Noname manuscript No.
(will be inserted by the editor)

Bitwise Linear Mappings with Good Cryptographic Properties and Efficient Implementation

S. M. Dehnavi ·
A. Mahmoodi Rishakani ·
M. R. Mirzaee Shamsabad ·

Received: date / Accepted: date

Abstract Linear mappings are crucial components of symmetric ciphers. A special type of linear mappings are (0,1)-matrices which have been used in symmetric ciphers such as ARIA, E2 and Camellia as diffusion layers with efficient implementation. Bitwise linear maps are also used in symmetric ciphers such as SHA family of hash functions and HC family of stream ciphers. In this article, we investigate a special kind of linear mappings: based upon this study, we propose several linear mappings with only XOR and rotation operations. The corresponding matrices of these mappings can be used in either the former case as (0,1)-matrices of maximal branch number or in the latter case as linear mappings with good cryptographic properties. The proposed mappings and their corresponding matrices can be efficiently implemented both in software and hardware.

Keywords (0,1)-matrix · Bitwise linear map · Branch number · Diffusion layer · Symmetric cipher

1 Introduction

Linear mappings are crucial components of symmetric ciphers. MDS matrices are used as diffusion layers in symmetric ciphers [9–13]. Another type of diffusion layers are (0,1)-matrices. This type of matrices are used in symmetric ciphers such as ARIA [2], E2 [5] and Camellia [1] as diffusion layers with low

S. M. Dehnavi
Department of Mathematical and Computer Sciences, Kharazmi University, Tehran, Iran
E-mail: std_dehnavism@khu.ac.ir

A. Mahmoodi Rishakani
Department of Sciences, Shahid Rajaee Teacher Training University, Tehran, Iran

M. R. Mirzaee Shamsabad
Department of Mathematics and Computer Science, Shahid Bahonar University, Kerman, Iran

implementation cost. Bitwise linear maps are also used in symmetric ciphers such as SHA family [6] of hash functions and HC family [7,8] of stream ciphers.

In this article, we examine a special type of (bitwise) linear mappings: based upon this investigation, we propose several linear mappings. The corresponding matrices of these mappings can be used as (0,1)-matrices of maximal branch number with low implementation cost. Also, these mappings can be applied as linear mappings with good cryptographic properties. The presented mappings or their corresponding matrices can be efficiently implemented both in software and hardware: in comparison to [3,4,14] our proposed mappings have lower implementation costs.

In Section 2 we present preliminary notations and definitions. Section 3 is devoted to main theorem of the paper. Section 4 examines the implementation of the proposed mappings. In Section 5 we present a block cipher with large blocks, based on the proposed mappings.

2 Notations and Definitions

Hamming weight of a natural number or binary vector x is denoted by $w(x)$. The i-th bit of a natural number or a binary vector x is denoted by x_i. The notation $\wedge$ is used for AND operation, $\prec$ for left cyclic shift operation and $\oplus$ for XOR operation. The all-one vector is denoted by $\mathbf{1}$ and the zero vector by $\mathbf{0}$. The finite field of order 2^t is denoted by F_{2^t}.

There is a one-to-one correspondence between Z_{2^n}, the ring of integers modulo 2^n and F_2^n, Cartesian product of n copies of F_2:

$$\varphi : F_2^n \to Z_{2^n},$$

$$x = (x_{n-1}, ..., x_0) \to \varphi(x) = \sum_{i=0}^{n-1} x_i 2^i.$$

We use this correspondence throughout the paper.

Every function $f : F_2^m \to F_2$ is called a Boolean function and every function $f : F_2^m \to F_2^n$ with $n > 1$ is called a vectorial Boolean function or a Boolean map. Such a function can be represented as $(f_{n-1}, ..., f_0)$: the Boolean function $f_i : F_2^m \to F_2$, $0 \leq i < n$, is called the i-th component of f.

We denote the set of all $n \times n$ matrices over F_2 by $\mathcal{M}_n(F_2)$. A function $f : F_2^n \to F_2^n$ with the property

$$f(x \oplus y) = f(x) \oplus f(y), \quad x, y \in F_2^n,$$

is called a (bitwise) linear map. Obviously, there is a matrix in $\mathcal{M}_n(F_2)$ which we denote by M_f such that

$$f(x) = xM_f^T, \quad x \in F_2^n.$$

Here, M_f^T is the transpose of M_f.

