On Cryptographic Applications of Matrices Acting on Finite Commutative Groups and Rings

S. M. Dehnavi[1], A. Mahmoodi Rishakani[2], M. R. Mirzaee Shamsabad[3]

[1]Faculty of Mathematical and Computer Sciences, Kharazmi University, Tehran, Iran
std_dehnavism@khu.ac.ir

[2]Faculty of Sciences, Shahid Rajaee Teacher Training University, Tehran, Iran
am.rishakani@srttu.edu

[3]Faculty of Mathematics and Computer Science, Shahid Bahonar University, Kerman, Iran
mohammadmirzaeesh@yahoo.com

Abstract: In this paper, we investigate matrices acting on finite commutative groups and rings. In fact, we study modules on ring of matrices over Z_N and also modules over the ring $(F_2^t, \oplus, \wedge)$; these new algebraic constructions are a generalization of some of the constructions which were previously presented by the authors of this paper. We present new linearized and nonlinear MDS diffusion layers, based on this mathematical investigation. Also, we study some types of nonlinear number generators over Z_{2^n} and we present a lower bound on the period of these new nonlinear number generators. As a consequence, we present nonlinear recurrent sequences over Z_{2^n} with periods which are multiples of the period of the corresponding sigma-LFSR's.

Keywords: Symmetric Cryptography, MDS Diffusion Layer, Group, Ring, Sigma-LFSR, Number Generator

1. Introduction

In this paper, we examine matrices acting on finite commutative groups and rings. We study modules on ring of matrices over Z_N and modules over the ring $(F_2^t, \oplus, \wedge)$. We show that these new algebraic constructions are a generalization of some of the constructions that are given in [1]. Based upon this mathematical investigation, we present new linearized and nonlinear MDS diffusion layers. MDS diffusion layers are used in symmetric ciphers [2-7] and they are studied in [1,8-14]. In [1], we presented new families of linear, linearized and nonlinear diffusion layers. We showed that these diffusion layers can be made randomized with a low implementation cost; moreover, we constructed nonlinear MDS maps of large sizes which are efficiently implemented in modern processors. In this paper, we generalize some of the concepts that have been presented in symmetric cryptographic literature, up to now.

Then, we study nonlinear number generators over the ring Z_{2^n} and we present a lower bound on the period of these nonlinear generators. As a result, we present nonlinear recurrent sequences over Z_{2^n} with periods which are multiples of the period of the corresponding sigma-LFSR's.

In Section 2, we present preliminary notations and definitions. Section 3 is devoted to construction of new MDS diffusion layers; in Section 4 we investigate nonlinear number generators and Section 5 is the conclusion.

2. Preliminary Notations and Definitions

In this paper, the number of elements or cardinality of a finite set A is denoted by $|A|$ and the Cartesian product of n copies of A is denoted by A^n. We use the symbol $\equiv$ for the natural isomorphism between algebraic structures and also for the equivalence of vectors. We denote the finite field with two elements by F_2. Any zero vector or matrix is denoted by **0,** the all-one vector by **1** and every identity matrix by I. We denote the ring of integers modulo N by Z_N.

Let S be a finite set with a distinguished element 0, and k, m and n be natural numbers such that $n = km$. Suppose that $x \in S^n$; the weight of x with respect to m-tuples is the number of nonzero m-tuples of x. More precisely, if

$$x = (x_1, \dots, x_1, x_k)^T$$

$$\equiv (x_{1,1}, \dots, x_{1,m}; x_{2,1}, \dots, x_{2,m}; \dots; x_{k,1}, \dots, x_{k,m})^T,$$

then we have,

$$w_m(x) = |\{1 \le i \le k | x_i \ne \mathbf{0}\}|.$$

Let S be a finite set and suppose that $f: S^k \to S^k$ is a map. The map f is called MDS iff for any two different vectors $X, Y \in S^k$, the vectors $\big(X, f(X)\big)$ and $\big(Y, f(Y)\big)$ in S^{2k} are different in at least $k+1$ coordinates. It's not hard to see that we can construct a $(2k, |S|^k, k+1)$-code over S with the help of f, which obviously is MDS.

