Discrepancy Transforms and their Applications

Guang Gong

Center for Applied Cryptographic Research
Department of Combinatorics & Optimization
University of Waterloo
Waterloo, Ontario N2L 3G1, CANADA
Email. ggong@cacr.math.uwaterloo.ca

Abstract. In this paper, a new transform of ultimately periodic binary sequences, called a *discrepancy transform*, is developed. The discrepancy transform is computed in terms of the Berlekamp-Massey algorithm. It is shown that the discrepancy transform is a one-to-one correspondence between a set consisting of all ultimately periodic binary sequences and a set of sequences of all zeros but finite ones. A characteristic of linear span profiles of sequences is discovered by means of the discrepancy transform. A dynamic version of the Berlekamp-Massey algorithm is the presented. In terms of a restriction of the discrepancy transform computed by this version, a family of nonlinear permutations of $GF(2^n)$ is constructed. Applying a class of such permutations to filter function generators yields a new type of pseudo-random sequence generators, called *D-filter generators*. Sequences generated by a D-filter generator have period $2^n - 1$ with the balance property and achieve the maximal linear span $2^n - 2$ in most of cases for different LFSRs. The D-filter generator is dynamic and easier to randomly switch at different communication sections. The number of bit operations for output of one bit is bounded by $O(n^3)$; thus, it can be efficiently implemented in both hardware and software. D-filter generators have important applications in stream cipher cryptosystems and secure communication network. It is worth to point it out that the discrepancy transform provide a way for analysis of the Berlekamp *iterative* algorithm in permutational *functional* models. It can be applied to various decoding techniques in which decoding algorithms are related to the Berlekamp algorithm.

Key words. The Berlekamp-Massey algorithm, pseudo-random sequences, permutation, Boolean function, cryptology, and coding.

1 Introduction

Pseudo-random sequence generators are widely used in secure communication environment, such as key stream generators in stream cipher cryptosystems, section key generators in block cipher cryptosystmes and pseudo-random number generators in public-key cryptosystems. In this paper, we develop a new transform of ultimately periodic sequences, which is computed in terms of the Berlekamp-Massey algorithm. We call it the *discrepancy transform.* We show that the discrepancy transform is a one-to-one correspondence between a set consisting of all ultimately periodic binary sequences and a set of sequences of all zeros but finite ones.

In 1984, Rueppel [21] addressed the problem that a large linear span can not guarantee unpredictability of a sequence. He then suggested to consider a linear span profile of a sequence as a complement for randomness of the sequence. Since then, a lot of work have been done along this line [13][14][20]. We discovered that a linear span profile of a sequence is controlled by runs of zeros in its discrepancy transform sequence. This allows us to be able to give a definition for smoothly increased linear span profiles in quantity. Considering runs of the best randomness in a discrepancy transform sequence, we also propose a new criterion for randomness measurement of periodic sequences, which we call an *optimal linear span.*

There are two frequently used transforms in design and analysis of pseudo-random sequences. One is the discrete Fourier transform which maps a periodic sequence over $GF(q)$ from $GF(q)$ (time domain) to a spectral sequence whose elements are taken from the extension $GF(q^n)$ (frequency domain). The number of nonzero spectra of the discrete Fourier transform of a given sequence is equal to the linear span of the sequence. The other transform is the Hadamard transform which maps a periodic sequence over $GF(q)$ to a sequence of elements in the complex number field and it provides correlation properties of the sequence. The new transform, the discrepancy transform, maps periodic sequences to the same domain, but with different structure and provides the property of linear span profiles of sequences.

By inspiration of the fact that discrepancy transform sequences control the behaviors of linear span profiles, we explore the inverse process for constructing possible good pseudo-random sequence generators. We first restrict the discrepancy transform to an n dimensional linear space over $GF(2)$, and give a dynamic version of the Berlekamp Massey algorithm. We then derive a family of nonlinear permutations of a finite field $GF(2^n)$, called *D-permutations.* Applying the inverse D-permutations to filter generators provides a new pseudo-random sequence generator, called D-filter generators. A Filter generator is to operate a Boolean function on a set of stages of a linear feedback shift register, and a sequence results from an output of the Boolean function. It has been discussed extensively in the literature [12], [10], [21], [5]. In general, it is not easy to find a large number of filter functions (i.e., Boolean functions) for which an output sequence has good statistic properties, correlation and linear span properties. Applying component functions of the new permutations as filter functions, we are able to obtain a pseudo-random sequences with good randomness and unpredictability and easy to be implemented in both hardware and software.

In this paper, we only apply the discrepancy transform to analysis and design of pseudo-reandom sequence generators with strong cryptographic properties. We would like to point it out that the discrepancy transform also provides a way for analysis of the Berlekamp *iterative* algorithm [1] in permutational *functional* models. This is a completely new sight to look at this iterative algoritnm. It can be applied to various decoding techniques in which decoding algorithms are related to the Berlekamp algorithm.

This paper is organized as follows. Chapters 2-3 discuss the discrepancy transforms and their application in analysis of linear span profiles of sequences. Chapters 4-5 investigates to apply restricted discrepancy transforms to construct a family of permutations of $GF(2^n)$. In Chapter 6, we apply the family of permutations to filter function generators so that we get a new pseudo-random sequence generators with strong unpredictability and randomness. Further security analysis and implementation of the new generator will be provided in Chapter 7.

We conclude this section by introducing some concepts and notations that are frequently used in this paper.

A. Ultimately Periodic Sequences

Let $\underline{\mathbf{a}} = (a_0, a_1, \cdots,)$ be a sequence of elements of $\mathbb{F}_2 = GF(2)$. If there exist integers $N > 0$ and $u \geq 0$ such that $a_{n+N} = a_n$, for all $n \geq u$, then the sequence is called *ultimately periodic* with a parameter (u, N) and N is called a *period* of the sequence. The smallest number among all the possible periods of an ultimately periodic sequence is called the *least period* of the sequence. An ultimately periodic sequence $(a_0, a_1, \cdots,)$ with least period N is called *periodic* if $a_{n+N} = a_n$ holds for all $n = 0, 1, \cdots$. We also denote a sequence with period N as $\underline{\mathbf{a}} = (a_0, a_1, \cdots, a_{N-1})$.

Let $f(x)$ be a polynomial over $\mathbb{F}_2$. The smallest number among possible positive integers t with $f(x)|x^t - 1$ is called the *period* of the polynomial $f(x)$.

Let $\underline{\mathbf{a}}$ be a binary sequence of period N. Let $f(x) = x^l + c_{l-1}x^{l-1} + \cdots + c_1 x + c_0 \in F_2[x]$. If $\underline{\mathbf{a}}$ satisfies the following recursive relation

$$a_n = \sum_{i=0}^{l-1} c_i a_{n-l+i}, n = l, l+1, \cdots, \tag{1}$$

then we say that $f(x)$ is a *characteristic polynomial* of $\underline{\mathbf{a}}$ over $\mathbb{F}_2$, and $\underline{\mathbf{a}}$ is *generated* by an linear feedback shift register (LFSR) with the characteristic polynomial $f(x)$. We use symbol (f, l) to represent an l-stage LFSR with the characteristic polynomial $f(x)$ where $l = deg(f)$. The polynomial, say $m(x)$, with the smallest degree among possible characteristic polynomials of the sequence $\underline{\mathbf{a}}$ is called the *minimal polynomial* of the sequence. $LS(\underline{\mathbf{a}})$, the *linear span* of the sequence, is said to be the degree of the minimal polynomial of the sequence, i.e., $LS(\underline{\mathbf{a}}) = deg(m(x))$.

B. Sequences with a Finite Length

We use the symbol $\underline{\mathbf{a}}^N = a_0, a_1, \cdots, a_{N-1}, a_i \in \mathbb{F}_2$ to represent a sequence with a finite length N. LFSR (f, l) is said to *generate* a finite sequence $a_0, a_1, \cdots, a_{N-1}$ when this sequence coincides with the first N output elements of the l-stage LFSR (f, l) for the initial state $(a_0, a_1, \cdots, a_{l-1})$. If $l \geq N$, the LFSR always generates the sequence. If $l < N$, then the LFSR *generates* the sequence if and only if the formula (1) is true for all n with $l \leq n < N$. We also say that $f(x)$ is a characteristic polynomial of the sequence $\underline{\mathbf{a}}^N$. Similarly, we have a concept for the linear span of the sequence $\underline{\mathbf{a}}^N$ which is said to be the the shortest length of LFSRs that generate the sequence. As convention, we use the polynomial 1 to generate zero sequence $0, \cdots, 0$ with a finite length or the sequence $(0, 0, \cdots,)$ of all zeros.

C. Golomb Randomness Postulate II

Randomness Postulate II was proposed by Golomb in [4]. Here we make a slight change such that this postulate can be applied to a sequence with a finite length. In a binary sequence, k consecutive zeros (or ones) is called a *run of zeros (or ones) of length k*.

Randomness Postulate II (Run Property). For a binary sequence of period N or a sequence with a finite length N, in every period or a length N, half the runs have length one, one-fourth have length two, one-eighth have length three, etc., as long as the number of runs so indicted exceeds 1. Moreover, for each of these lengths, there are equally many runs of 0's and of 1's.

D. Cyclotomic Cosets, Polynomial Representation of Functions and Trace Representation of Periodic Sequences

Cyclotomic cosets modulo $2^n - 1$: A cyclotomic coset containing s consists of

$$C_s = \{s, s2, s2^2, \cdots, s2^{n_s - 1}\}$$

where n_s is the smallest positive integer such that $2^{n_s} s \equiv s \pmod{2^n - 1}$. The smallest number in C_s is called a *coset leader modulo* $2^n - 1$. Note that $n_s | n$.

Let $\mathbb{F}_q = GF(q)$, a finite field with q elements. The trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ is defined by $Tr_1^n(x) = x + x^2 + \cdots + x^{2^{n-1}}$. For any function $f : \mathbb{F}_{2^n} \longrightarrow F_2$, by the Lagrange interpolation, or equivalently, by the discrete Fourier transform, it has a polynomial representation as follows

$$f(x) = \sum c_i x^i, \text{ where } c_i \in \mathbb{F}_{2^n} \text{ with } c_{i2^j} = c_i^{2^j}. \tag{2}$$

In other words, $f(x)$ can be represented as sum of the trace functions $Tr_1^{n_r}(\beta_r x^r)$ where $r \in I$, the set consisting of all cyclotomic cosets modulo $2^n - 1$. I.e.,

$$f(x) = \sum_{r \in I} Tr_1^{n_r}(\beta_r x^r), \beta_r \in \mathbb{F}_{2^{n_r}}. \tag{3}$$

For any binary sequence $\{a_k\}$ of period $2^n - 1$, it can be represented by

$$a_k = f(\alpha^k), k = 0, 1, \cdots, \tag{4}$$

where α is a primitive element in $\mathbb{F}_{2^n}$ and $f(x)$ is given by (2), or equivalently, by (3). (4) is called the *trace representation* of the sequence. By this representation, $LS(\{a_k\})$, the linear span of $\{a_k\}$, is given by

$$LS(\{a_k\}) = |\{0 \le i < 2^n - 1 | c_i \ne 0\}| \tag{5}$$

where the c_i are the coefficients of $f(x)$ in (2), or equivalently,

$$LS(\{a_k\}) = \sum_{\beta_r \ne 0} n_r$$

where the β_r and n_r are defined by (3).