Let $f : F_2^n \to F_2^n$ be a linear map. The differential branch number of f is defined as

$$b_f^d = \min_{x \neq \mathbf{0}} \{w(x) + w(f(x))\} = \min_{x \neq \mathbf{0}} \{w(x) + w(xM_f^T)\}.$$

The linear branch number of f is defined as

$$b_f^l = \min_{x \neq \mathbf{0}} \{w(x) + w(xM_f)\}.$$

If we have $b_f^d = b_f^l$, then we say that the branch number of f is b_f^d and denote it by b_f.

Let n be a natural number. We define

$$L_n = \{f : F_2^{2^n} \to F_2^{2^n} : f(x) = \bigoplus_{j=1}^{t} (x \prec i_j), 0 \leq i_1 < \ldots < i_t < 2^n, t = 1 \ mod \ 2, t > 1\}.$$

Let f be in L_n. It is not hard to see that the rows of M_f are cyclic shifts of each other and any row of M_f has t ones: in this case we write $w_{_f} = t$.

Example 1 Consider the linear mapping $f \in L_2$ with

$$f : F_2^4 \to F_2^4,$$

$$f(x) = x \oplus (x \prec 1) \oplus (x \prec 3).$$

We have

$$f(x_3, x_2, x_1, x_0) = (x_2 \oplus x_0 \oplus x_3, x_1 \oplus x_3 \oplus x_2, x_0 \oplus x_2 \oplus x_1, x_3 \oplus x_1 \oplus x_0),$$

or equivalently,

$$f(x) = xM_f^T = (x_3, x_2, x_1, x_0) \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

Here, $w_f = 3$.

We denote the r times composition of a mapping f by itself by $f^{(r)}$. For example we have

$$f^{(3)}(x) = f \circ f \circ f(x).$$

We denote by $o_{_f}$ the order of a linear invertible mapping: $o_{_f}$ is the least natural number such that $f^{(o_f)}$ is the identity function. The number of fixed points of a mapping f, i.e. the points with property $f(x) = x$, is denoted by $p_{_f}$. The complement of a binary vector x is denoted by $\overline{x}$.

Let R be a finite commutative ring with identity. We denote by $R^\star$ the set of all invertible elements of R, by $R[x]$ the ring of polynomials over R and by $\frac{R[x]}{<p(x)>}$ the ring of polynomials modulo a polynomial $p(x) \in R[x]$. Let $p(x) \in R[x]$; we denote by $w(p)$ the number of terms in standard representation of p.

3 Main Theorem

In this section, we investigate some properties of L_n from mathematical viewpoint and lay a theoretical foundation for applications presented in following sections.

Theorem 1 *Let $f \in L_n$ with*

$$f(x) = \bigoplus_{j=1}^{t} (x \prec i_j),\ \ 0 \leq i_1 < \ldots < i_t < 2^n,\ \ t = 1 \ mod\ 2,\ \ t > 1.$$

Then,

a) *The order of f is a power of two and $f^{-1} = f^{(2^n-1)}$.*

b) $\overline{f(x)} = f(\overline{x})$ *and for any $1 \leq r < 2^n$ we have $f(x \prec r) = f(x) \prec r$.*

c) $w(x) = w(f(x))\ mod\ 2$.

d) $b_f^d = b_f^l$.

e) $b_f = 0\ mod\ 2$, *and* $4 \leq b_f \leq t + 1$.

f) $\max_{x \neq \mathbf{1}}\{w(x) + w(f(x))\} = 2^{n+1} - b_f$.

g) *The number of fixed points of f is a power of two and $2 \leq p_f \leq 2^{n-1}$.*