We denote the set (ring) of all $n \times n$ matrices with entries in a finite commutative ring with identity R by $\mathcal{M}_n(R)$ and the set of all $n \times n$ binary matrices by $\mathcal{B}_n$. Suppose that n, k and m are natural numbers, R is a finite commutative ring with identity, $n = km$ and $A \in \mathcal{M}_n(R)$. We can represent A (as a block-wise matrix) by

$$A = [A_{i,j}]_{k \times k}, \ A_{i,j} \in \mathcal{M}_m(R), \quad 1 \le i, j \le k. \tag{1}$$

Let $f: F_2^n \to F_2^n$ be a function with $n = km$. The *differential branch number* of f with respect to *m*-bit words is defined as

$$\min_{\substack{x,y \in \mathbb{F}_2^n \\ x \ne y}} \{w_m(x \oplus y) + w_m(f(x) \oplus f(y))\},$$

and the *linear branch number* of f with respect to *m*-bit words is defined as

$$\min_{\substack{\alpha,\beta \in \mathbb{F}_2^n \\ P(\alpha.x \oplus \beta.f(x)=0) \ne \frac{1}{2} \\ (\alpha,\beta) \ne (0,0)}} \{w_m(\alpha) + w_m(\beta)\}.$$

Here, $\oplus$ is the XOR operation and . is the dot product in F_2^n. The probability $P(\alpha . x \oplus \beta . f(x) = 0) \ne \frac{1}{2}$ is equivalent to

$$|\{\, x \in \mathbb{F}_2^n | \alpha . x \oplus \beta . f(x) = 0\}| \ne 2^{n-1}.$$

A function $f: F_2^n \to F_2^n$ is called *linearized* iff, for all $x, y \epsilon F_2^n$, we have,

$$f(x \oplus y) = f(x) \oplus f(y).$$

It is not hard to see that for a linearized function *f*, the differential branch number of *f* with respect to *m*-bit words is equal to

$$\min_{\substack{x \in \mathbb{F}_2^n \\ x \neq 0}} \{w_m(x) + w_m(M_f x)\},$$

and the linear branch number of f with respect to m-bit words is equal to

$$\min_{\substack{x \in \mathbb{F}_2^n \\ x \neq 0}} \{w_m(x) + w_m(M_f^T x)\};$$

where, M_f is the (bit-wise) matrix corresponding to f.

Let $f: F_2^n \to F_2^n$, with $n = km$. The function f (or the corresponding matrix of f, if it is linearized) is called MDS with respect to m-bit words iff the differential and the linear branch numbers of f are equal to $k+1$. It can be easily seen that MDS functions in this sense are special cases of MDS functions with respect to the aforementioned general definition on a finite set S.

For a commutative ring R with identity, the determinant of A in R is denoted by $d_R(A)$ and the (multiplicative) order of an element $r \in R$ is denoted by $o(r)$, if it exists. We denote the XOR operation by $\oplus$, the AND operation by $\wedge$, the right cyclic shift or rotation operation by $>>>$ and the right shift operation by $\gg$. The gcd of two natural numbers a and b is denoted by (a, b).

Let G be a finite (additive) commutative group of order N. We know that G^n is a finite commutative group of order N^n such that the order of every element in G^n divides N. We can construct a (left) $\mathcal{M}_n(Z_N)$-module with the scalar product (acting on G^n) as

$$A.X = (g'_1, \dots, g'_n)^T,$$

where,

$$A = [a_{i,j}] \in \mathcal{M}_n(Z_N), \quad X = (g_1, \dots, g_n)^T \in G^n,$$

and,

$$g'_i = a_{i,1}g_1 + \cdots + a_{i,n}g_n, \qquad 1 \leq i \leq n.$$

3. Construction of New MDS Diffusion Layers

In this section, we present new MDS maps over finite commutative groups and rings. In the proof of the following lemma, we use some concepts from [15, Chap. 13-14].

Lemma 3.1: Suppose that G is a finite (additive) commutative group of order N (with identity 0) and $A \in \mathcal{M}_n(Z_N)$ with $\left(d_{Z_N}(A), N\right) = 1$. Then, the map

$$f: G^n \to G^n,$$

$$f(X) = A.X,$$

is a bijection.