Note. In this paper, we will restrict ourselves to $\mathbb{F}_2$. But all the results obtained here can be easily generalized to an arbitrary finite field. For an introduction of sequence design and analysis, the reader is referred to [4], [21], [6].

2 Discrepancy Transforms

In this section, we will introduce the discrepancy transform and the inverse discrepancy transform. First we list the following notation which will be used in this section and the next section.

- $R = \{\{a_i\} | a_i \in \mathbb{F}_2\}$, a ring of binary sequences with infinite elements.
- $R_0 \subset R$ which contains all ultimately periodic sequences of R.
- $R_{-1} = \{(d_0, d_1, \cdots, d_{r-2}, d_{r-1}, 0, 0, \cdots) \in R\} \subset R$. I.e., if $\underline{\mathbf{d}} = \{d_i\} \in R_{-1}$, then there is a positive integer such that $d_i = 0, \forall i \geq r$. We denote it as $\{d_i\} = (d_0, d_1, \cdots, d_{r-1}, \dot{0})$, and call r the *ending point* of $\underline{\mathbf{d}}$ if $d_{r-1} \neq 0$.

Definition 1. *Let* $\underline{\mathbf{a}} = \{a_i\} \in R$. *For any* $n > 0$, *and let* $LFSR(f_{n-1}, l_{n-1})$ *generates a sequence* $a_0, a_1, \cdots, a_{n-1}$. *We put* $l = l_{n-1}$ *and* $f_{n-1} = x_l + \sum_{i=0}^{l-1} c_{n-1,i} x^i$. *Let*

$$d_n = a_n + \sum_{i=0}^{l-1} c_{n-1,i} a_{n-l+i}, n = 1, 2, \cdots. \tag{6}$$

Then d_n *is called* a next discrepancy bit *of the sequence, and* $\{f_i\}$ *is called a linear span profile of the sequence.*

Berlekamp Massey Algorithm (BMA) Let $a_0, a_1, \cdots, a_{N-1}$ be a binary sequence where $N > 0$. Then we have the following iterative formula to construct LFSR (f_n, l_n) that generates the sequence $a_0, a_1, \cdots, a_n$ for $n = 0, \cdots, N-1$.

1. The initial Step. Let $n_0 \geq 0$ be the index of the first nonzero bit of the sequence, i.e.,

$$a_0 = a_1 = \cdots = a_{n_0 - 1} = 0, \text{ and } a_{n_0} = 1. \tag{7}$$

   We then set

$$d_i = a_i, 0 \leq i \leq n_0,$$
$$f_0 = f_1 = \cdots = f_{n_0-1} = 1 \text{ and } l_0 = l_1 = \cdots = l_{n_0-1} = 0, \text{ for } n_0 > 0,$$
$$f_{-1} = 1 \text{ and } l_{-1} = 0 \text{ for } n_0 = 0,$$
$$f_{n_0}(x) = x^{n_0+1} + 1, \text{ and } l_{n_0} = n_0 + 1.$$

2. Loop Body. Now suppose that we already constructed $f_0, f_1, \cdots, f_{n-1}$, where LFSR (f_{n-1}, l_{n-1}) generates the sequence $a_0, a_1, \cdots, a_{n-1}$. Using (6) we compute the next discrepancy bit d_n.
   (a) If $d_n = 0$, then LFSR (f_{n-1}, l_{n-1}) still generates the sequence $a_0, a_1, \cdots, a_n$. We set that $f_n = f_{n-1}$ and $l_n = l_{n-1}$.

(b) If $d_n = 1$, then LFSR (f_{n-1}, l_{n-1}) generates the sequence $a_0, a_1, \cdots, a_{n-1}$, but not the sequence $a_0, a_1, \cdots, a_n$. Here $n > n_0$. LFSR (f_n, l_n) that generate the latter sequence can be constructed as follows. Suppose that m with $0 \leq m < n$ is the last number that the LFSR changes the length, i.e.,

$$l_{m-1} < l_m = \cdots = l_{n-1}.$$

and LFSR (f_{m-1}, l_{m-1}) generates the sequence $a_0, a_1, \cdots, a_{m-1}$, but not the sequence $a_0, a_1, \cdots, a_m$. Let

$$a = (m-1) - l_{m-1} + 1 \text{ and } b = (n-1) - l_{n-1} + 1. \tag{8}$$

i) If $a \geq b$, then $f_n(x) = f_{n-1}(x) + x^{a-b} f_{m-1}(x)$ and $l_n = l_{n-1}$.

ii) If $a < b$, then $f_n(x) = x^{b-a} f_{n-1}(x) + f_{m-1}(x)$ and $l_n = b - a + l_{n-1}$.

Repeat the process 2 till $n = N - 1$. Then LFSR (f_{N-1}, l_{N-1}) generates the sequence $a_0, a_1, \cdots, a_{N-1}$.

Note. The algorithm given here is a version of the BMA which generates a characteristic polynomial of the sequence. It is slightly different from the original BMA in [17]. The original version and other versions [15] [22] of the BMA generate a feedback polynomial of the sequence, which is the reciprocal polynomial of the characteristic polynomial of the sequence. The version provided here is easier to see the effect under the left shift operator on a sequence and the relationship between the constants a and b defined by (8) which will be used in Section 3. For a complete treatment of the BMA in this version, please see [6] (Chapter 6).

Definition 2. *Let* $\underline{\mathbf{a}} = \{a_i\} \in R_0$ *be a binary sequence with parameter* (u, N)*, and let* $M = 2N + u$*. Let* $D(\underline{\mathbf{a}}) = \{d_n\}$ *be a sequence in* R_{-1} *where* d_n *is the next discrepancy bit computed by the BMA for* $0 \leq n < M$ *and* $d_n = 0$ *for all* $n \geq M$*. Then* D *is called a* discrepancy transform *from* R_0 *to* R_{-1}*. The sequence* $\{d_i\}$ *is called a* discrepancy (transform) sequence *of* $\{a_i\}$*.*

For example, $\underline{\mathbf{a}} = (1001011)$ be a sequence of period 7. Then

$$D(\underline{\mathbf{a}}) = \{d_i\} = (1101010000\cdots) = (110101\,\dot{0}).$$

Let $LS(x)$ represents the linear span of a sequence x. The following result is clear from the BMA.

Proposition 1. *Let* $\underline{\mathbf{a}} = \{a_i\}$ *be a sequence in* R_0 *with period* N *and* $D(\underline{\mathbf{a}}) = \{d_i\}$ *be the discrepancy sequence of* $\underline{\mathbf{a}}$*. If* $LS(\underline{\mathbf{a}}) = l$*, then* $d_n = 0, \forall n \geq 2l$*.*

Theorem 1. *D is a bijective map between R_0 and R_{-1}.*

Proof. Let $\underline{\mathbf{a}} = \{a_n\} \in R_0$ be an ultimately sequence with parameter (u, N). From the BMA, the polynomials $f_n, 0 \leq n < M$, constructed by the BMA are uniquely determined. Since the elements of $\{d_n\}$ is computed by the formula (6), then it is clear that D is an injective. So, we only need to show that D is surjective. I.e., we need to prove that for any sequence $\underline{\mathbf{d}}$ in R_{-1}, there exists an ultimately periodic sequence $\underline{\mathbf{a}} \in R_0$ such that $\underline{\mathbf{d}}$ is the discrepancy sequence of $\underline{\mathbf{a}}$. We construct a sequence $\underline{\mathbf{a}}$ from $\underline{\mathbf{d}}$ by switching the places of a_n and d_n in the BMA. A detail of these steps is stated as follows.

1. Let n_0 be the index of the first nonzero bit of $\underline{\mathbf{d}} = (d_0, d_1, \cdots, d_{r-1}, \dot{0})$. Then we set
$$a_i = d_i, 0 \leq i \leq n_0. \tag{9}$$
Using the BMA we construct $f_i, 0 \leq i \leq n_0$.
2. Suppose that we already constructed $a_0, a_1, \cdots, a_{n-1}$, and $f_0, f_1, \cdots, f_{n-1}$ by the BMA. We then construct a_n by switching the places of a_n and d_n in the formula (6), i.e.,
$$a_n = d_n + \sum_{i=0}^{l-1} c_{n-1,i} a_{n-l+i} \tag{10}$$
where $l = l_{n-1}$. Repeat this step till $n = r - 1$.
3. For all $n \geq r$, let a_n be generated by f_{r-1}.

Therefore LFSR (f_{r-1}, l_{r-1}) generates the sequence $\underline{\mathbf{a}}$. Thus $\underline{\mathbf{a}}$ is an ultimately periodic sequence with the parameter (u, t) where $t = per(g)$ where $f_{r-1} = x^t g(x)$ with $g(0) \neq 0$. (For a proof of this result, see Theorem 8.27 and its proof in [16].) In other words, we get that $a_{n+t} = a_n$ for all $n \geq u$. So, $\underline{\mathbf{a}} \in R_0$ and $D(\underline{\mathbf{a}}) = \underline{\mathbf{d}}$. Thus D is a surjective map from R_0 to R_{-1}. Therefore D is a bijective map between R_0 and R_{-1}.

According to Theorem 1, D is invertible and $D^{-1}(\underline{\mathbf{d}})$ is constructed by steps 1-3 in the proof of Theorem 1. The inverse map D^{-1} of D is called the *inverse discrepancy transform (IDT)*, and the sequence $D^{-1}(\underline{\mathbf{d}})$ is called an *inverse discrepancy (transform) sequence* of $\underline{\mathbf{d}}$.

From the proof of Theorem 1, we have the following result on the inverse discrepancy sequences.