Proof **a)** *We have*

$$f^{(2)}(x) = \bigoplus_{j=1}^{t} (x \prec (2i_j\ mod\ 2^n)),$$

and by induction,

$$f^{(2^n)}(x) = \bigoplus_{j=1}^{t} (x \prec (2^n i_j\ mod\ 2^n)).$$

Since $x \prec (2^n i_j\ mod\ 2^n) = x$ for every $x \in F_2^{2^n}$ and t is odd, then

$$f^{(2^n)}(x) = x, \quad x \in F_2^{2^n},$$

which means that o_f is a power of two, f is invertible and

$$f^{-1}(x) = f^{(2^n-1)}(x), \quad x \in F_2^{2^n}.$$

b) *We note that for every natural number r and every odd natural number q we have*

$$\overline{(x \prec r)} = \overline{x} \prec r, \quad 1 \leq r < 2^n,$$

$$\overline{\bigoplus_{i=1}^{q} x_i} = \bigoplus_{i=1}^{q} \overline{x_i}.$$

This means that $\overline{f(x)} = f(\overline{x})$.

c) *Let* e_k *be the binary representation of* 2^k *for every nonnegative integer* k. *We prove the fact by induction on the weight of the input. We have* $f(\mathbf{0}) = \mathbf{0}$ *and*

$$f(e_k) = \bigoplus_{j=1}^{t} e_{k+i_j \bmod 2^n}, \quad 0 \leq k < 2^n.$$

This means that $w(f(e_k)) = t$, $0 \leq k < 2^n$, *which is an odd number. Now suppose that the induction hypothesis is true for* $k = r$, $1 \leq r < 2^n$. *We prove that for every* $x \in F_2^{2^n}$ *with* $w(x) = r + 1$ *we have*

$$w(x) = w(f(x)) \bmod 2.$$

We know that there exist $0 \leq j < 2^n$ *and* $x' \in F_2^{2^n}$ *such that* $x = x' \oplus e_j$. *By the identity*

$$w(x \oplus y) = w(x) + w(y) - 2w(x \wedge y), \tag{1}$$

we get

$$w(x \oplus y) = w(x) + w(y) \bmod 2.$$

Now by induction hypothesis and (1) we have

$$\begin{aligned} w(f(x)) &= w(f(x' \oplus e_j)) \\ &= w(f(x')) + w(f(e_j)) \bmod 2, \\ &= w(x') + w(e_j) \bmod 2, \\ &= w(x' \oplus e_j) \bmod 2, \\ &= w(x) \bmod 2. \end{aligned}$$

d) *We know that*

$$f(x_{2^n-1}, \ldots, x_0) = (y_{2^n-1}, \ldots, y_0),$$

with

$$y_s = \bigoplus_{j=1}^{t} x_{s+i_j \bmod 2^n}, \quad 0 \leq s < 2^n.$$

For $f' \in L_n$, *corresponding to* M_f^T, *we have*

$$f'(x_{2^n-1}, \ldots, x_0) = (z_{2^n-1}, \ldots, z_0),$$

with

$$z_s = \bigoplus_{j=1}^{t} x_{s+2^n-i_j \bmod 2^n}, \quad 0 \leq s < 2^n.$$

Define

$$\phi : F_2^{2^n} \to F_2^{2^n},$$

$$\phi(x_{2^n-1}, x_{2^n-2}, \ldots, x_2, x_1, x_0) = (x_1, x_2, \ldots, x_{2^n-2}, x_{2^n-1}, x_0).$$

We note that for every $x \in F_2^{2^n}$ *we have* $w(x) = w(\phi(x))$. *Also*

$$w(f'(x)) = w(f(\phi(x))), \quad x \in F_2^{2^n},$$

because

$$(f'(x))_0 = (f(\phi(x))_0,$$

and

$$(f'(x))_s = (f(\phi(x))_{2^n-s}, \quad 0 < s < 2^n.$$

Now

$$\begin{aligned} b_f^d &= \min_{x \neq \mathbf{0}} \{w(x) + w(f(x))\} \\ &= \min_{x \neq \mathbf{0}} \{w(\phi(x)) + w(f(\phi(x)))\} \\ &= \min_{x \neq \mathbf{0}} \{w(x) + w(f'(x))\} \\ &= b_{f'}^d \\ &= b_f^l. \end{aligned}$$