Proof: Suppose that the statement does not hold. Then, there are two distinct vectors X_1 and X_2 with $A.X_1 = A.X_2$; or equivalently, there is a nonzero vector

$$X = X_1 - X_2 = (g_1, \dots, g_n)^T$$

with $A.X = \mathbf{0}$. We know that there exists a matrix A' with $AA' = A'A = I$. Multiplying the two sides of $A.X = \mathbf{0}$ by A', we have $I.X = 0$; which means that $g_i = 0$, $1 \leq i \leq n$. This is a contradiction. ■

Theorem 3.2: Suppose that $n = mk$, G is a finite (additive) commutative group of order N and $A \in \mathcal{M}_n(Z_N)$ is a block-wise matrix with regard to representation (1). Suppose that each block-wise square submatrix of A is nonsingular as a matrix over Z_N. Then, A, acting on G^m, defines an MDS map.

Proof: Similar to the proof of [1, The. 3.1] and regarding Lemma 3.1, the theorem is proved. ■

Corollary 3.3: Suppose that t is given, $n = mk$ and $M = [\mathfrak{m}_{i,j}] \in \mathcal{B}_n$ is an MDS matrix with respect to m-bit words; then the following map is a linearized MDS map with respect to mt-bit words:

$$f: F_2^{nt} \equiv (F_2^t)^{km} \to F_2^{nt} \equiv (F_2^t)^{km},$$

$$f(X_1, \dots, X_k) = (Y_1, \dots, Y_k),$$

with $X_i = (X_{i,1}, \dots, X_{i,m})$ and $Y_i = (Y_{i,1}, \dots, Y_{i,m})$, $1 \leq i \leq k$, and,

$$Y_{i,j} = \bigoplus_{\substack{\mathfrak{m}_{(i-1)m+j,s} = 1 \\ 1 \le s \le n}} \left(X_{\left[\frac{s-1}{m}\right]+1,1+((s-1) \ mod \ m)} \right), \qquad 1 \le i \le k, \qquad 1 \le j \le m.$$

We note that $X_{i,j}, Y_{i,j} \in F_2^t$, for $1 \le i \le k, 1 \le j \le m$.

Proof: In Theorem 3.2, put $G \equiv (F_2^t, \oplus)$. ■

We note that Theorem 5.2 of [1] is somehow a special case of Theorem 3.2 with $G \equiv (Z_{2^t}, +)$.

Corollary 3.4: Suppose that $n = mk$ with $m > 1$ and $M = [\mathfrak{m}_{i,j}] \in \mathcal{B}_n$ be an MDS matrix with respect to m-bit words; then the following map is a nonlinear MDS map with respect to mt-bit words:

$$f: F_2^{nt} \equiv (F_2^t)^{km} \to F_2^{nt} \equiv (F_2^t)^{km},$$

$$f(X_1, \dots, X_k) = (Y_1, \dots, Y_k),$$

with $X_i = (X_{i,1}, \dots, X_{i,m})$ and $Y_i = (Y_{i,1}, \dots, Y_{i,m})$, $1 \le i \le k$, and,

$$Y_{i,j} = \left(\prod_{\substack{\mathfrak{m}_{(i-1)m+j,s}=1 \\ 1 \le s \le n}} \left(2X_{\left[\frac{s-1}{m}\right]+1,1+((s-1) \ mod \ m)} + 1 \right) \ mod \ 2^{t+1} \right) \gg 1,$$

$$1 \le i \le k, \ \ 1 \le j \le m.$$

Proof: We know that the odd elements of $Z_{2^{t+1}}$ construct a (*multiplicative*) commutative group of order 2^t. According to Theorem 3.1, the map f (without the right shift) is MDS with respect to $m(t+1)$-bit words. On the other hand, we know that the least significant bits of all the inputs and outputs of f (without the right shift) are one. So, after deleting these *one* bits, the resulting map would be an MDS map with respect to mt-bit words. ■

Example: It is not hard to see that the following matrix is MDS with respect to 2-bit words; equivalently, its linear and differential branch numbers are 3, with respect to 2-bit words:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}. \tag{2}$$