Corollary 1. *With the notation in Theorem 1.*

(a) f_{r-1} *is the minimal polynomial of* $D^{-1}(\underline{\mathbf{d}})$*, so that* l_{r-1} *is the linear span of the inverse discrepancy sequence, i.e.,* $LS(D^{-1}(\underline{\mathbf{d}})) = l_{r-1}$*. Furthermore,* $l_{r-1} = \lceil r/2 \rceil$ *where* $\lceil x \rceil$ *represents the least integer that is not less than* x*.*

(b) $D^{-1}(\underline{\mathbf{d}})$ *is an ultimately periodic sequence with the parameter* (u, t) *where* $u \leq l_{r-1}$ *and* $t = per(g)$ *where* $f_{r-1}(x) = x^t g(x)$ *with* $g(0) \neq 0$*.*

Proof. Without loss of generality, we can suppose that $d_{r-1} = 1$. Otherwise, the ending point of $\underline{\mathbf{d}}$ will degenerate to $r - 1$. According to the proof of Theorem 1, f_{r-1} is a characteristic polynomial of $D^{-1}(\underline{\mathbf{d}})$. Note that f_{r-1} is constructed by the BMA. Hence f_{r-1} has the smallest degree among all characteristic polynomials of $D^{-1}(\underline{\mathbf{d}})$. Thus f_{r-1} is the minimal polynomial of the inverse discrepancy sequence. So that $l_{r-1} = LS(D^{-1}(\underline{\mathbf{d}}))$. Since $2l_{r-1} \leq r$ and $d_{r-1} = 1$, then $l_{r-1} = \lceil r/2 \rceil$. The second result directly follows from the result (a).

Example 1. Let $\underline{\mathbf{d}} = (1001011\,\dot{0}) \in R_{-1}$ with $r = 7$. Then

$$D^{-1}(\underline{\mathbf{d}}) = \underline{\mathbf{a}} = 11101111011110\cdots \in R_0$$

which is a periodic sequence with period 5. I.e., $a_{n+5} = a_n$ for all $n \geq 0$. Furthermore, $f_6 = x^4+x^3+x^2+x+1$ which has period 5. Note that the first 7 elements of $\underline{\mathbf{d}}$ are taken from the elements in a period of an m-sequence with period 7.

Example 2. Let $\underline{\mathbf{d}} = (110011010001011\,\dot{0}) \in R_{-1}$ with $r = 15$. Then

$$\begin{aligned} D^{-1}(\underline{\mathbf{d}}) = {} & 10001110 \\ & 0010101101000011001001111101110 \\ & 0010101101000011001001111101110\cdots. \end{aligned}$$

Hence $f_{14}(x) = x^8 + x^7 + x^6 + x^5 + x^3 = x^3 g(x)$ where $g(x) = x^5 + x^4 + x^3 + x^2 + 1$ a primitive polynomial over $\mathbb{F}_2$. Therefore $LS(D^{-1}(\underline{\mathbf{d}})) = 8$ and $D^{-1}(\underline{\mathbf{d}}) = \underline{\mathbf{a}}$ is an ultimately periodic sequence with the parameter $(3, 31)$. I.e., $a_{n+31} = a_n$ for all $n \geq 3$. Note that the first 15 element of $\underline{\mathbf{d}}$ are taken from the elements of a period of a modified de Bruijn sequence [18] with period 15.

3 Runs of Discrepancy Sequences and Linear Span Profiles

In this section, we first show a characteristic of linear span profiles of sequences in terms of their discrepancy transform sequences. Then we give a criterion for a smoothly linear span profile and an optimal linear span by means of runs of the best randomness in the discrepancy sequence.

The following two lemmas come from the BMA. A proof for the first lemma can be found in [17]. As for a proof for the second lemma, it can be derived from the first lemma. However we omit details here due to short of space.

Lemma 1. *Let $\underline{\mathbf{a}} \in R_0$, $\{d_n\}$ be its discrepancy sequence related to LFSR $(f_n, l_n), n = 0, 1, \cdots,$ which are constructed by the BMA. For any $n > 0$ and $c \in \mathbb{F}_2$, if $(d_{n-1}, d_n) = (c, 0)$, then $f_n = f_{n-1}$, so that $l_n = l_{n-1}$. If $(d_{n-1}, d_n) = (c, 1)$, then $f_n \neq f_{n-1}$ and $l_n = l_{n-1} \Longleftrightarrow 2l_{n-1} > n$ and $l_n = n + 1 - l_{n-1} \Longleftrightarrow 2l_{n-1} \leq n$.*

Lemma 2. *With the notation in Lemma 1. Let m, n, a and b be defined at the loop body in the BMA. Then $a \geq b \Longleftrightarrow 2l_{n-1} > n$ and $a < b \Longleftrightarrow 2l_{n-1} \leq n$.*

In a proof of the following theorem, we will use a notation that $x = (x_0, x_1, \cdots, x_{n-1})$ is a string for $n > 0$ and $x = \emptyset$ if $n = 0$ and $l(x) = n$, the length of the string.

Theorem 2. *Let* $\underline{\mathbf{a}} \in R_0$ *and* $\underline{\mathbf{d}}$ *be its discrepancy sequence. Let* $\mu(\underline{\mathbf{d}}^r)$ *be the greatest length of runs of 0's in* $\underline{\mathbf{d}}^r = (d_0, d_1, \cdots, d_{r-1})$*. Then* $\{l_n\}$*, the linear span profile of* $\underline{\mathbf{a}}$*, satisfies*

$$l_n - l_{n-1} \leq \mu(\underline{\mathbf{d}}^r) + 1, \ \forall n > 0. \tag{11}$$

Proof. If $l_n = l_{n-1}$, then (11) is true. Suppose that $l_n \neq l_{n-1}$, then we have $l_n > l_{n-1}$. If

$$l_0 = l_1 = \cdots = l_{n-1} = 0,$$

then $d_i = 0$, $0 \leq i < n$, and $l_n = n + 1$ from the initial step in the BMA. Thus

$$l_n - l_{n-1} = n + 1 = l(d_0, d_1, \cdots, d_{n-1}) + 1 \leq \mu(\underline{\mathbf{d}}^r) + 1.$$

If $l_{n-1} > 0$, according to the loop step in the BMA, there exists a unique $m \geq 0$ such that

$$l_{m-1} < l_m = l_{m+1} = \cdots = l_{n-1} < l_n.$$

From Lemma 1, for any i in $I = \{m, m+1, \cdots, n-1\}$, if $(d_{i-1}, d_i) = (c, 1), c \in \mathbb{F}_2$, then f_i changes. But the linear span l_i doesn't changes. Let $a = (m-1) - l_{m-1} + 1$ and $b_i = (i-1) - l_{i-1} + 1, i \in I$. Since the l_i are unchanged for such i, applying Lemma 2, it follows that

$$a - b_i \geq 0, m \leq i < n, \text{ but } a - b_n < 0. \tag{12}$$

Let j be the greatest number in I such that

$$(d_{j-1}, d_j) = (c, 1), c \in \mathbb{F}_2, \text{ and } d_{j+1} = \cdots = d_{n-1} = 0.$$

Thus $(d_{j+1}, d_{j+2}, \cdots, d_{n-1})$ is a run of 0's in $\underline{\mathbf{d}}^r$ with length $n - 1 - (j+1) + 1 = n - j + 1$. From the BMA, $l_n = b_n - a + l_{n-1}$. Together with (12), we have

$$\begin{aligned} l_n - l_{n-1} &= b_n - a < b_n - b_j = n - l_{n-1} - (j - l_{j-1}) \\ &= n - j = l(d_{j+1}, \cdots, d_{n-1}) + 1 \leq \mu(\underline{\mathbf{d}}^r) + 1. \end{aligned}$$

Thus the result is true.

From the proof of Theorem 2, we have the following corollary directly.

Corollary 2. *With the notation in Theorem 2. For any* $n > 0$*,*

$$l_n - l_{n-1} = l(d_{j+1}, d_{j+2}, \cdots, d_{n-1}) + 1$$

where j *is the greatest number in a set of* $\{m, m+1, \cdots, n-1\}$ *such that* $d_j = 1$ *and* $(d_{j+1}, d_{j+2}, \cdots, d_{n-1})$ *is a run of 0's where* m *is an integer satisfying* $l_{m-1} < l_m = l_{m+1} = \cdots = l_{n-1}$*. In other words, the difference between* l_n *and* l_{n-1} *is 1 more than the length of the run of 0's preceded to* d_n*.*

According to Theorem 2 and Corollary 2, the behavior of the linear span profile of a periodic sequence is completely determined by lengths of runs of 0's in the discrepancy sequence. If we consider the inverse process, then physical meaning of a discrepancy sequence becomes more clear. In other words, the inverse process can be considered as follows: Given a sequence $\underline{\mathbf{d}} \in R_{-1}$ as a controlling state of a pseudo-random sequence generator (PSG), the PSG generates an inverse discrepancy sequence $D^{-1}(\underline{\mathbf{d}}) = \{a_i\}$ in the following fashion. Each clock cycle $n > 0$, if $d_n = 0$, then the PSG uses the previous LFSR to generate a current bit a_n. If $d_n = 1$, then the PSG reloads a new LFSR to generate a current bit a_n. So the nth bit of output of the PSG is generated by the previous LFSR or a new LFSR depending on $\{d_n\}$. In the discepancy sequence, a run of 0's of length t means that the PSG doesn't change the LFSR during t consecutive clock cycles. A run of 1's of length t means that the PSG changes LFSR at each clock cycle during t consecutive clock cycles where the lengths of these LFSRs may not change. Runs of the best randomness of a discrepancy sequence is that it satisfies Golomb Randomness Postulate II. In this case, a frequency that the PSG changes LFSRs can be considered as a random variable with a uniform distribution. We summarize these discussions into the following criteria for measuring randomness of pseudo-random sequences.

Let $\underline{\mathbf{a}}$ be a sequence of period N and $\underline{\mathbf{d}} = (d_0, d_1, \cdots, d_{r-1}, \dot{0})$ be its discrepancy sequence. Note that if a sequence of period N or length N satisfies Golomb Randomness Postulate II, then the greatest length of runs in the sequence is bounded by $\sigma(N) = \lceil log_2^N \rceil + 1$. So $\sigma(r)$ is the best bound for $\mu(\underline{\mathbf{d}}^r)$, the greatest length of the runs of zeros in $\underline{\mathbf{d}}^r$, regarding the randomness of runs in $\underline{\mathbf{d}}^r$.

- *Smoothly Linear Span Profile:* If $\mu(\underline{\mathbf{d}}^r) < \sigma(r)$ for any shift of $\underline{\mathbf{a}}$, then we say that $\underline{\mathbf{a}}$ has a *smoothly linear span profile.*
- *Optimal Linear Span:* If $\underline{\mathbf{d}}^r$ satisfies Golomb Randomness Postulate II for any shift of $\underline{\mathbf{a}}$, and $LS(\underline{\mathbf{a}})$, the linear span of $\underline{\mathbf{a}}$, satisfies that

$$N/2 - \epsilon < LS(\underline{\mathbf{a}}) < N \text{ where } 0 \leq \epsilon \leq c\sigma(r) \tag{13}$$

where $c \geq 0$ is a constant, then we say that $\underline{\mathbf{a}}$ has an *optimal linear span.*

Note that if a sequence has an optimal linear span, then it has a smoothly linear span profile as we pointed out before.