e) *By Case* **c**, b_f *is even. Besides,* f *is a permutation and for every* $x \in F_2^{2^n}$ *with* $w(x) = 1$ *we have* $w(f(x)) = t$. *So*

$$4 \leq b_f \leq t + 1.$$

f) *We have*

$$b_f = \min_{x \neq \mathbf{0}} \{w(x) + w(f(x))\}.$$

So, from Case **b**,

$$\begin{aligned} 2^{n+1} - b_f &= \max_{x \neq \mathbf{0}} \{2^n - w(x) + 2^n - w(f(x))\}, \\ &= \max_{x \neq \mathbf{0}} \{w(\overline{x}) + w(\overline{f(x)})\}, \\ &= \max_{x \neq \mathbf{1}} \{w(x) + w(f(x))\}. \end{aligned}$$

g) *We know that fixed points of every linear mapping construct a linear subspace of* $F_2^{2^n}$ *and so* p_f *would be a power of two. Now since* $f(\mathbf{0}) = \mathbf{0}$ *and* $f(\mathbf{1}) = \mathbf{1}$ *and* f *cannot be the identity function, we get*

$$2 \leq p_f \leq 2^{n-1}.$$

We know that in designing bitwise linear maps, the most desirable targets are F_2^{16}, F_2^{32} and F_2^{64}, because almost all of the modern processors are 16, 32 or 64-bits. Also, in the case of (0,1)-matrices, these numbers are suitable. We have verified the following lemma by programming:

Lemma 1 *Let*

$$f_t : F_2^{16} \to F_2^{16},$$

$$f_t(x) = \bigoplus_{i=0}^{t} \left(x \prec \left(\frac{i(i+1)}{2} \ mod\ 16 \right) \right), \quad t = 2, 4, 6,$$

and

$$g_t : F_2^{32} \to F_2^{32},$$

$$g_t(x) = \bigoplus_{i=0}^{t} \left(x \prec \left(\frac{i(i+1)}{2} \ mod\ 32 \right) \right), \quad t = 2, 4, 6, 8, 10.$$

Then we have

$$b_{f_t} = t + 2, \quad t = 2, 4, 6,$$

and

$$b_{g_t} = t + 2, \quad t = 2, 4, 6, 8, 10.$$

We know that f_6 and g_{10} are mappings of maximal (known) branch number [15,16]. As a practical application, suppose that m is a natural number: the matrix $M_{g_{10}}$ is a (0,1)-matrix that can be viewed as a matrix over F_{2^m}. So, the branch number of $M_{g_{10}}$ with respect to m-bit words [13] would be 12.

In some applications in symmetric cryptography, like the case of block ciphers with SPN structure, we should know the inverse of mappings. In the following examples, we present linear mappings of maximal branch number with the property that the implementation cost for the mapping itself and its inverse are the same.

Example 2 We have found the following mapping in L_4 by programming:

$$f : F_2^{16} \to F_2^{16},$$

$$f(x) = x \oplus (x \prec 1) \oplus (x \prec 2) \oplus (x \prec 3) \oplus (x \prec 4) \oplus (x \prec 11) \oplus (x \prec 14),$$

with

$$f^{-1}(x) = x \oplus (x \prec 2) \oplus (x \prec 5) \oplus (x \prec 12) \oplus (x \prec 13) \oplus (x \prec 14) \oplus (x \prec 15).$$

The mappings f anf f^{-1} have the following properties

$$p_{f^{-1}} = p_f = 2,$$

$$b_{f^{-1}} = b_f = 8,$$

$$w_f = w_{f^{-1}} = 7.$$

We know that b_f is the maximal value [15,16] and p_f is the minimum value.

