Algebraic Properties of Modular Addition Modulo a Power of Two

S. M. Dehnavi[1], Alireza Rahimipour[2]

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

[2]Faculty of Sciences, Qom University, Qom, Iran
a.rahimipour@stu.qom.ac.ir

Abstract; *Modular addition modulo a power of two, is one of the most applicable operators in symmetric cryptography; therefore, investigating cryptographic properties of this operator has a significant role in design and analysis of symmetric ciphers. Algebraic properties of modular addition modulo a power of two have been studied for two operands by Braeken in fse'05. Also, the authors of this paper, have studied this operator, in some special cases, before. In this paper, taking advantage of previous researches in this area, we generalize algebraic properties of this operator for more than two summands. More precisely, we determine the algebraic degree of the component Boolean functions of modular addition of arbitrary number of summands modulo a power of two, as a vectorial Boolean function, along with the number of terms and variables in these component functions. As a result, algebraic degrees of the component Boolean functions of Generalized Pseudo-Hadamard Transforms are computed.*

Keywords; *Modular addition modulo a power of two; Boolean function; Algebraic Normal Form; Algebraic degree; Pseudo-Hadamard Transform.*

I. INTRODUCTION

Modular addition modulo 2^t is one of the most used operators in symmetric cryptography. Here, t is a positive integer which is usually equal to the size of tipical processors, i.e. 8, 16, 32 or 64. For instance, modular addition is used in Bluetooth [1] and RC4 [2] stream ciphers and IDEA [3], RC6 [4], Twofish [5] and MARS [6] block ciphers. In [7], algebraic properties of this operator for two operands have been studied and the ANF (Algebraic Normal Form) of its component Boolean functions are determined; also, we examined some algebraic properties of modular addition modulo a power of two in special cases in [8]. We note that for a lot of applications in design and analysis of symmetric ciphers, it is important and useful to know the algebraic degree of the component functions and the number of terms and variables in these functions for modular addition modulo a power of two. In [8], we obtained these parameters for modular addition modulo a power of two with a power of two summands and we proposed an algorithm for computing algebraic degrees of modular addition component Boolean functions in general case.

In this paper, we present an explicit formula for algebraic degrees of the component Boolean functions of modular addition modulo a power of two with arbitrary number of summands, along with the number of terms and variables in these functions. Then, as a consequence, we determine the algebraic degree of the component Boolean functions of generalized Pseudo-Hadamard Transformations; these types of transformations are used in some symmetric ciphers like Twofish.

In Section II we present preliminary definitions and theorems; in Section III we find the algebraic degree of component Boolean functions of modular addition in some special cases. Section IV presents an algorithm for finding these degrees in general case. Section V is dedicated to our main results for finding algebraic degree of the component functions of modular addition modulo a power of two, in general case. Section VI studies the algebraic degree of component Boolean functions of generalized PHT's and Section VII is the conclusion.

II. PRILIMINARY DEFINITIONS AND THEOREMS

Let F_2 be the field of order 2. Cartesian product of t copies of F_2 can be considered as a vector space. According to the definition of F_2^t, there is a one-to-one correspondence φ between F_2^t and Z_{2^t}, ring of integers modulo 2^t, as follows:

$$\varphi : {F_2}^t \to Z_{2^t}$$
$$(x_{t-1},..., x_0) \mapsto \varphi(x) = \sum_{i=0}^{t-1} x_i 2^i.$$

A partial order $\preceq$ on F_2^t can be defined as follows:

$$x \preceq a \quad \Leftrightarrow \quad \forall i,\ x_i \le a_i\ ,\ 0 \le i < \mathrm{t}.$$

In the above representation, if

$$x = (x_{t-1},..., x_0), \quad u = (u_{t-1},..., u_0),$$

then x^u is defined as

$$x^u = {x_0}^{u_0} ... {x_{t-1}}^{u_{t-1}}.$$

Each function $f : {F_2}^t \to F_2$ is called a Boolean function. Suppose that f is a Boolean function; f can be represented by its ANF as follows:

$$f(x) = \bigoplus_{u \in Z_{2^t}} h_u x^u, \quad h_u \in F_2; \tag{1}$$

here, the coefficients are determined as

$$h_u = h(u) = \bigoplus_{x \preceq u} f(x).$$

Algebraic degree of a Boolean function is defined as the number of variables in the longest term of its ANF, or equivalently, the maximum Hamming weight $wt(u)$ of nonzero u's. Each function $f : {F_2}^t \to {F_2}^m$ with $m > 1$ is called a *vectorial Boolean function*. Obviously, f is equivalent to

$$(f_{m-1}, ..., f_0),$$

where each f_i, $0 \le i < m$, is a Boolean function $f_i : {F_2}^t \to F_2$. It is well-known that modular addition modulo a power of two, can be represented in Boolean form as follows:

Suppose that $x = (x_{t-1}, ..., x_0)$, $y = (y_{t-1}, ..., y_0)$ and $r = x + y \mod 2^t$. If $r = (r_{t-1}, ..., r_0)$, then

$$\begin{aligned} &r_1 = x_1 \oplus y_1 \oplus c_1, \quad && c_1 = 0 \\ &r_i = x_i \oplus y_i \oplus c_i, \quad && c_i = x_{i-1}y_{i-1} \oplus x_{i-1}c_{i-1} \oplus y_{i-1}c_{i-1} \qquad i > 1. \end{aligned} \tag{2}$$

Theorem 2.1 [7]: Suppose that the ANF of a Boolean function

$$f : {F_2}^t \to F_2$$

is x^u, with $u \in Z_{2^t}$; then ANF of the function $f(x+y)$ is of the form

$$f(x+y) = \bigoplus_{c=0}^{u} x^{(u-c)} y^c; \tag{3}$$

here, the subtraction is done in Z.

Theorem 2.2 [7]: Suppose that $y_1, y_2, ..., y_r \in F_2^t$ and f is defined as in Theorem 2.1; then ANF of $f(y_1 + y_2 + ... + y_r)$ is of the form

$$f(y_1 + y_2 + ... + y_r) = \bigoplus_{\substack{k_1, ... k_r \ge 0 \\ k_1 + ... + k_r = u}} y_1^{k_1} y_2^{k_2} ... y_r^{k_r}. \tag{4}$$

Regarding Theorem 2.2, the algebraic degree of the component Boolean functions of modular addition modulo 2^t can be determined as follows:

For $u = 2^0, 2^1, ... 2^{t-1}$ and $f(x) = x^u$, we can acquire the algebraic degrees of the aforementioned component functions via relation (4) and the fact that all the terms in the rightmost of this relation are different. So, if we find the maximum of the values $\sum_{i=1}^{r} w(k_i)$ in all sets $\{k_1, k_1, ..., k_r\}$, we can find the algebraic degree of these component Boolean functions.

III. THE CASE $r = 2^n$

The results of this section have been presented in [8]; but we review them here, because, our new theorems are proved with the aid of their notations and concepts.

Let *n*, *u* and *t* be three nonnegative integers. According to the discussions of Section II, we consider the equation

$$X_1 + X_2 + ... + X_{2^n} = 2^u, \tag{5}$$

where X_i's , $1 \le i \le 2^n$, are in Z, and $0 \le u < t$.

Now, we transform X_i's to vectors in F_2^t. Regarding Theorem 2.2 and relation (4), we seek for solutions with maximum Hamming weight sum, which we call them *optimum solutions*.

Theorem 3.1: With the above notations, for $u > n$, Hamming weight sum of the solutions with maximum Hamming weight is equal to

$$\sum_{i=1}^{2^n} w(X_i) = 2^n(u-n) + 2^{2n-u}, \qquad n \ge u-n, \tag{6}$$

$$\sum_{i=1}^{2^n} w(X_i) = (2^n - 1)(u-n) + n + 1, \qquad n < u-n; \tag{7}$$

and if $u \le n$, the maximum Hamming weight sum is equal to 2^u.

Proof: Consider two cases:

Case 1) $u > n$: Consider two categories: Category I corresponds to the case $n \ge u-n$, and category II corresponds to the case $n < u-n$. At first, we present a solution for each category and then we prove that these solutions are optimum solutions.