We did tests for some known generators with small parameters. We considered three types of known pseudo-random sequences whose linear spans satisfy (13) for general parameters. They are de Bruijn sequences [3] with period 2^n, the self-shrink sequences [19] with period 2^{n-1}, and the elliptic curve sequences of type I [8] with period 2^{n+1} where n is the parameter related to their construction. If $2^n - 1$ is a prime, then we have quadratic sequences with period $2^n - 1$ [?] which satisfy the condition (13). For their discrepancy sequences, none of them satisfies Golomb Randomness Postulate II. However, the experimental results showed that some of them did satisfy the condition for smoothly linear span profiles.

When we use the inverse process to generate pseudo-random sequences discussed above, it is clear that the nth bit depends on the previous $n-1$ bits. Thus it is impossible to hold or store the entire bits of an inverse discrepancy sequence in practical cryptosystems. How we can generate a sequence while considerably preserving the feature provided by inverse discrepancy sequences with good randomness and extremely reducing the computational cost both in time and space. This is the purpose of the remaining sections.

4 Restricted Discrepancy Transforms

In this section, we will discuss a restriction of the discrepancy transform on $\mathbb{F}_2^{(n)}$.

Let $V = \mathbb{F}_2^{(n)}$. Then V can be embedded into R_0 [11] via

$$(x_0, x_1, \cdots, x_{n-1}) \longmapsto (x_0, x_1, \cdots, x_{n-1}, x_0, x_1, \cdots, x_{n-1}, \cdots) \in R_0.$$

Thus we have D_V, a restriction of D on V, as follows

$$D_V(a_0, a_1, \cdots, a_{n-1}) = (d_0, d_1, \cdots, d_{n-1}) \tag{14}$$

where $d_i, 0 \leq i < n$ are computed by the BMA. Note that any function from V to V can be represented by it's n component functions. I.e., we can write

$$D_V(x_0, x_1, \cdots, x_{n-1}) = (g_{n,0}, g_{n,1}, \cdots, g_{n,n-1}), x_i \in F_2$$

where $g_{n,j} = g_{n,j}(x_0, x_1, \cdots, x_{n-1})$ is a function from V to $\mathbb{F}_2$, i.e., a Boolean function in n variables $x_0, x_1, \cdots, x_{n-1}$.

Lemma 3. *D_V is a permutation of $\mathbb{F}_{2^n}$.*

Proof. According to Theorem 1, D_V is a bijective map on V. Since V is isomorphic to the finite field $\mathbb{F}_{2^n}$, then D_V is a permutation of $V = \mathbb{F}_{2^n}$.

We call D_V a *restricted discrepancy transform (RDT)* on V and D_V^{-1} the *inverse restricted discrepancy transform (IRDT)* on V.

Example 3. In the following, we represent D_V for $n = 1, 2, 3, 4$ as a truth table, a Boolean function and an element of S_{2^n}, the symmetric group of permutations on the set $\{0, 1, 2, \cdots, 2^n - 1\}$, respectively. Here we regard an element of V as a binary representation of an integer. I.e., we view V as $\mathbb{Z}_{2^n}$, a ring of integers modulo 2^n.

Table 1. Truth Table of D_V

x_0	x_1	D_V	$g_{2,0}$	$g_{2,1}$
0	0		0	0
1	0		1	1
0	1		0	1
1	1		1	0

For $n = 1$, $D_V : 0 \mapsto 0$ and $1 \mapsto 1$. So $D_V = x_0$, the identity map. For $n = 2$, from Table 1, we can compute the algebraic normal form (ANF) of D_V as follows

$$g_{2,0}(x_0, x_1) = x_0 \text{ and } g_{2,1}(x_0, x_1) = x_0 + x_1.$$

As a permutation of S_4,

$$D_V = \begin{pmatrix} 0\,1\,2\,3 \\ 0\,3\,2\,1 \end{pmatrix} = (13).$$

For $n = 3$, from Table 2, we have the AFN of D_V as follows

Table 2. Truth Table of D_V

x_0	x_1	x_2	D_V	$g_{3,0}$	$g_{3,1}$	$g_{3,2}$
0	0	0		0	0	0
1	0	0		1	1	0
0	1	0		0	1	0
1	1	0		1	0	1
0	0	1		0	0	1
1	0	1		1	1	1
0	1	1		0	1	1
1	1	1		1	0	0

$$g_{3,0}(x_0, x_1, x_2) = x_0,$$

$$g_{3,1}(x_0, x_1, x_2) = x_0 + x_1, \text{ and}$$

$$g_{3,2}(x_0, x_1, x_2) = x_0 x_1 + x_2.$$

As a permutation of S_8,

$$D_V = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,3\,2\,5\,4\,7\,6\,1 \end{pmatrix} = (1357).$$

For $n = 4$, from Table 3, the AFN of D_V is as follows:

$$g_{4,0}(x_0, x_1, x_2, x_3) = x_0,$$

$$g_{4,1}(x_0, x_1, x_2, x_3) = x_0 + x_1,$$

$$g_{4,2}(x_0, x_1, x_2, x_3) = x_0 x_1 + x_2, \text{ and}$$

$$g_{4,3}(x_0, x_1, x_2, x_3) = x_1 + x_1 x_2 + x_0 x_1 x_2 + x_3.$$

Table 3. Truth Table of D_V

x_0	x_1	x_2	x_3	D_V	$g_{4,0}$	$g_{4,1}$	$g_{4,2}$	$g_{4,3}$
0	0	0	0		0	0	0	0
1	0	0	0		1	1	0	0
0	1	0	0		0	1	0	1
1	1	0	0		1	0	1	1
0	0	1	0		0	0	1	0
1	0	1	0		1	1	1	0
0	1	1	0		0	1	1	0
1	1	1	0		1	0	0	1
0	0	0	1		0	0	0	1
1	0	0	1		1	1	0	1
0	1	0	1		0	1	0	0
1	1	0	1		1	0	1	0
0	0	1	1		0	0	1	1
1	0	1	1		1	1	1	1
0	1	1	1		0	1	1	1
1	1	1	1		1	0	0	0

As a permutation of S_{16},

$$D_V = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 3 & 10 & 13 & 4 & 7 & 6 & 9 & 8 & 11 & 2 & 5 & 12 & 15 & 14 & 1 \end{pmatrix} = (1,3,13,15)(2,10)(5,7,9,11).$$

From this example, we observed that

$$g_{n,0} = g_{1,0}, 1 \leq n \leq 4,$$

$$g(n,1) = g(2,1), 2 \leq n \leq 4,$$

$$g(n,2) = g(3,2), 3 \leq n \leq 4.$$

This is a general result which we state it in the following theorem.

Theorem 3. *Let $D_V = (g_{n,0}, g_{n,1}, \cdots, g_{n,n-1})$ be the restricted discrepancy transform on V. Then*

(a)

$$g_{n,i}(x_0, x_1, \cdots, x_{n-1}) = g_{i+1,i}(x_0, x_1, \cdots, x_i), 0 \leq i < n \tag{15}$$

Precisely, for $i = 0, 1, 2,$ and 3, we have

$$g_{1,0}(x_0) = x_0,$$

$$g_{2,1}(x_0, x_1) = x_0 + x_1,$$

$$g_{3,2}(x_0, x_1, x_2) = x_0 x_1 + x_2,$$

$$g_{4,3}(x_0, x_1, x_2, x_3) = x_1 + x_1 x_2 + x_0 x_1 x_2 + x_3.$$

(b)

$$D_V(x_0, x_1, \cdots, x_{n-1}) = (x_0, x_0 + x_1, g_{3,2}, g_{4,3}, \cdots, g_{n,n-1})$$

(c)

$$g_{n,n-1}(x_0, x_1, \cdots, x_{n-2}, 1) = 1 + g_{n,n-1}(x_0, x_1, \cdots, x_{n-2}, 0) \tag{16}$$

which is equivalent to

$$g_{n,n-1}(x_0, x_1, \cdots, x_{n-1}) = h(x_0, x_1, \cdots, x_{n-2}) + x_{n-1}, n > 1 \tag{17}$$

where $h(x_0, x_1, \cdots, x_{n-2})$ is a Boolean function in $n-1$ variables $x_0, x_1, \cdots, x_{n-2}$.

(d) D_V is an nonlinear permutation of $\mathbb{F}_{2^n}$ for $n > 2$.

Proof. Since $D_V(a_0, a_1, \cdots, a_{n-1}) = (d_0, d_1, \cdots, d_{n-1})$, according to the BMA, d_i, the ith discrepancy bit, only depends on $a_0, a_1, \cdots, a_i$ for any i with $0 \leq i < n$. This establishes (15). From Example 1, the second half of assertion (a) is clear. Assertion (b) follows from (a) directly. For the result (c), by the BMA, $d_{n-1} = a_{n-1} + c$ where c is a constant determined by $a_0, a_1, \cdots, a_{n-2}$. Thus $d_{n-1} = c$ for $a_{n-1} = 0$ and $d_{n-1} = 1 + c$ for $a_{n-1} = 1$. Since $d_{n-1} = g_{n,n-1}(a_0, a_1, \cdots, a_{n-1})$, then $g_{n,n-1}(a_0, a_1, \cdots, a_{n-2}, 0) = c$ and $g_{n,n-1}(a_0, a_1, \cdots, a_{n-2}, 1) = 1 + c$. Hence the identity (16) follows. Applying the result on the Boolean functions in [4] (Theorem 1, Assertions 8 and 9 in Chapter VI), (16) is equivalent to (17). Note that a permutation on V is linear if and only if its each component function is linear. According to (a) and (b), the third component function $g_{n,2} = g_{3,2}$ is nonlinear for $n > 2$. So D_V is nonlinear on V for $n > 2$ which gives (d).

The inverse restricted discrepancy transform D_V^{-1} has similar properties as those of D_V. First, we look at an example. We put $D_V^{-1}(x) = (f_{n,0}, f_{n,1}, \cdots, f_{n,n-1})$ where $f_{n,j} = f_{n,j}(x_0, x_1, \cdots, x_{n-1}), 0 \leq j < n$.

Example 2. IRDT $D_V^{-1}(x)$ for small dimensions.