Example 3 We have found the following mapping in L_5 by programming:

$$f : F_2^{32} \to F_2^{32},$$
$$f(x) = x \oplus (x \prec 8) \oplus (x \prec 9) \oplus (x \prec 12) \oplus (x \prec 22) \oplus (x \prec 24)$$
$$\oplus (x \prec 25) \oplus (x \prec 26) \oplus (x \prec 28) \oplus (x \prec 29) \oplus (x \prec 30),$$

with

$$f^{-1}(x) = (x \prec 2) \oplus (x \prec 4) \oplus (x \prec 5) \oplus (x \prec 7) \oplus (x \prec 8) \oplus (x \prec 10)$$
$$\oplus (x \prec 15) \oplus (x \prec 16) \oplus (x \prec 17) \oplus (x \prec 19) \oplus (x \prec 26).$$

The mappings f anf f^{-1} have the following properties

$$p_{f^{-1}} = p_f = 2,$$
$$b_{f^{-1}} = b_f = 12,$$
$$w_f = w_{f^{-1}} = 11.$$

We know that b_f is the maximal (known) value [15,16] and p_f is the minimum value.

4 Implementation

In this section, we examine some algebraic properties of L_n and based on this investigation, we present linear mappings with efficient implementation in software and hardware.

There is a natural one-to-one correspondence between F_{2^n} and $\frac{F_2[x]}{<x^{2^n}\oplus 1>}$ which maps

$$a = (a_{2^n-1}, \ldots, a_1, a_0) \in F_{2^n},$$

to

$$\bigoplus_{i=0}^{2^n-1} a_i x^i \in \frac{F_2[x]}{< x^{2^n} \oplus 1 >}.$$

Moreover, there is a similar correspondence between mappings in L_n and invertible elements of $\frac{F_2[x]}{<x^{2^n}\oplus 1>} \setminus \{x\}$ which maps

$$f(x) = \bigoplus_{j=1}^{t} (x \prec i_j), \quad 0 \le i_1 < \ldots < i_t < 2^n, \quad t = 1 \ mod\ 2, \quad t > 1,$$

to

$$\bigoplus_{j=1}^{t} x^{i_j}.$$

Now it is easy to verify that for every $a \in F_2^{2^n}$, $f(a)$ corresponds to

$$\left(\bigoplus_{i=0}^{2^n-1} a_i x^i\right)\left(\bigoplus_{j=1}^{t} x^{i_j}\right) \ mod\ (x^{2^n} \oplus 1).$$

Example 4 Consider $f \in L_3$ as

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

$$f(x) = x \oplus (x \prec 2) \oplus (x \prec 5).$$

Let $a = (1,0,0,0,1,1,0,0)$. We have $f(a) = (1,1,0,0,1,0,1,1)$. If we correspond the mappings in L_3 with invertible polynomials in $\frac{F_2[x]}{<x^8 \oplus 1>} \setminus \{x\}$ and the vectors in F_2^8 with polynomials in $\frac{F_2[x]}{<x^8 \oplus 1>}$, then $f(a)$ corresponds to $fa \ mod \ (x^8 \oplus 1)$. In fact we have

$$fa \ mod \ (x^8 \oplus 1) = (1 \oplus x^2 \oplus x^5)(x^2 \oplus x^3 \oplus x^7) \ mod \ (x^8 \oplus 1)$$

$$= 1 \oplus x \oplus x^3 \oplus x^6 \oplus x^7,$$

which corresponds to $(1,1,0,0,1,0,1,1)$.

Note 1 Let n be a natural number and R be the ring $\frac{F_2[x]}{<x^{2^n} \oplus 1>}$. We have

$$R^\star = \{p \in R : w(p) = 1 \ mod \ 2\}.$$

Example 5 Let

$$f_1 : F_2^{16} \to F_2^{16},$$

$$f_1(x) = (x \prec 3) \oplus (x \prec 4) \oplus (x \prec 9),$$

and

$$f_2 : F_2^{16} \to F_2^{16},$$

$$f_2(x) = x \oplus (x \prec 7) \oplus (x \prec 13).$$

It is straightforward to verify that

$$f_1 \circ f_2(x) = x \oplus (x \prec 3) \oplus (x \prec 4) \oplus (x \prec 6) \oplus (x \prec 9) \oplus (x \prec 10) \oplus (x \prec 11).$$

Now, considering the corresponding polynomials in $\frac{F_2[x]}{<x^{16} \oplus 1>}$,

$$p_1 = x^3 \oplus x^4 \oplus x^9,$$

$$p_2 = 1 \oplus x^7 \oplus x^{13},$$

we have

$$p_1 p_2 \ mod \ (x^{16} \oplus 1) = x \oplus x^3 \oplus x^4 \oplus x^6 \oplus x^9 \oplus x^{10} \oplus x^{11},$$

which corresponds to $f_1 \circ f_2$.