Consider the function

$$f: F_2^{16} \equiv (F_2^4)^4 \to F_2^{16} \equiv (F_2^4)^4,$$

$$f(X_1, X_0) = (Y_1, Y_0),$$

where,

$$Y_1 = (Y_1^H, Y_1^L), \quad Y_0 = (Y_0^H, Y_0^L), \quad X_1 = (X_1^H, X_1^L), \quad X_0 = (X_0^H, X_0^L),$$

with

$$Y_1^H = \left((2X_1^H + 1)(2X_0^H + 1)(2X_0^L + 1) \;\; mod \;\; 2^5\right) \gg 1,$$

$$Y_1^L = \left((2X_1^L + 1)(2X_0^L + 1) \;\; mod \;\; 2^5\right) \gg 1,$$

$$Y_0^H = \left((2X_1^H + 1)(2X_0^H + 1) \;\; mod \;\; 2^5\right) \gg 1,$$

$$Y_0^L = \left((2X_1^H + 1)(2X_1^L + 1)(2X_0^L + 1) \;\; mod \;\; 2^5\right) \gg 1.$$

According to Theorem 3.1, f is MDS with respect to 8-bit words.

Theorem 3.5: Suppose that $n = mk$, $M_i = \left[\mathfrak{m}_{r,s}^i\right] \in \mathcal{B}_n$, $1 \le i \le t$, are t MDS matrices with respect to m-bit words and $A = \left[a_{r,s}\right] \in \mathcal{M}_n(F_2^t) \equiv \mathcal{B}_{nt}$ with

$$a_{r,s} = (\mathfrak{m}_{r,s}^1, \dots, \mathfrak{m}_{r,s}^t), \quad 1 \le r, s \le n.$$

Then, A is an MDS matrix with respect to mt-bit words.

Proof: According to [1, The. 3.1], let R be the ring $(F_2^t, \oplus, \wedge)$. Since the operations of XOR and AND are parallel bitwise operations, so the MDSness of A, or equivalently, nonsingularity of each block-wise square submatrix of A, which is equivalent to the fact that the determinant of every block-wise square submatrix of A is equal to **1**, is a direct result of the MDSness of M_i's, $1 \leq i \leq t$: we note that in $(F_2^t, \oplus, \wedge)$, the only invertible element is **1**. ■

Example: It can be verified that the linear and differential branch numbers of the following matrices are 3, with respect to 2-bit words:

$$\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}.$$

So, the following matrix is MDS over the ring $(F_2^2, \oplus, \wedge)$; or, this matrix is MDS with respect to 4-bit words:

$$\begin{pmatrix} 11 & 00 & 11 & 10 \\ 00 & 11 & 00 & 11 \\ 11 & 00 & 10 & 01 \\ 10 & 11 & 01 & 11 \end{pmatrix} \equiv \begin{pmatrix} 3 & 0 & 3 & 2 \\ 0 & 3 & 0 & 3 \\ 3 & 0 & 2 & 1 \\ 2 & 3 & 1 & 3 \end{pmatrix}. \qquad (3)$$

The defining equations for the function f, corresponding to the matrix (3), is

$$f: F_2^8 \equiv (F_2^2)^4 \to F_2^8 \equiv (F_2^2)^4,$$

$$f(X_1, X_0) = (Y_1, Y_0),$$

where,

$$Y_1 = (Y_1^H, Y_1^L), \quad Y_0 = (Y_0^H, Y_0^L), \quad X_1 = (X_1^H, X_1^L), \quad X_0 = (X_0^H, X_0^L),$$

with

$$Y_1^H = (3 \wedge X_1^H) \oplus (3 \wedge X_0^H) \oplus (2 \wedge X_0^L) = X_1^H \oplus X_0^H \oplus (2 \wedge X_0^L),$$

$$Y_1^L = (3 \wedge X_1^L) \oplus (3 \wedge X_0^L) = X_1^L \oplus X_0^L,$$

$$Y_0^H = (3 \wedge X_1^H) \oplus (2 \wedge X_0^H) \oplus (1 \wedge X_0^L) = X_1^H \oplus (2 \wedge X_0^H) \oplus (1 \wedge X_0^L),$$

$$Y_0^L = (2 \wedge X_1^H) \oplus (3 \wedge X_1^L) \oplus (1 \wedge X_0^H) \oplus (3 \wedge X_0^L) = (2 \wedge X_1^H) \oplus X_1^L \oplus (1 \wedge X_0^H) \oplus X_0^L.$$