Category I :

$$\begin{aligned} &X_1 = ... = X_{2^j} = 2^{u-n+1} + 2^{u-n} - 1 \\ &X_{2^j+1} = ... = X_{2^n} = 2^{u-n} - 1 \end{aligned} \qquad u = 2n - j \ ,\ 0 \le j \le n-1 \ , \tag{8}$$

and for Category II :

$$\begin{aligned} &X_1 = X_2 = ... = X_{2^n-1} = 2^{u-n} - 1, \\ &X_{2^n} = 2^n + 2^{u-n} - 1; \end{aligned} \tag{9}$$

Hamming weight sum of these solutions are as (6) and (7); and clearly, these solutions satisfy Equation (5). Consider a table (Table *A*) for each category: *A* has 2^n columns. The columns of *A* correspond to representation of X_i's in F_2^t. Each column is ordered bottom-up from indices 1 up to *t*. We denote entries in this table by

$$A(i, j), \quad 1 \le i \le t, \quad 1 \le j \le 2^n .$$

$A(*, j)$ and $A(i,*)$ denote the column *j* and the row *i* of *A*, respectively. Also, by $one(A)$ we refer to number of '1' entries in *A*. If $A(i, j) =$'1' then we define the significance of $A(i, j)$ as 2^{i-1}; and the significance

of $A(i, j)$ is defined as zero, otherwise. Finally, $sum(A)$ is defined as the sum of the significances of all entries in A. Now, consider the two categories:

I) $n \geq u - n$: Suppose that $u = 2n - j,\ 0 \leq j < n$. You can see Table A in figure 1. Since for $1 \leq i \leq n - u + 1$, all '1' entries in A have least possible significances, so the presented solution is optimum.

II) $n < u - n$: In this case, Table A is modified to figure 2. Suppose that a Table B corresponds to another solution

$$\{Y_1, Y_2, ..., Y_{2^n-1}, Y_{2^n}\}, \tag{10}$$

and $one(B) > one(A)$. We define B^* in such a way that in each row i, for every nonzero entry in $A(i,*)$, we replace the corresponding entry in $B(i,*)$ with a '0' entry, if the corresponding entry in $A(i,*)$ is a '1' entry. We define A^* in the same manner. You can see the Tables A^* and B^* in figure 3.

Assume that there exist k '1' entries in $A^*(s_i + 1, t_i)$ for $1 \leq i \leq k$ and m '1' entries in $B^*(l_j + 1, 2^n)$ for $1 \leq j \leq m$, $n < l_j < u - n$. We have,

$$sum(A^*) = 2^{s_1} + 2^{s_2} + ... + 2^{s_k} = 2^{l_1} + 2^{l_2} + ... + 2^{l_m} = sum(B^*). \tag{11}$$

Since all '1' entries in B^* have different significances (we note that there are '1' entries only in $B^*(i, 2^n)$, $n < i \leq u - n + 1$), after simplification of the left-hand side, we can omit equal terms in two sides of Equation (11). Now,

$$sum(A^*) = sum(B^*) \quad \text{and} \quad one(B^*) > one(A^*).$$

We note that none of the 2^{s_i}'s and 2^{l_j}'s are equal and so, two sides of (11) have different terms. Suppose that t_1 is the least power, without loss of generality. We have,

$$1 + 2^{s_2 - s_1} + ... + 2^{s_k - s_1} = 2^{l_1 - s_1} + 2^{l_2 - s_1} + ... + 2^{l_m - s_1},$$

which is a contradiction; so (7) is optimum.

Case 2) $n \geq u$: We present the two following solutions:

For $n = u$ we have $X_1 = X_2 = ... = X_{2^n} = 1,$ and for $n > u$:

$$X_1 = X_2 = ... = X_{2^u} = 1,\ \ X_{2^u+1} = ... = X_{2^n} = 0.$$

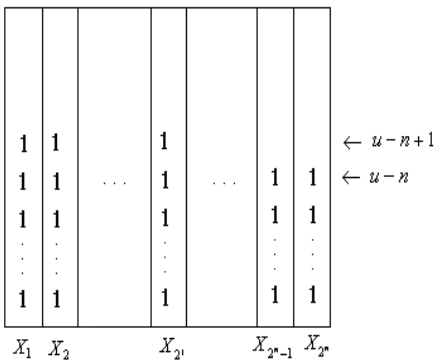


Figure1

Since all '1' entries in A have least possible significances, so the presented solution is optimum. You can see Table A in figure 4.