From the algebraic viewpoint, $R_1 = (\mathcal{L}_n, \oplus, \circ)$ is a finite commutative ring with identity. Here $\circ$ is the operator of composition of functions and

$$\mathcal{L}_n = \{f : F_2^{2^n} \to F_2^{2^n} : f(x) = \bigoplus_{j=1}^{t}(x \prec i_j), 0 \leq i_1 < \ldots < i_t < 2^n, 0 \leq t < 2^n\}.$$

We note that t in the above definition is a nonnegative integer and the case $t = 0$ means that the zero function is contained in $\mathcal{L}_n$. Let $R_2 = \frac{F_2[x]}{<x^{2^n} \oplus 1>}$, $G_1 = (F_2^n, \oplus)$ and $G_2 = \left(\frac{F_2[x]}{<x^{2^n} \oplus 1>}, \oplus\right)$. Obviously, G_1 is an R_1-module with scalar product

$$fa = f(a), \quad a \in F_2^n, \quad f \in L_n,$$

and G_2 is an R_2-module with natural scalar product.

With regard to previous discussions, the proof of next theorem is easy.

Theorem 2 *As stated above, G_1 is an R_1-module and G_2 is an R_2-module. There is an isomorphism of modules between these two modules. Further,*
a) *We have the one-to-one corrspondence*

$$\psi : R_2^\star \setminus \{x\} \to L_n,$$

$$\psi(\sum_{j=1}^{t} x^{i_j}) = \bigoplus_{j=1}^{t}(x \prec i_j),$$

with the property

$$\psi(p_1 p_2) = \psi(p_1) \circ \psi(p_2), \quad p_1, p_2 \in R_2^\star.$$

b) *Let $a = (a_{2^n-1}, \ldots, a_1, a_0)$ be in $F_2^{2^n}$. There is also a one-to-one correspondence between $\{f(a) : a \in F_2^{2^n}\}$ and*

$$\{\psi(f)a \ mod \ (x^{2^n} \oplus 1) : a = \bigoplus_{i=0}^{2^n-1} a_i x^i\}.$$

Based upon the previous mathematical investigation, we were motivated to search multiplication of polynomials or composition of functions. We found some mappings of this type and of maximal branch number by programming. These mappings have lower implementation costs compared to what is presented in cryptographic literature, up to our knowledge.

Example 6 Consider the linear mappings

$$f_1 : F_2^{32} \to F_2^{32},$$

$$f_1(x) = x \oplus (x \prec 1) \oplus (x \prec 2),$$

and

$$f_2 : F_2^{32} \to F_2^{32},$$

$$f_2(x) = x \oplus (x \prec 2) \oplus (x \prec 7),$$

and

$$f_3 : F_2^{32} \to F_2^{32},$$
$$f_3(x) = x \oplus (x \prec 4) \oplus (x \prec 10),$$

and

$$f : F_2^{32} \to F_2^{32},$$
$$f(x) = f_1 \circ f_2 \circ f_3(x).$$

We have $p_f = 2$ and $b_f = 12$.

Note 2 Let m and s be natural numbers and $M \in \mathcal{M}_m(F_2)$. A rough estimation for the number of XOR operations needed in implementing the action of M on s-bit words is the total number of *one* entries in M.

Now, it is clear that for any (0,1)-matrix M in $\mathcal{M}_{32}(F_2)$ with maximal (known) branch number 12, the total number of one entries is lower bounded by $11 \times 32 = 352$ and the lower buond for XOR's needed for implementation of M is $32 \times 10 = 320$: the mapping in Example 3 has this property. Note that we have not done any other optimizations. The matrix that corresponds to the mapping of Example 6 can be implemented just with $2 \times 3 \times 32 = 192$ XOR's without optimization, which is the best up to our knowledge.

5 Block Ciphers with Large Block Size

In this section, we verify further algebraic properties of L_n and propose a block ciher with large block size. The proof of the following lemma is easy.