Corollary 3.6: Suppose that $n = mk$, $M = [\mathfrak{m}_{i,j}] \in \mathcal{B}_n$ is an MDS matrix with respect to m-bit words and $A = [a_{r,s}] \in \mathcal{M}_n(F_2^t) \equiv \mathcal{B}_{nt}$ with

$$a_{r,s} = (\mathfrak{m}_{r,s}, \dots, \mathfrak{m}_{r,s}), \quad 1 \le r, s \le n.$$

Then A is an MDS matrix with respect to mt-bit words.

We note that Corollary 3.6 is somehow equivalent to Corollary 3.3.

Lemma 3.7: Let r be an odd number, A_i's, $1 \le i \le r$, be r pairwise commutable matrices in $\mathcal{B}_n$ such that the order of all A_i's, $1 \le i \le r$, are nonnegative powers of two. Then, $A = A_1 \oplus \dots \oplus A_r$ is invertible in $\mathcal{B}_n$.

Proof: Since the order of all A_i's, $1 \le i \le r$, are nonnegative powers of two, we suppose that the maximum of these orders is 2^s. Now, from the pairwise commutability of A_i's, we have,

$$(A_1 \oplus \dots \oplus A_r)^{2^s} = (A_1)^{2^s} \oplus \dots \oplus (A_r)^{2^s} = I \oplus \dots \oplus I = I.$$

And this ends the proof. ∎

Theorem 3.8: Suppose that $n = mk$, $M = [\mathfrak{m}_{i,j}] \in \mathcal{B}_n$ is an MDS matrix with respect to m-bit words, the number of nonzero entries of M is r and $A_i \in \mathcal{B}_n$, $1 \le i \le r$. If the order of all A_i's, $1 \le i \le r$, are nonnegative powers of two and A_i's, $1 \le i \le r$, are pairwise commutable, then the matrix $\mathcal{M} = [m_{i,j}] \in \mathcal{B}_{nt}$ with

$$m_{i,j} = \begin{cases} A_{f(i,j)} & \mathfrak{m}_{i,j} = 1, \\ \mathbf{0} & \mathfrak{m}_{i,j} = 0, \end{cases}$$

is MDS with respect to mt-bit words. Here, f is an arbitrary map from the set of indices (i, j) with $\mathfrak{m}_{i,j} = 1$ to $\{1, \dots, r\}$.

Proof: Since each block-wise submatrix of M is nonsingular, so the determinant of every block-wise submatrix of $\mathcal{M}$ is equal to XOR of an odd number of matrices, each of which is a product of matrices of order 2^{d_w}, for some d_w's. Since the product of any number of commutating matrices of order 2^{d_w}, for some d_w's, is a matrix of order 2^d, for some d, so, using Lemma 3.7, the theorem is proved. ∎

We note that in Theorem 3.8, A_i's can be the XOR of an odd number of (distinct) arbitrary nonnegative powers of a matrix A of order 2^d, for some d.

Example: We know that (2) is a matrix in $\mathcal{B}_4$ with linear and differential branch numbers 3 with respect to 2-bit words. Let $t = 8$ and $A_f \in \mathcal{B}_8$ be the corresponding matrix of the linearized function

$$f: F_2^8 \to F_2^8,$$

$$f(x) = x \oplus (x \gg 5);$$

then,

$$\begin{pmatrix} I & 0 & I & A_f \\ 0 & A_f & 0 & I \\ I & 0 & A_f & 0 \\ I & I & 0 & A_f \end{pmatrix},$$

is a matrix in $\mathcal{B}_{32}$ with linear and differential branch numbers 3, with respect to 16-bit words: we note that $A_f^2 = I$.