For $n = 1$, $D_V^{-1} : 0 \mapsto 0, 1 \mapsto 1$. I.e., $D_V^{-1} = D_V$, the identity map. For $n = 2$, from Table 4, we have the

Table 4. Truth Table of D_V^{-1}

x_0	x_1	D_V^{-1}	$f_{2,0}$	$f_{2,1}$
0	0		0	0
1	0		1	1
0	1		0	1
1	1		1	0

AFN of D_V^{-1} $f_{2,0}(x_0, x_1) = x_0$ and $f_{2,1}(x_0, x_1) = x_0 + x_1 = g_{2,1}$. As a permutation of S_4,

$$D_V^{-1} = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 3 & 2 & 1 \end{pmatrix} = (13) = D_V.$$

For $n = 3$, from Table 5, we have the folllowing AFN of D_V^{-1},

Table 5. Truth Table of D_V^{-1} for $n = 3$

x_0	x_1	x_2	D_V^{-1}	$f_{3,0}$	$f_{3,1}$	$f_{3,2}$
0	0	0		0	0	0
1	0	0		1	1	1
0	1	0		0	1	0
1	1	0		1	0	0
0	0	1		0	0	1
1	0	1		1	1	0
0	1	1		0	1	1
1	1	1		1	0	1

$$f_{3,0} = x_0,$$

$$f_{3,1}(x_0, x_1) = x_0 + x_1 = f_{2,1}, \text{ and}$$

$$f_{3,2}(x_0, x_1, x_2) = x_0 + x_0x_1 + x_2.$$

As a permutation of S_8,

$$D_V^{-1}(3) = \begin{pmatrix} 0\,1\,2\,3\,4\,5\,6\,7 \\ 0\,7\,2\,1\,4\,3\,6\,5 \end{pmatrix} = (1753).$$

For $n = 4$, from Table 6, the AFN of D_V^{-1} is as follows

Table 6. Truth Table of D_V^{-1}

x_0	x_1	x_2	x_3	D_V^{-1}	g_0	g_1	g_2	g_3
0	0	0	0		0	0	0	0
1	0	0	0		1	1	1	1
0	1	0	0		0	1	0	1
1	1	0	0		1	0	0	0
0	0	1	0		0	0	1	0
1	0	1	0		1	1	0	1
0	1	1	0		0	1	1	0
1	1	1	0		1	0	1	0
0	0	0	1		0	0	0	1
1	0	0	1		1	1	1	0
0	1	0	1		0	1	0	0
1	1	0	1		1	0	0	1
0	0	1	1		0	0	1	1
1	0	1	1		1	1	0	0
0	1	1	1		0	1	1	1
1	1	1	1		1	0	1	1

$$f_{4,0} = x_0,$$

$$f_{4,1}(x_0, x_1) = x_0 + x_1 = f_{2,1},$$

$$f_{4,2}(x_0, x_1, x_2) = x_0 + x_0x_1 + x_2,$$

$$f_{4,3}(x_0, x_1, x_2, x_3) = x_0 + x_1 + x_1x_2 + x_0x_1x_2 + x_3.$$

As a permutation of S_8,

$$D_V = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 15 & 10 & 1 & 4 & 11 & 6 & 5 & 8 & 7 & 2 & 9 & 12 & 3 & 14 & 13 \end{pmatrix} = (1, 15, 13, 3)(2, 10)(5, 11, 9, 7).$$

Using the similar arguments used for establishing Theorem 3, we can show the following corollary.

Corollary 3. *Let $D_V^{-1}(x)(f_{n,0}, f_{n,1}, \cdots, f_{n,n-1})$ be the inverse of D_V. Then D_V^{-1} is nonlinear for $n > 2$ and*

$$D_V^{-1}(x_0, x_1, \cdots, x_{n-1}) = (f_{1,0}, f_{2,1}, f_{3,2}, f_{4,3}, \cdots, f_{n,n-1})$$

where

$$f_{i,i-1} = f_{i,i-1}(x_0, x_1, \cdots, x_{i-1}), 1 \leq i \leq n.$$

Precisely, for $i = 1, 2, 3,$ and 4, we have

$$f_{1,0}(x_0) = x_0 = g_{1,0},$$

$$f_{2,1}(x_0, x_1) = x_0 + x_1 = g_{2,1},$$

$$f_{3,2}(x_0, x_1, x_2) = x_0 + x_0x_1 + x_2,$$

$$f_{4,3}(x_0, x_1, x_2, x_3) = x_0 + x_1 + x_1x_2 + x_0x_1x_2 + x_3.$$

By this method, for fixed n, we only can construct one pair of nonlinear permutations D_V and D_V^{-1} from the BMA. In order to construct a family of permutations on V in terms of the discrepancy transform, we modify the initial step and the loop step in the BMA. This will be discussed in the next section.

5 A Family of Permutations Derived from A Variation of the BMA

In this section, we first give a variation of the Berlekamp-Massey Algorithm (VBMA). Then we construct a family of permutations of $\mathbb{F}_q$ and give a lower bound for the size of the family of the permutations.

Variation of the Berlekamp-Massey Algorithm (VBMA)

With the same notation as in the BMA. For $0 \leq n_0 < n$ and $0 < v < n$, let

$$R = \{r_{n_0}(x) = x^{n_0+1} + \sum_{i=1}^{n_0} t_i x^i + 1 | t_i \in \mathbb{F}_2\}, \tag{18}$$

and

$$U = \{u_v(x) = x^v + \sum_{i=0}^{v-1} k_i x^i \mid k_i \in \mathbb{F}_2\}. \tag{19}$$

1. Initial Step: Choose one of polynomials in R, say $r_{n_0}(x)$, to generate the sequence $(a_0, a_1, \cdots, a_{n_0}) = (0, 0, \cdots, 0, 1)$.
2. Loop Step. If $d_n = 0$, then we set $f_n = f_{n-1}$. If $d_n = 1$, we select one of polynomials in U, say $u_v(x)$. If $a \geq b$, then $v = a - b$, we construct

$$f_n = f_{n-1} + u_v(x) f_{m-1},$$

If $a < b$, then $v = b - a$, we construct

$$f_n = u_v(x) f_{n-1} + f_{m-1}.$$

Then f_n generates the sequence $a_0, a_1, \cdots, a_n$. Repeat this process till $n = N - 1$.

Theorem 4. *With the notation in the VBMA. Let g be given by*

$$g(a_0, a_1, \cdots, a_{n-1}) = (d_0, d_1, \cdots, d_{n-1}), \tag{20}$$

where $d_i, 0 \leq i < n$ are discrepancy bits computed by the VBMA. If $r_{n_0}(x)$ and $u_v(x)$ used in the VBMA are unchanged for fixed n_0 and $v = a - b$ if $a \geq b$ and $v = b - a$ if $a < b$, then g is a well-defined map from V to V. Moreover, it is a permutation of V. In particular, if we choose that $r(x) = x^{n_0+1} + 1$ and $u(x) = x^v$, then $g(x) = D_V(x)$ which is discussed in the last section.

Proof. If $r_{n_0}(x)$ and $u_v(x)$ in the VBMA are unchanged for each n_0 and v, then a polynomial f_i that generates $a_0, a_1, \cdots, a_i$ is uniquely determined for each $i : 0 \leq i < n$. Note that from formula (6) the discrepancy bit d_i only depends on f_i and a_i linearly. Thus g is well-defined on V. Again using the formula (6), we have

$$(d_0, d_1, \cdots, d_{n-1})^T C = (a_0, a_1, \cdots, a_{n-1})^T$$

where $x = (x_0, x_1, \cdots, x_{n-1})^T$ is the transpose of x and

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots 0 & 0 \\ c_{1,0} & 1 & 0 & 0 & \cdots 0 & 0 \\ c_{2,0} & c_{2,1} & 1 & 0 & \cdots 0 & 0 \\ \vdots & & & & & \\ c_{n-1,0} & c_{n-1,1} & c_{n-1,2} & c_{n-1,3} & \cdots c_{n-1,n-2} & 1 \end{pmatrix}. \tag{21}$$

The entries of ith row of C are the coefficients of f_{i-1} which generates the sequence $a_0, a_1, \cdots, a_{i-1}$. Since $det(C) = 1$, then C is invertible. Therefore f is a permutation of V.

Definition 3. *Let $g(x) = (g_{n,0}, g_{n,1}, \cdots, g_{n,n-1})$ where $x = (x_0, x_1, \cdots, x_{n-1}) \in V$ and*

$$g_{n,i} = g_{n,i}(x_0, x_1, \cdots, x_{n-1})$$

which is constructed in Theorem 4. Then $g(x)$ called a discrepancy permutation *on V, a D-permutation of V for a short.*

Let

$$\Delta(n) = \{\text{ all D-permutations on } V\}.$$

Example 3. $|\Delta(n)| = 1$ for $n = 1, 2$. For $n = 3$, we then have an option to choose $t_{1,j}(x) = x^2 + x + 1$ for $n_0 = 1$, but for U set the only choice is $u(x) = x^v$. Thus we have the following truth table. The algebraic

Table 7. Truth Table of $g(x)$ for $n = 3$

x_0	x_1	x_2	$g(x)$	$g_{3,0}$	$g_{3,1}$	$g_{3,2}$
0	0	0		0	0	0
1	0	0		1	1	0
0	1	0		0	1	1
1	1	0		1	0	1
0	0	1		0	0	1
1	0	1		1	1	1
0	1	1		0	1	0
1	1	1		1	0	0

normal form of $g(x)$,

$$g(x_0, x_1, x_2) = (x_0, x_0 + x_1, x_1 + x_2), (x_0, x_1, x_2) \in \mathbb{F}_2^{(3)}$$

Therefore $|\Delta(3)| = 2$. For $n = 4$, the segment $(0, 1)$ can be generated by the polynomials $r_{1,j}(x) = x^2 + t_1 x + 1, t_1 \in \mathbb{F}_2$ at the initial step of the VBMA where $j = t_1$. The segment $(0, 0, 1)$ can be generated by the polynomials $r_{2,j}(x) = x^3 t_2 x^2 + t_1 x + 1, t_i \in \mathbb{F}_2$ where $j = t_1 + 2t_2$. But $r_{2,0}(x)$ and $r_{2,1}(x)$ map $(0, 0, 1, 0)$ to $(0, 0, 1, 0)$ and $r_{2,2}(x)$ and $r_{2,3}(x)$ map $(0, 0, 1, 0)$ to $(0, 0, 1, 1)$. Thus for the four polynomials $r_{2,j}$ there are only two possible changes for the image of $g(x)$. The possible polynomials in U used for $\mathbb{F}_2^{(4)}$ are $u_{1,0}(x) = x$ and $u_{1,1}(x) = x + 1$. Therefore there are $2^3 = 8$ D-permutations on $\mathbb{F}_2^{(4)}$. I.e., $\Delta(4) = 8$.