Lemma 2 *Let n be a natural number and $p \in \frac{F_2[x]}{<x^{2^{n+1}} \oplus 1>}$. We know that there are $\chi_0, \chi_1 \in \frac{F_2[x]}{<x^{2^n} \oplus 1>}$ such that*

$$p = \chi_0 \oplus x^{2^n} \chi_1.$$

We have

$$w(p \ mod \ (x^{2^n} \oplus 1)) = w(\chi_1 \oplus \chi_0).$$

In particular,

$$w(p) \geq w(p \ mod \ (x^{2^n} \oplus 1)).$$

Theorem 3 *Suppose that n, t with $t = 1 \ mod \ 2$, $t > 1$ and $0 \leq i_1 < \ldots < i_t < 2^n$ are natural numbers and the mapping $f \in L_n$ with*

$$f : F_2^{2^n} \to F_2^{2^n},$$

$$f(x) = \bigoplus_{j=1}^{t} (x \prec i_j),$$

is given. Consider the mapping $g \in L_{n+1}$ with

$$g : F_2^{2^{n+1}} \to F_2^{2^{n+1}},$$

$$g(x) = \bigoplus_{j=1}^{t} (x \prec i_j).$$

Then we have $b_g \geq b_f$.

Proof Suppose that a is a nonzero element in $\frac{F_2[x]}{<x^{2^{n+1}} \oplus 1>}$. *Let the corresponding polynomial of f in* $\frac{F_2[x]}{<x^{2^n} \oplus 1>}$ *is p. We know that there are* $\chi_0, \chi_1 \in \frac{F_2[x]}{<x^{2^n} \oplus 1>}$ *such that*

$$a = \chi_0 \oplus x^{2^n} \chi_1.$$

We distinguish two cases:
a) $\chi_1 \neq \chi_0$*: In this case g(a) is equivalent to*

$$pa \ \ mod \ \ (x^{2^{n+1}} \oplus 1).$$

We know that

$$\begin{aligned} w(pa \ \ mod \ \ (x^{2^{n+1}} \oplus 1)) &= w(p(\chi_0 \oplus x^{2^n} \chi_1) \ \ mod \ \ (x^{2^{n+1}} \oplus 1)) \\ &\geq w(p(\chi_0 \oplus \chi_1) \ \ mod \ \ (x^{2^n} \oplus 1)), \end{aligned}$$

by Lemma 2. Now by the above discussion, equation (1) and the fact that $\chi_0 \oplus \chi_1 \neq 0$, *we have*

$$\begin{aligned} w(a) + w(g(a)) &\geq w(\chi_1) + w(\chi_0) + w(p(\chi_0 \oplus \chi_1) \ \ mod \ \ (x^{2^n} \oplus 1)) \\ &\geq w(\chi_1 \oplus \chi_0) + w(p(\chi_0 \oplus \chi_1) \ \ mod \ \ (x^{2^n} \oplus 1)) \\ &\geq b_f. \end{aligned}$$

b) $\chi_1 = \chi_0 = \chi$*: Let*

$$p\chi \ mod \ (x^{2^{n+1}} \oplus 1) = \gamma_0 \oplus x^{2^n} \gamma_1,$$

and $\gamma = \gamma_0 \oplus \gamma_1$. *It is not hard to see that*

$$pa \ mod \ (x^{2^{n+1}} \oplus 1) = \gamma \oplus x^{2^n} \gamma.$$

On the other hand,

$$p\chi \ mod \ (x^{2^n} \oplus 1) = \gamma.$$

Thus,

$$\begin{aligned} w(a) + w(g(a)) &= 2w(\chi) + w(pa \ mod \ (x^{2^{n+1}} \oplus 1)) \\ &= 2w(\chi) + 2w(p\chi \ mod \ (x^{2^n} \oplus 1)) \\ &\geq 2b_f \\ &\geq b_f. \end{aligned}$$

Since the above discussion is true for every nonzero a in $\frac{F_2[x]}{<x^{2^{n+1}} \oplus 1>}$, *so we have* $b_g \geq b_f$.

