1986.

[45] 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.

[46] R.A. Scholtz and L.R. Welch, GMW sequences, *IEEE Trans. on Inform. Theory*, vol. IT-30, No. 3, pp. 548-553, May 1984.

[47] T. Siegenthaler and R. Forre, Generation of binary sequences with controllable complexity and ideal $r-$tuple distribution, *Advances in Cryptology-Eurocrypt'87*, Lecture Notes in Computer Science, vol. 304, Springer-Verlag, 1987.

[48] T. Siegenthaler, Correlation-immunity of nonlinear combing functions for cryptographic applications, *IEEE Trans. Inform. Theory*, vol. IT-30, Sep. 1984, pp. 776-780.

[49] 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.

[50] M.K. Simon, J.K. Omura, R.A. Scholtz and B.K. Levitt, *Spread Spectrum Communications Handbook*, McGraw-Hill, Inc., Revised version, 1994.

[51] J.A. Solinas, An Improved algorithm for arithmetic on a family of elliptic curves, *Advances in Cryptology-Crypto'97*, Lecture Notes in Computer Science, vol. 1294, Springer-Verlag, 1997, pp. 367-371.

[52] N. Zierler and W.H. Mills, Products of linear recurring sequences, *Journal of Algebra*, **27**(1973).