Similarly, we have the result in Theorem 3 for D-permutations.

Theorem 5. *Let $g = (g_{n,0}, g_{n,1} \cdot \cdots, g_{n,n-1})$ with $g_{n,i} = g_{n,i}(x_0, x_1, \cdots, x_{n-1})$ be a D-permutation of $\mathbb{F}_2^{(n)}$.*

(a)

$$g_{n,i}(x_0, x_1, \cdots, x_{n-1}) = g_{i+1,i}(x_0, x_1, \cdots, x_i), 0 \leq i < n. \quad (22)$$

Precisely, for $i = 0, 1, 2, 3,$ we have

$$g_{1,0}(x_0) = x_0$$

$$g_{2,1}(x_0, x_1) = x_0 + x_1$$

$$g_{3,2}(x_0, x_1, x_2) \in I_3 = \{x_0 x_1 + x_2, x_1 + x_2\}$$

$$g_{4,3}(x_0, x_1, x_2, x_3) \in I_4$$

where I_4 contains the following 8 Boolean functions.

$$x_1 + x_1x_2 + x_0x_1x_2 + x_3$$
$$x_0x_1 + x_3$$
$$x_1 + x_2 + x_0x_2 + x_3$$
$$x_2 + x_0x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 + x_3$$
$$x_0x_2 + x_3$$
$$x_1 + x_0x_2 + x_1x_2 + x_0x_1x_2 + x_3$$
$$x_2 + x_1x_2 + x_0x_1x_2 + x_3$$
$$x_1 + x_2 + x_0x_1 + x_3$$

(b)

$$g(x) = (x_0, x_0 + x_1, g_{3,2}, g_{4,3}, \cdots, g_{k,k-1}, \cdots, g_{n,n-1}), x \in V \tag{23}$$

where $g_{3,2} \in I_3$ and $g_{4,3} \in I_4$.

(c) For each $2 \leq k \leq n$,

$$g_{k,k-1}(x_0, x_1, \cdots, x_{k-2}, 1) = 1 + g_{k,k-1}(x_0, x_1, \cdots, x_{k-2}, 0) \tag{24}$$

which is equivalent to

$$g_{k,k-1}(x_0, x_1, \cdots, x_{k-1}) = h(x_0, x_1, \cdots, x_{k-2}) + x_{k-1}, \tag{25}$$

where $h(x_0, x_1, \cdots, x_{k-2})$ is a Boolean function in $k-1$ variables $x_0, x_1, \cdots, x_{k-2}$.

(d) Any D-permutation g is nonlinear for $n \geq 4$.

Proof. From the VBMA and similar argument as used for establishing Theorem 3, the formula (22), and the assertions(b) and (c) are true. For the second part of the assertion 1, all the need is to do tedious computation by using the VBMA. According to (a) and (b), any D-permutation $g(x)$ on V can be represented by (23). Since a map from $\mathbb{F}_2^{(n)}$ to $\mathbb{F}_2^{(n)}$ is linear if and only if every component of the map is linear. By the result (a) $g_{n,n-1}(x_0, x_1, \cdots, x_{n-1})$ is nonlinear for $n > 3$ which establishes (d).

In order to investigate a bound of $|\Delta(n)|$, we need the following fact.

Fact 1 *For $g(x)$, a monic polynomial over $\mathbb{F}_2$ of degree t, let*

$$G(g) = \{ \text{ LFSR sequences generated by } g(x)\}.$$

Then

$$|G(g)| = 2^t. \tag{26}$$

(See [4].)

Theorem 6. *The cardinal number of $\Delta(n)$, the set consisting of all D-permutations on V, is bounded by*

$$|\Delta(n)| \geq \begin{cases} 2^{n(n-2)/4} & \text{if } n \text{ even} \\ 2^{(n-1)(n-3))/4} & \text{if } n \text{ odd} \end{cases}.$$

Proof. Let $K = \lfloor \frac{n-1}{2} \rfloor$ where $\lfloor x \rfloor$ is the greatest integer less than x. Let $r_{n_0}(x)$ be a polynomial of degree $n_0 + 1$ in the set R and $u_v(x)$ be a polynomial of degree v in U where R and U are defined by (18) and (19), respectively. For $g(a_0, a_1, \cdots, a_{n-1}) = (d_0, d_1, \cdots, d_{n-1})$, we consider

$$(a_0, a_1, \cdots, a_{n-1}) = (0, \cdots, 0, \overset{n_0}{1}, *, \cdots, *) \tag{27}$$

where $0 < n_0 < K$. There are 2^{n-1-n_0} sequences with the above form. Note that $r_{n_0}(x)$ has degree $n_0 + 1$. If all sequences with the form given by (27) are generated by $r_{n_0}(x)$, from Fact 1, we have

$$|G(r_{n_0})| = 2^{n_0}.$$

Since $0 < n_0 < K$, then $n - 1 - n_0 > n - 1 - K > K$ which is a contradiction. So there exists some $(a_0, a_1, \cdots, a_{n-1})$ with the form of (27) such that it is not generated by $r_{n_0}(x)$. Therefore a choice of $r_{n_0}(x)$ will effect $(d_{n_0+1}, d_{n_0+2}, \cdots, d_{n-1})$. Hence it results in different permutations for different choices of $r_{n_0}(x)$ if $n_0 < K$. So for the initial step, there are $2 \cdot 2^2 \cdots 2^{K-1} = 2^{1+2+\cdots+K-1} = 2^{K(K-1)/2}$ choices for $r_{n_0}(x)$ which will produce different $g(x)$. At the loop step, for $g(a_0, a_1, \cdots, a_{n-1}) = (d_0, d_1, \cdots, d_{n-1})$, we consider

$$(a_0, a_1, \cdots, a_{n-1}) = (1, \cdots, 1, \overset{t}{0}, *, \cdots, *) \tag{28}$$

where $1 < t < K + 1$. For such a sequence $(a_0, a_1, \cdots, a_{n-1})$, its discrepancy sequence $(d_0, d_1, \cdots, d_{n-1})$ has the following form

$$(d_0, d_1, \cdots, d_{n-1}) = (1, 0, \cdots, 0, \overset{t}{1}, *, \cdots, *) \tag{29}$$

Let (f_j, l_j) with $0 \leq j < t$ be LFSR that generates the sequence $(a_0, a_1, \cdots, a_j)$. Let m, a and b be the same as in the VBMA. Note that $l_0 = l_1 = \cdots = l_{t-1} = 1$ and $f_0 = f_1 = \cdots = f_{t-1} = x + 1$. Hence we have

$$a = 0, \text{ and } b = t - l_{t-1} = t - 1.$$

Therefore $v = b - a = t - 1 > 0$ if $t > 1$. By the VBMA,

$$f_t = u_v(x)(x + 1) + 1 \text{ and } l_t = t.$$

Similarly as above, applying Fact 1, there are at most 2^{t-1} sequences in the form (28) that can be generated by f_t. On the other hand, There are 2^{n-1-t} different sequences with the form of (28). Since $n - 1 - t = n - 2 - (t - 1) > n - 2 - (K + 1) = n - 1 - K > K$, then $2^{n-1-t} > 2^K \geq 2^{t-1}$. Therefore there exists at least one sequence in the form of (28) such that it is not generated by f_t. Thus u_v will effect the successive discrepancy computation. So that it will produce different $g(x)$ for different choices of u_v where $0 \leq v < K$. The number of choices for the sequences in the form of (28) is equal to $2 \cdot 2^2 \cdots 2^{K-1} = 2^{K(K-1)/2}$. These sequences correspond to $u_v(x), 0 < v < K$. So there are $2^{K(K-1)/2}$ choices for such $u_v(x)$. Together with the choices of $r_{n_0}(x)$, there are at least $2^{K(K-1)/2}2^{K(K-1)/2} = 2^{K(K-1)}$ different $g(x)$. Therefore

$$|\Delta(n)| \geq 2^{K(K-1)}.$$

By a simple computation for n even or odd, the result follows.

6 A Dynamic Filter Generators Constructed by D-Permutations

In this section, we propose a new type of pseudo-random sequence generators by applying the inverse D-permutations and discuss their cryptographic properties. Let $g(x)$ be a D-permutation on V. By using Theorem 5, we can write $g^{-1}(x)$, the inverse of $g(x)$, as follows

$$g^{-1}(x) = (g_{1,0}^{-1}, g_{2,1}^{-1}, \cdots, g_{n,n-1}^{-1}), x \in V.$$

With the same notation K, R, U in the last section. Let $\Delta_1(n)$ contain the D-permutations in $\Delta(n)$ which are constructed from choosing $r_{n_0}(x) \in R$ and $u_v(x) \in U$ if $0 < n_0, v < K$ and $r_{n_0}(x) = x^{n_0+1} + 1$ and $u_v(x) = x^v$ if $n_0, v \geq K$. According to Theorem 6 we have

$$\Delta_1(n) = 2^{K(K-1)}. \tag{30}$$

***D*-filter Generator**:

- **Input:**

  parameters: one LFSR $(h(x), n)$ which generates an m-sequence $\{d_i\}$ with period $2^n - 1$.

  Key:

  (a) output function $f = g_{n,n-1}^{-1}(x_0, x_1, \cdots, x_{n-1})$, the nth component function of the D-permutation $g^{-1}(x)$ where $g \in \Delta_1(n)$.

  (b) initial state $(d_0, d_1, \cdots, d_{n-1})$ of the LFSR.

  Compute

$$a_i = f(d_i, d_{i+1}, \cdots, d_{i+n-1}), i = 0, 1, \cdots \tag{31}$$

- **Output:** the sequence $a_0, a_1, a_2, \cdots$.

We say the sequence $\underline{\mathbf{a}}$ a *D-filter sequence* and $f = g_{n,n-1}^{-1}$ a *D-filter function.* We also write $\underline{\mathbf{a}} = f(\underline{\mathbf{d}})$.

In the following examples, we take $g(x) = D_V(x)$, the one computed by the BMA instead of by the VBMA.

Example 4. Let $n = 4$ and

$$\underline{\mathbf{d}} = (000100110101111)$$

be an m-sequence of period 15 generated by $h(x) = x^4 + x + 1$. Then a D-filter sequence $\underline{\mathbf{a}}$ is given by

$$\underline{\mathbf{a}} = (101010110011001)$$

This sequence is balanced with period 15 and linear span 10. If $n = 5$ and

$$\underline{\mathbf{d}} = (1000010101110110001111100110100)$$

is an m-sequence of period 31 generated by $h(x) = x^5 + x^2 + 1$. Then a D-filter sequence is as follows

$$\underline{\mathbf{a}} = (1101001110101001001011010011100)$$

which is balanced with period 31 and linear span 30.