IV. An algorithm for optimum solutions

In this section, like in [8], we present a method for efficiently solving the problem of finding the algebraic degree of component Boolean functions of modular addition modulo a power of two with arbitrary number of summands. Regarding the notations and assumptions of Section IV, we start from $A(1,1)$ and put '1' entries in the tabe A in entries $A(1,1), A(1,2), \ldots, A(2,1), A(2,2), \ldots$, and continue this procedure until inserting an extra '1' entry in A, yields $sum(A) \geq 2^u$. We let other entries be '0'. Now, if $sum(A) > 2^u$, then conversely, starting from the penultimate row, we delete '1' entries from A until $sum(A) = 2^u$; othrewise, we delete '1' entries from the lower rows and continue this procedure similarly. We note that this solution is such that in each row, other than the last row, at most one of the entries is '0', since otherwise, these two entries can be replaced by one '1' entry from the above row.

Now we claim that this solution has maximum Hamming weight sum. Assume that there exists another solution with greater Hamming weight sum. Again, relate a Table B to this solution. As before, we construct A^* and B^*. Suppose that there exist m '1' entries in $A(k_i+1, s_i)$, $1 \leq i \leq m$, and n '1' entries in $A(l_j+1, t_j)$, $1 \leq j \leq n$. From equation (5), we have:

$$2^{l_1} + 2^{l_2} + \ldots + 2^{l_n} = 2^{k_1} + 2^{k_2} + \ldots + 2^{k_m}. \tag{12}$$

Similar to the Category II of Case 1 in Theorem 3.3, without loss of generality, suppose that l_1 is the least power; then we have,

$$1 + 2^{l_2 - l_1} + \ldots + 2^{l_n - l_1} = 2^{k_1 - l_1} + \ldots + 2^{k_m - l_1}, \tag{13}$$

which is a contradiction.

V. The Main Theorems

In Section IV, we presented a method for efficiently solving the problem of finding the algebraic degree of component Boolean functions of modular addition modulo a power of two, in *general case*. In this section, we obtain the explicit formula of these degrees.

Let n, u and t be three nonnegative integers. According to the discussions of Section II, we consider the equation

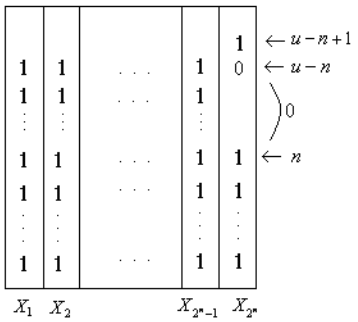


Figure 2

$$X_1 + X_2 + ... + X_n = 2^u, \tag{14}$$

where X_i's , $1 \le i \le n$, are in Z, and $0 \le u < t$. As we know, this equation has

$$\binom{2^u + n - 1}{2^u}$$

nonnegative integer solutions, which is equal to the *number of terms* in the ANF of the *u*-th component function of modular addition modulo a power of two. So, we have:

Fact 5.1: The number of terms in the ANF of the *u*-th component function of modular addition modulo 2^t with n summands, is equal to

$$\binom{2^u + n - 1}{2^u}.$$

Also, it is easy to verify that the number of variables in the ANF of the *u*-th component function is equal to $n(u+1)$:

Fact 5.2: The number of variables in the ANF of the *u*-th component function of modular addition modulo 2^t with n operands, is equal to $n(u+1)$.

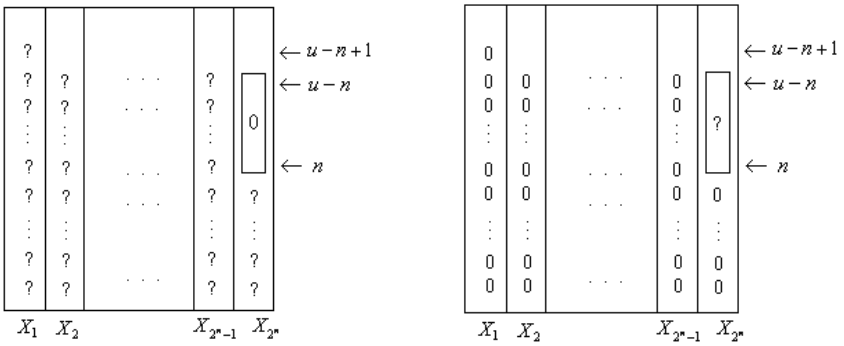
According to the algorithm proposed in Section IV, we obtain the optimum solutions for the equation

$$X_1 + X_2 + ... + X_n = 2^u \tag{15}$$

in general case. These solutions are equal to algebraic degrees of the component Boolean functions of modular addition modulo 2^t, because we have,