Corollary 3.9: Suppose that t is given, $n = mk$, $M = [\mathfrak{m}_{i,j}] \in \mathcal{B}_n$ be an MDS matrix with respect to m-bit words, the number of nonzero entries in M is r and z_s's, $1 \le s \le r$, be r arbitrary nonnegative numbers less than 2^t; then the following map is a linearized MDS map with respect to $m2^t$-bit words:

$$f: F_2^{n2^t} \equiv \left(F_2^{2^t}\right)^{km} \to F_2^{n2^t} \equiv \left(F_2^{2^t}\right)^{km},$$

$$f(X_1, \dots, X_k) = (Y_1, \dots, Y_k),$$

with $X_i = (X_{i,1}, \dots, X_{i,m})$ and $Y_i = (Y_{i,1}, \dots, Y_{i,m})$, $1 \le i \le k$, and,

$$Y_{i,j} = \bigoplus_{\substack{\mathfrak{m}_{(i-1)m+j\,,s} \neq 0 \\ 1 \le s \le n}} \left(\left(X_{\left\lceil \frac{s-1}{m} \right\rceil +1\,,1+((s-1)\ mod\ \ m)}\right) >>> z_s\right), \quad 1 \le i \le k, \ \ 1 \le j \le m.$$

Proof: It is easily seen that the rotation operations are pairwise commutable and the order of each rotation operation in $F_2^{2^t}$ is a nonnegative power of two. ∎

4. Nonlinear Number Generators

In this section, we study nonlinear number generators with provable lower bounds on the period, with the aid of matrices over finite commutative rings with identity.

Theorem 4.1: Suppose that R is a finite commutative ring with identity and $A \in \mathcal{M}_m(R)$. If $o(d_R(A)) = p$, then $o(A)$ is a multiple of p.

Proof: Suppose that $o(A) = t$ is not a multiple of p. By Euclidian lemma, there exist q and $r < p$ with $t = qp + r$. Now,

$$d_R(A^t) = (d_R(A))^t = (d_R(A))^r.$$

On the other hand, we have $(d_R(A))^t = 1$ which leads to $(d_R(A))^r = 1$; and this is a contradiction. ■

There is a well-known fact about the (multiplicative) order of elements in Z_{2^n}:

Theorem 4.2: In Z_{2^n}, we have $o(5) = o(2^n - 5) = 2^{n-2}$.

Corollary 4.3: Suppose that $A \in \mathcal{M}_m(Z_{2^n})$ and $d_{Z_{2^n}}(A) \in \{5, 2^n - 5\}$. Then $o(A)$ is a multiple of 2^{n-2}.

Lemma 4.4: Suppose that $A = [a_{u,v}] \in \mathcal{M}_m(Z_{2^n})$ and $d(A) \in \{5, 2^n - 5\}$. Define the matrix $A' = [\mathfrak{a}_{u,v}] \in \mathcal{B}_m$ as

$$\mathfrak{a}_{u,v} = \begin{cases} 1 & a_{u,v} \;\; is \;\; odd, \\ 0 & a_{u,v} \;\; is \;\; even. \end{cases}$$

If $o(A') = 2^m - 1$, then $o(A)$ is a multiple of $2^{n-2}(2^m - 1)$.

Proof: From Corollary 4.3, we know that $o(A)$ is a multiple of 2^{n-2}. On the other hand, $o(A)$ is a multiple of $2^m - 1$, because, the least significant bits of the entries of $(A')^r$, for every r, are equal to the corresponding entries in A^r. Now, $o(A)$ is a multiple of $2^{n-2}(2^m - 1)$ because $(2^{n-2}, 2^m - 1) = 1$. ■

The next theorem is an obvious result of the previous discussions.

Theorem 4.5: Suppose that m, t, s and $w > 1$ are given. Let $M_{j_k} = [\mathfrak{m}_{u,v}^{j_k}] \in \mathcal{B}_m$, $1 \le k \le s$, $0 \le j_1 < \ldots < j_s < t$, and $\{S_i\}_{i \ge 0}$ with

$$S_{i+t} = M_{j_s} S_{i+j_s} \oplus \dots \oplus M_{j_1} S_{i+j_1}, \quad i \geq 0,$$

is the generated sequence of a primitive sigma-LFSR with a nonzero initial state S_0. Define a new sequence

$$S'_{i+t} = M'_{j_s} S'_{i+j_s} + \cdots + M'_{j_1} S'_{i+j_1} \ mod \ \ 2^w, \quad i \geq 0,$$

with $M'_{j_k} = [m^{j_k}_{u,v}] \in \mathcal{M}_m(Z_{2^w})$ and the following property

$$m^{j_k}_{u,v} \ \ mod \ \ 2 = \begin{cases} 1 & \mathfrak{m}^{j_k}_{u,v} = 1, \\ \\ 0 & \mathfrak{m}^{j_k}_{u,v} = 0. \end{cases}$$