Recall that $per(\underline{\mathbf{a}})$ represents period of a sequence $\underline{\mathbf{a}}$. Let $H((a_0, a_1, \cdots, a_t))$ denote the Hamming weight of the sequence $(a_0, a_1, \cdots, a_t)$.

Theorem 7. *Any D-filter sequence is balanced with the maximal period $2^n - 1$. I.e.,*

$$per(\underline{\mathbf{a}}) = 2^n - 1 \text{ and } H(\underline{\mathbf{a}}^{2^n-1}) = 2^{n-1}.$$

A proof of Theorem 7 can be found in [7]. But here we give a simple proof for a completeness. First we need the following results.

Fact 2 *Let $g(x) = (g_0, g_1, \cdots, g_{n-1})$ where $x = (x_0, x_1, \cdots, x_{n-1}) \in V$ be a permutation of V. For each component function g_k with $0 \le k < n$*

$$g_k(x) = c$$

has 2^{n-1} solutions in V for each $c \in \mathbb{F}_2$.

Lemma 4. *Let $\underline{\mathbf{v}} = \{v_i\}$ be a binary sequence and let $N = 2^n - 1$ be a period of $\underline{\mathbf{v}}$. If $H(\underline{\mathbf{v}}^N) = 2^{n-1}$, then N is the least period of $\underline{\mathbf{v}}$. I.e., the sequence has period N.*

Proof. Let $t = per(\underline{\mathbf{v}})$, the period of the sequence $\underline{\mathbf{v}}$. Since N is a period of $\underline{\mathbf{v}}$, then $t|N$. Hence we can write $N = ts$ where t and s are both odd. Let $H(\underline{\mathbf{v}}^t) = w$. Hence $H(\underline{\mathbf{v}}^N) = sw = 2^{n-1}$. But s is odd. This forces that $s = 1$. So that $t = 2^n - 1$.

Proof of Theorem 7. Let

$$S = \{(d_i, d_{i+1}, \cdots, d_{i+n-1}) | 0 \le i < 2^n - 1\} \cup \{(0, 0, \cdots, 0)\}. \tag{32}$$

Since $\underline{\mathbf{d}} = (d_0, d_1, d_2, \cdots,)$ is an m-sequence of period $2^n - 1$, then $S = V$. Note that $g^{-1}(x)$ is a permutation of V from Theorem 4. Applying Fact 1,

$$g_{n,n-1}^{-1}(x_0, x_1, \cdots, x_{n-1}) = 1$$

has 2^{n-1} solutions in V. Hence $H(\underline{\mathbf{a}}^N) = 2^{n-1}$ where $N = 2^n - 1$. Note that N is a period of $\underline{\mathbf{a}}$. Applying Lemma 4, N is the least period of $\underline{\mathbf{a}}$.

In the following, we will investigate a relationship between the polynomial representation of a D-filter function and the trace representation of its D-filter sequence, and the effect of changing LFSRs. Note that $\mathbb{F}_{2^n}$ and $\mathbb{F}_2^{(n)}$ are isomorphic as the linear spaces via

$$(x_0, x_1, \cdots, x_{n-1}) \mapsto x_0\alpha_0 + x_1\alpha_1 + \cdots + x_{n-1}\alpha_{n-1}, x_i \in \mathbb{F}_2. \tag{33}$$

where $\{\alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$ is a basis of $\mathbb{F}_{2^n}$. So we can consider a Boolean function in n variables as a polynomial function $f \in \mathbb{F}_2[x]$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. (See (D) in Section 1.). In the following, we will not distinguish them.

Theorem 8. *Let $f(x)$ be a D-filter function in a polynomial representation and $\underline{\mathbf{a}} = f(\underline{\mathbf{d}})$ be a D-filter sequence. Let $A(x)$ be the trace (or polynomial) representation of the D-filter sequence $\underline{\mathbf{a}}$. Then*

$$A(x) = f(\sigma(x))$$

where $\sigma(x) = \sum_{k=0}^{n-1} c_k x^{2^k}, c_k \in \mathbb{F}_{2^n}$, a linear permutation of $\mathbb{F}_{2^n}$.

Proof. Let $h(x)$ be a primitive polynomial that generates the m-sequence $\underline{\mathbf{d}}$. Let α be a root of $h(x)$ in the extension $\mathbb{F}_{2^n}$ and let $\mathbb{F}_{2^n}$ be defined by $h(x)$. From (4) in Section 1, we have the following trace representation of $\underline{\mathbf{d}} = \{d_i\}$:

$$d_i = Tr_1^n(\beta\alpha^i), \beta \in \mathbb{F}_{2^n}, i = 0, 1, \cdots, 0 \neq \beta \in \mathbb{F}_{2^n}. \tag{34}$$

From the definition of the D-filter sequence, we have

$$a_i = f(d_i, d_{i+1}, \cdots, d_{i+n-1}), i = 0, 1, \cdots. \tag{35}$$

Note that S, defined by (32), the set of all states of the LFSR with $h(x)$, is isomorphic to $\mathbb{F}_{2^n}$ as the finite fields via

$$\alpha^i \longrightarrow (d_i, d_{i+1}, \cdots, d_{i+n-1}), 0 \le i < 2^n - 1, 0 \longrightarrow 0. \tag{36}$$

Let $\{\eta_0, \eta_1, \cdots, \eta_{n-1}\}$ be the dual basis of $\{1, \alpha, \cdots, \alpha^{n-1}\}$. For $x \in \mathbb{F}_{2^n}$, therefore, we have $x = \sum_j x_j\alpha^j, x_j = Tr_1^n(\eta_j x) \in \mathbb{F}_2$. Together with the isomorphism (33) and (36) with setting $x = \alpha^i$, it follows that

$$x = (Tr_1^n(\eta_0 x), Tr_1^n(\eta_1 x), \cdots, Tr_1^n(\eta_{n-1}x)) \mapsto y = (Tr_1^n(\beta x), Tr_1^n(\beta\alpha x), \cdots, Tr_1^n(\beta\alpha^{n-1}x)). \tag{37}$$

Let C be the linear transform from the basis $\{\eta_j\}$ to the basis $\{\alpha^j\}$. I.e.,

$$(1, \alpha, \cdots, \alpha^{n-1})^T = C(\eta_0, \eta_1, \cdots, \eta_{n-1})^T. \tag{38}$$

From (37), it follows that $y^T = Cx^T$. Let σ be the polynomial form of C, then $\sigma = \sum_j c_j x^j, c_j \in \mathbb{F}_{2^n}$. Therefore

$$a_i = f(d_i, d_{i+1}, \cdots, d_{i+n-1}) = f(\sigma(\alpha^i)), i = 0, 1, \cdots.$$

On the other hand, we have $a_i = A(\alpha^i)$. Thus $A(x) = f(\sigma(x))$.

Remark 1. According to (5) in Section 1, linear span of the D-filter sequence $\underline{\mathbf{a}}$ is equal to the number of nonzero coefficients in $A(x)$. Theorem 8 shows that $A(x)$ can also be computed in terms of a composition of the polynomial representation of the D-filter function and the linear transformation from the basis $\{\eta_0, \eta_1, \cdots, \eta_{n-1})$ to the basis $\{1, \alpha, \cdots, \alpha^{n-1}\}$ where the former is the dual basis of the latter.

Corollary 4. *Let f be a D-filter function. Let $\underline{\mathbf{d}} = \{d_i\}$ and $\underline{\mathbf{e}} = \{e_i\}$ be two m-sequences generated by different primitive polynomials. Let $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ be two D-filter sequences with $\underline{\mathbf{a}} = f(\underline{\mathbf{d}})$ and $\underline{\mathbf{b}} = f(\underline{\mathbf{e}})$ respectively. Let $A(x)$ and $B(x)$ be the trace representations of $\underline{\mathbf{a}}$ and $\underline{\mathbf{b}}$ respectively. Then*

$$B(x) = A(\tau(x))$$

where $\tau(x) = \sum_{i=0}^{n-1} k_i x^{2^i}, k_i \in \mathbb{F}_{2^n}$, a linear permutation of $\mathbb{F}_{2^n}$.

Proof. Let $h(x)$ and $k(x)$ be two primitive polynomials that generate $\underline{\mathbf{d}}$ and $\underline{\mathbf{e}}$, respectively. Let α and β be the root of $h(x)$ and $k(x)$ in the extension $\mathbb{F}_{2^n}$, respectively. Let

$$\tau : (1, \beta, \cdots, \beta^{n-1}) \longrightarrow (1, \alpha, \cdots, \alpha^{n-1}) \tag{39}$$

be the linear transform from the basis $\{\beta_j, 0 \le j < n\}$ to the basis $\{\alpha^j, 0 \le j < n\}$. Thus τ is a linear permutation of $\mathbb{F}_{2^n}$. From Theorem 8, $b_i = f(\sigma(\beta^i)), i = 0, 1, \cdots$. Thus $b_i = f(\sigma(\tau(\alpha^i))), i = 0, 1, \cdots$. Applying Theorem 8 again, we get $B(x) = f(\sigma(y)) = A(y) = A(\tau(x))$ where $y = x^r$ with $\beta = \alpha^r$.

Remark 2. Note that the results in Theorem 8 and Corollary 4 are true for any Boolean function f. It is worth to point it out that Corollary 4 shows an important fact. I.e., the effect of a change of the LFSR in a filter generator is equivalent to do a linear transformation to the stage positions of the original LFSR.

Remark 3. For a D-filter generator, a D-filter function f, which is the nth component function of a D-permutation in $\Delta_1(n)$, is a Boolean functions in n variables. It can be written as $f(x_0, x_1, \cdots, x_{n-1}) = h(x_0, x_1, \cdots, x_{n-2}) + x_{n-1}$ (Theorem 4). According to the results in [12] or [21], any D-filter sequence may achieve the maximal linear span $2^n - 2$ (see the experimental results below). Experimental results also shown that all such f have the maximal order, i.e., the product term $x_0 x_1 \cdots x_{n-2}$ will appear in h.