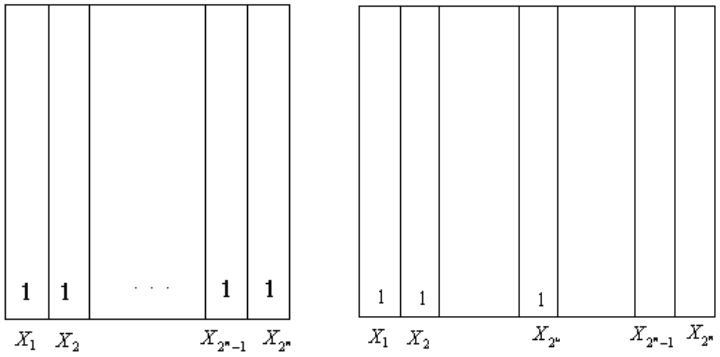
$$f(y_1 + y_2 + ... + y_n) = (y_1 + y_2 + ... + y_n)^{2^u} = \bigoplus_{\substack{k_1,...k_n \ge 0 \\ k_1+...+k_n = 2^u}} y_1^{k_1} y_2^{k_2} ... y_n^{k_n}.$$

Note 5.3: In equation (15), if $n > 2^u$, then some of X_i's are zero and so (15) is modified to an equation with $n \le 2^u$.



A^* and B^*

Figure 3



Case $n = u$ and Case $n > u$

Figure 4

Theorem 5.4: The optimum solutions for (15) have Hamming weight

$$nr + j - wt(X^*),$$

for $n, u > 0$; here,

$$r = \left\lceil \log_2 \left(\frac{2^u + n}{n}\right) \right\rceil, \quad j = 2^{u-r} + \left\lfloor n2^{-r} \right\rfloor - n + 1, \quad X^* = \left\lfloor n2^{-r} \right\rfloor 2^r - n + 2^r .$$

Proof: According to the presented algorithm, we construct Table A in Figure 5. Since the significance of each entry in $A(i,*)$ is 2^{i-1}, in order to find r, we have,

$$n(2^r - 1) \le 2^u < n(2^{r+1} - 1). \tag{16}$$

Simplifying (16), we get

$$r = \left\lceil \log_2 \left(\frac{2^u + n}{n}\right) \right\rceil,$$

and for j, we have,

$$n(2^r - 1) + (j-1)2^r < 2^u \le n(2^r - 1) + j2^r,$$

which leads to

$$j = \left\lfloor 2^{u-r} + n2^{-r} - n \right\rfloor + 1.$$

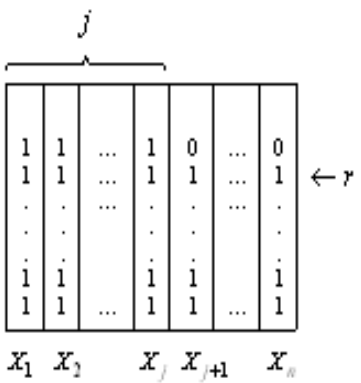


Figure 5

Adding $A(r+1, j) = '1'$ to Table A, leads to $sum(A) > 2^u$; so optimum Hamming weight is obtained by subtracting the Hamming weight of the extra amount from $wt(sum(A))$. The extra amount is equal to

$$X^* = (n(2^r - 1) + j2^r) - 2^u. \tag{17}$$

Substituting the values of j, r in (17), yields

$$X^* = \left\lfloor n2^{-r} \right\rfloor 2^r - n + 2^r.$$

If we denote r, j and X^* corresponding to u-th component function of modular addition modulo a power of two (in Theorem 5.1) by r_u, j_u and X_u^*, then by some easy calculations, we can verify that for $u > \log_2(n^2 - n)$ we have,

$$r_{u+1} = r_u + 1,$$
$$j_{u+1} = j_u,$$
$$wt(X_{u+1}^*) = wt(X_u^*) + 1;$$

so we have the following result:

Result 5.5: *The algebraic degrees of component Boolean functions of modular addition modulo a power of two with n summands, form an arithmetic progression with common difference $n-1$, for $u > \log_2(n^2 - n)$.*