Example 7 **(A Block Cipher with Large Block Size)** Consider

$$f, f_1, f_2, f_3 : F_2^{64} \to F_2^{64}$$

with $f = f_1 \circ f_2 \circ f_3$ and

$$f_1(x) = x \oplus (x \prec 1) \oplus (x \prec 2),$$

$$f_2(x) = x \oplus (x \prec 2) \oplus (x \prec 7),$$

$$f_3(x) = x \oplus (x \prec 4) \oplus (x \prec 10).$$

By Theorem 3 and Example 6, $b_f \geq 12$. Consider M_f as a (0,1)-matrix over $F_{2^{16}}$; the branch number of M_f with respect to 16-bit words would be greater than 12. Now we can design a block cipher with Feistel scheme and with internal SPN structure. The internal structure consists of subkey XORing, a layer of 64 parallel Sboxes and diffusion layer M_f. If we use the inverse map over F_2^{16} as the Sbox, then the probability of differential and linear characteristics of one round of the proposed cipher is bounded by $2^{-14\times 12} = 2^{-168}$. Since the block size is 2048 bits, so, 12 rounds of this type has practical security against differential and linear cryptanalysis. Because our purpose in this article is not designing a cipher, so we did not present a key schedule for the presented cipher, although it can be designed with the aid of its round. The proposed cipher suits modern 64-bit processors.

References

1. K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima and T. Tokita, Camellia: a 128-bit block cipher suitable for multiple platforms - design and analysis, in Proceedings of the 7th Annual International Workshop on Selected Areas in Cryptography (SAC '00), vol. 2012 of Lecture Notes in Computer Science, pp. 39-56, 2000.

2. Daesung Kwon, Jaesung Kim, S. Park, Sangwoo Park, Soo Hak Sung, Yaekwon Sohn, Jung Hwan Song, Yongjin Yeom, E-Joong Yoon, Sangjin Lee, Jaewon Lee, Seongtaek Chee, Daewan Han, and Jin Hong, New block cipher: ARIA, in Information Security and Cryptology-ICISC 2003, vol. 2971 of Lecture Notes in Computer Science, pp. 432-445, Springer, Berlin, Germany, 2004.

3. B. Aslan and M. T. Sakall, Algebraic construction of cryptographically good binary linear transformations, Security and Communication Networks, vol. 7, no. 1, pp. 53-63, 2014.

4. M. T. Sakall and B. Aslan, On the algebraic construction of cryptographically good 32 × 32 binary linear transformations, Journal of Computational and Applied Mathematics, vol. 259, pp. 485-494, 2014.

5. M. Kanda, S. Moriai, K. Aoki, H. Ueda, Y. Takashima, K. Ohta, and T. Matsumoto, E2 - A New 128-bit Block Cipher, IEICE Transactions Fundamentals - Special Section on Cryptography and Information Security, vol. E83-A no. 1, pp. 48-59, 2000.

6. Secure Hash Standard, FIPS PUB 180-4, available via http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

7. Wu, Hongjun, "A New Stream Cipher HC-256". Fast Software Encryption - FSE 2004, LNCS 3017: 226-244.

8. Wu, Hongjun (2004). "The Stream Cipher HC-128" available via http://www.ecrypt.eu.org/stream/p3ciphers/hc/hc128_p3.pdf

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

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

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

12. 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

13. A Mahmoodi Rishakani, S. M. Dehnavi, M. R. Mirzaee Shamsabad, Hamidreza Maimani, Einollah Pasha, "New concepts in design of lightweight MDS diffusion layers", 11th International ISC Conference on Information Security and Cryptology (ISCISC), 2014

14. Bon Wook Koo, Hwan Seok Jang, Jung Hwan Song, "On Constructing of a 32 × 32 Binary Matrix as a Diffusion Layer for a 256-Bit Block Cipher", Information Security and Cryptology - ICISC 2006.

15. Markus Grassl, Bounds on the Minimum Distance of Linear Codes and Quantum Codes, 2009, Available at http://www.codetables.de

16. Wolfgang Ch. Schmid and Rudolf Schurer, MinT, the online database for optimal parameters of (t, m, s)-nets, 2009, Available via http://mint.sbg.ac.at