For fixed D-filter function f, let

$$D(f) = \{f(\underline{\mathbf{d}}) | \underline{\mathbf{d}} \text{ all m-sequences } \}.$$

According to Corollary 4, we can write

$$D(f) = \{f(\mu(\underline{\mathbf{d}})) | \mu = \sigma\tau, \text{ all } \tau \text{ defined by (39) } \}.$$

Note that all D-filter sequences in $D(f)$ are shift-distinct. Since there are $\phi(2^n - 1)/n$ different primitive polynomials of degree n over $\mathbb{F}_2$, so there are $\phi(2^n - 1)/n$ shift distinct D-filter sequences with D-filter function f. Thus $D(f) = \phi(2^n - 1)/n$. The experimental results show that most of shift-distinct D-filter sequences in $D(f)$ achieve the maximal linear span $2^n - 2$ for each f and a few of them have the linear spans taken at the slightly smaller value $2^n - 2 - (2n + m)$ where $m|n$ or $m = 0$. In the following table, we take f the nth component function of D_V, the one computed by the BMA (i.e., it is computed by choosing $r_{n_0} = x^{n_0+1} + 1 \in R$ and $u_v = x^v \in U$.) We list the experimental results for the linear span property of the sequences in $D(f)$ for $4 \leq n \leq 13$. In the table, we put

- $p = 2^n - 1$, the period of D-filter sequences.
- $S(n) = \phi(2^n - 1)/n$, the number of shift-distinct D-filter sequences in $D(f)$.
- $\{\tau_i\}$, a set of possible values of the linear spans of the D-filter sequences in $D(f)$.
- $T(\tau_i)$, the number of shift-distinct D-filter sequences in $D(f)$ with the linear span τ_i. $\{T(\tau_i)\}$ corresponds to $\{\tau_i\}$. Note that $\sum_i T(\tau_i) = S(n)$.

Table 8. Distribution of Linear Spans of $\Delta(f)$ for $4 \leq n \leq 13$

n	p	$S(n)$	$\{\tau_i\}$	$\{T(\tau_i)\}$
4	15	2	14, 10	1, 1
5	31	6	30	6
6	63	6	62, 60, 51, 50	3, 1, 1, 1
7	127	18	126, 119, 112	15, 2, 1
8	255	16	254, 252, 250, 246, 240	8, 3, 2, 2, 1
9	511	48	510, 507, 501, 492	34, 12, 1, 1
10	1023	60	1022, 1020, 1017, 1015, 1012, 1000	32, 15, 6, 2, 2, 1
11	2047	176	2046, 2035	160, 16
12	4095	144	4094, 4092, 4091, 4090, 4089, 4088 4087, 4086, 4085, 4084, 4083, 4082 4081, 4078, 4070	57, 17, 22, 13, 1, 12 5, 2, 3, 1, 2, 6 1, 1, 1
13	8191	630	8190	630

7 Further Security Analysis and Implementation of D-Filter Generators

1. *Dynamic property:*

The D-filter generator is dynamic. The filter functions can be easily changed at each communication section. Usually, in order to enfance security of a filter generator, a common method in practical systems is to add a linear transformation between an LFSR and a filter function due to the fact that it is difficult to find a large number of good filter functions. In detail, let us look at Corollary 4. We have $\underline{\mathbf{e}} = f(\mu(\underline{\mathbf{d}}))$ where $\mu = \sigma \circ \tau$ is a linear permutation of $\mathbb{F}_{2^n}$ and τ is obtained from a change of the LFSR. However, one can use any of linear permutations to replace τ. In other words, one can consider $f \circ \mu$ as a new filter function in the filter generator. In this way, the filter functions can be different for each communication section. But the dynamic property of the D-filter generators is completely different, because it is achieved by using a set of nonlinear functions in $\Delta_1(n)$. Obviously, each D-filter function also can be combined with a linear transformation of $\mathbb{F}_{2^n}$ as usual.

2. The key size is $(2^n - 1)|\Delta_1(n)| = (2n-1)2^{K(K-1)}$ where $K = \lfloor (n-1)/2 \rfloor$.

3. The security of the D-filter generator only depends on the difficulty of finding the initial state of the LFSR that generates an m-sequence $\underline{\mathbf{d}}$ when we suppose that the attacker already got the information on the D-filter function. Since a D-filter sequence is obtained by taking bits from the nth component in the permutation $g^{-1}(d_i, d_{i+1}, \cdots, d_{i+n-1})$, even an attacker can get s consecutive bits of a D-filter sequence with $0 < s < t$ (t should be less than the length of streams used in each communication section), it is no better than exhausting search for the initial state, which needs $2^n - 1$ trials.

4. We tested the unconditional randomness of D-filter sequences including statistic tests, correlation tests and linear span related tests. Note that $\Delta_1 = 2$ for $n = 5$ and $n = 6$, $\Delta_1 = 6$ for $n = 7, 8$, $\Delta_1 = 12$ for $n = 9, 10$ and $\Delta_1 = 20$ for $n = 11, 12$. We tested all of these short sequences and they passed the tests.

A strategy for implementing it in hardware is that put two extra buffers to hold random bits for R set and U set. The following figure shown this approach. In Fig.1, each of the labeled R-register and U-register holds $K(K-1)$ bits. For each $t = 1, 2, \cdots K-1$, the initial step or the loop block reads t bits from the R-register or U-register starting from the $1 + 2 + \cdots + t - 1 = t(t-1)/2$th point to form a r_t polynomial or a u_t polynomial. At each communication section, one can reload an initial state of the LFSR and both the R-register and the U-register or only reload an initial state of the LFSR and keep both the R-register and the U-register unchanged or keep one of these register unchanged. This is how dynamic behavior of the D-filter generator works.

The number of bit operations for applying the VBMA to compute linear span of a sequence $d_0, d_1, \cdots, d_{n-1}$ is determined by the matrix of (21). So it is bounded by $O(n^3)$. Therefore the number of bit operations for output of one bit is bounded by $O(n^3)$. Thus D-filter generators can be efficiently implemented in both hardware and software.

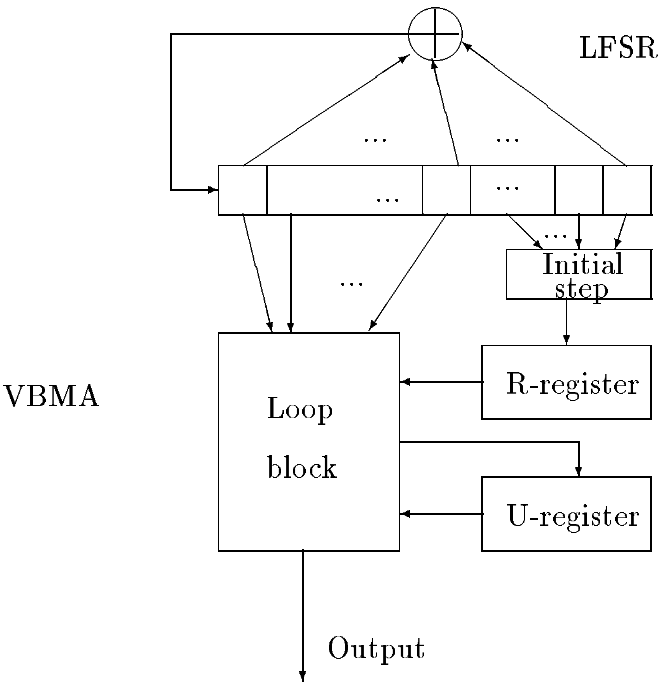

Fig. 1 Implementation Architecture of D-Filter Generator

8 Conclusion

The discrepancy transform, a new transform of ultimately periodic sequences, is developed. A characteristic of linear span profiles is obtained be means of the discrepancy transform sequences. A restriction of the discrepancy transform, computed by the variance of the Berlekamp-Messay algorithm, derives a family of a new type of nonlinear permutations of $GF(2^n)$, called *D-permutations*. A lower bound for the number of D-permutations is given. Applying the nth component function of a D-permutation to a filter generator yields a dynamic filter generator, called a D-filter generator. It is shown that D-filter generators have strong cryptographic property; thus, they have important applications in stream cipher cryptosystems and secure communication systems.

ACKNOWLEDGEMENT

The author would like to acknowledge useful discussions with Doug Stinson and Alfred Menezes.

References

1. E.R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.
2. N.G. de Bruijn, A combinatorial problem, *Kononklijke Nederlands Akademi van Wetenchappen, Proc.,* vol. 49, Pr. 2, 1946, pp. 758-764.

3. 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.
4. S.W. Golomb, *Shift Register Sequences*, Revised Edition, Aegean Park Press, 1982, pp. 25.
5. 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. A English translation of the main results in the dissatation will appear soon at the website of the Center for Applied Cryptographic Research, University of Waterloo, http://www.cacr.math.uwaterloo.ca.
6. G. Gong, *Sequence Analysis*, Lecture Notes, Chapter 6, University of Waterloo, http://www.cacr.math.uwaterloo.ca/ ggong/CO739x/739xcover.html, 1999.
7. G. Gong, On $q-$ary cascaded GMW sequences, *IEEE Trans. on Inform. Theory*, vol. 42, No. 1, January 1996, pp. 263-267, Proposition 2.
8. G. Gong, T. Berson and D. Stinson, Elliptic curve pseudo-random sequence generators, *Proceedings of the Sixth Annual Workshop on Selected Area in Cryptography*, August 9-10, 1999, Kingston, Canada.
9. G. Gong and S.W. Golomb, Binary Sequences with Two-Level Autocorrelation, *IEEE Trans. on Inform. Theory*, vol. 45, No.2, March 1999, pp.692-693.
10. Tor 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.
11. N. Jacobson, *Basic Algebra I*, W.H. Freeman and Company, San Francisco, 1974, pp. 116-118.
12. 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.
13. H. Niederreiter, Keystream sequences with a good linear complexity profile for every starting point, *Advances in Cryptology-EUROCRYPT'89*, Lecture Notes in Computer Science, vol. 434, Springer-Verlag, Berlin, 1990, pp. 523-532.
14. H. Niederreiter, Some computable complexity measures for binary sequences, *Sequences and their Application, Proceedings of of SETA'98, Discrete Mathematics and Theoretical Computer Science*, Springer-Verlag, Berlin, 1999, pp.67-78.
15. H. Niederreiter and M. Vielhaber, Simultaneous shifted continued fraction expansions in quadratic time, *Applicable Algebra Engrg. Comm. Comput.* **9** (1998), pp. 125-138.
16. R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Volume 20, Addison-Wesley, 1983.
17. J.L. Massey, Shift-register synthesis and BCH decoding, *IEEE Trans. on Inform. Theory* vol. IT-15, January 1969.
18. 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.
19. W. Meier and O. Staffelbach, The self-shrinking generator, *Advances in Cryptology-EUROCRYPT'94*, Lecture Notes in Computer Science, vol. 950, Springer-Verlag, Berlin, 1995, pp. 205-214.
20. F. Paper, Stream cipers, *Electrotechnik und Maschinenbau* **104** (1987), pp. 564-568.
21. R.A. Rueppel, *Analysis and Design of Stream Ciphers*, Springe-Verlag, 1986, pp.53.
22. L.R. Welch and R.A. Scholtz, Continued fractions and Berlekamp's algorithm, *IEEE Trans. Inform. Theory*, vol. IT-25, 1979, pp. 19-27.