Then,

a) The period of the corresponding (companion) matrix of the sequence $\{S'_i\}_{i\geq 0}$ is a multiple of $2^{tm} - 1$.
b) The period of the nonlinear sequence $\{S'_i\}_{i\geq 0}$ is a multiple of $2^{tm} - 1$, in the case that all of the entries of the initial state S'_0 are not even simultaneously.

5. Conclusion

In this paper, we examined matrices over finite commutative groups and rings; in fact, we studied modules on ring of matrices over Z_N and modules over the ring $(F_2^t, \oplus, \wedge)$. We showed that these new algebraic constructions are a generalization of some of the constructions which were presented in [1]. We presented new linearized and nonlinear MDS diffusion layers, based on this mathematical investigation.

Then, we studied nonlinear generators over Z_{2^n} and we presented a lower bound on the period of these nonlinear generators. At last, we presented nonlinear recurrent sequences over Z_{2^n} with periods which are multiples of the period of the corresponding sigma-LFSR's.

References

[1] S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad, Hamidreza Maimani, Einollah Pasha, "Construction of New Families of MDS Diffusion Layers", Cryptology ePrint, Report 2014/011, available via http://eprint.iacr.org/2014/011.pdf.

[2] J. Daemen, V. Rijmen, AES proposal: Rijndael. Selected as the Advanced Encryption Standard. Available from http://nist.gov/aes

[3] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish: A 128-bit Block Cipher; 15 June, 1998

[4] P. Ekdahl, T. Johansson, SNOW a new stream cipher, Proceedings of first NESSIE Workshop, Heverlee, Belgium, 2000

[5] Chinese State Bureau of Cryptography Administration, Cryptographic algorithms SMS4 used in wireless LAN products, available at: http://www.oscca.gov.cn/Doc/6/News-1106.htm

[6] Dengguo Feng, Xiutao Feng, Wentao Zhang, Xiubin Fan and Chuankun Wu, Loiss: A Byte-Oriented Stream Cipher, Available at http:// www.eprint.iacr.org/2010/489.pdf

[7] ETSI/SAGE: Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3 Document 2: ZUC Specification. Version 1.5, 4th January 2011. Tech. rep., ETSI (2011), http://www.gsmworld.com/documents/EEA3-EIA3-ZUC-v1-5.pdf

[8] A. Klimov, Applications of T-functions in Cryptography, Thesis for the degree of Ph.D., Weizmann Institute of Science, 2005.

[9] F. J. MacWilliams and N.J.A. Sloane, “The Theory of Error-Correcting Codes”, North-Holland, Amsterdam, 1998.

[10] Blaum, M., Roth, R. M.: On Lowest Density MDS Codes. IEEE TRANSACTIONS ON INFORMATION THEORY, vol. 45(1), pp. 46-59 (January 1999)

[11] Daniel Augot, Matthieu Finiasz, Exhaustive Search for Small Dimension Recursive MDS

Diffusion Layers for Block Ciphers and Hash Functions, arXiv:1305.3396v1, 15 May 2013.

[12] Pascal Junod, Statistical Cryptanalysis of Block Ciphers, Phd Thesis, Lausanne, EPFL, 2005

[13] Mahdi Sadjadieh, Mohammad Dakhilalian, Hamid Mala, Pouyan Sepehrdad, Recursive Diffusion Layers for Block Ciphers and Hash Functions, fse2012, USA, 2012

[14] Joan Daemen and Vincent Rijmen, The design of rijndael: Aes - the advanced encryption standard, Springer, 2002.

[15] Victor Shoup, “A Computational Introduction to Number Theory and Algebra” (Version 2), Cambridge University Press, 2008.