VI. Generalized Pseudo-Hadamard Transformations

Pseudo-Hadamard Transforms (PHT's) are used in symmetric cryptography. For example, in block cipher Twofish, PHT is used in this form:

Let x, y be the input words and x', y' be corresponding output words. Then PHT is defined as

$$x' = 2x + y,$$
$$y' = x + y.$$

Algebraic degree of the second relation was obtained in previous sections. Now we want to obtain the algebraic degree of the first relation. According to relation (3),

$$f(2x + y) = (2x + y)^{2^u} = \bigoplus_{\substack{k,k' \geq 0 \\ k+k' = 2^u}} (2x)^k y^{k'}.$$

Algebraic degrees of component Boolean functions of $2x + y$ are derived by substituting $2^u = 2^0, 2^1, \ldots 2^{t-1}$ in the above formula. Because the least significant bit of $2x$ is zero, in order to find these degrees, k must be even. Maximum Hamming weight of optimum solution is achieved via

$$k + k' = 2^u; \quad k' \geq 0, \ k \text{ is enen.}$$

In the sequel, we suppose that $u > 2$. In this case, Table A in the presented algorithm is modified to Figure 6. Regarding Table A, we have,

$$2(2^r - 1) - 1 \leq 2^u < 2(2^{r+1} - 1) - 1;$$

and after simplification, r is obtained as follows:

$$r = \lfloor \log_2 (2^u + 3) \rfloor - 1.$$

The value of r is also equal to

$$r = u + \left\lfloor \log_2 (1 + \frac{3}{2^u}) \right\rfloor - 1 = u - 1,$$

and j is such that

$$2(2^r - 1) + (j-1)2^r - 1 < 2^u \le 2(2^r - 1) + j2^r - 1,$$

which leads to

$$j = 2^{u-r} + \lfloor 3.2^{-r} \rfloor - 1.$$

Therefore j is changed to

$$j = \lfloor 3.2^{-r} \rfloor + 1.$$

Since $r > 0$, so $j = 1,2$, and,

$$X^* = 2(2^r - 1) - 1 + j2^r - 2^u.$$

In the case $u > 2$ and $j = 1$ we have $X^* = 2^{u-1} - 3$ with $wt(X^*) = u - 2$ and for $j = 2$ we have $X^* = 2^u - 3$ with $wt(X^*) = u - 1$. Thus, Hamming weight of optimum solution is equal to

$$2r - 1 - wt(X^*),$$

for $u > 2$.

Algebraic degrees of component Boolean functions of transformations of the form $\sum_{i=1}^{n} 2^{l_i} X_i$, which we call them generalized PHT's, can be derived in the same manner. We note that in our definition, $2^{l_i} \le 2^u$. According to (4), for component Boolean functions of generalized PHT's, we have,

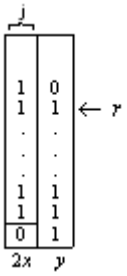


Figure 6

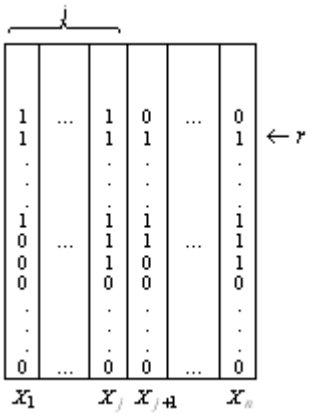


Figure 7

$$f(\sum_{i=1}^{n} 2^{l_i} X_i) = (\sum_{i=1}^{n} 2^{l_i} X_i)^{2^u} = \bigoplus_{\substack{k_1,\dots k_n \geq 0 \\ k_1+\dots+k_n=2^u}} (2^{l_1} X_1)^{k_1} \dots (2^{l_n} X_n)^{k_n}.$$

Algebraic degrees of component Boolean functions of $\sum_{i=1}^{n} 2^{l_i} X_i$ is obtained from optimum solutions of $k_1 + k_2 + \dots + k_n = 2^u$ with constraints $k_n > 2^{l_n}, \dots, k_1 > 2^{l_1}$. We suppose that the equation $k_1 + k_2 + \dots + k_n = 2^u$ is simplified before applying the algorithm. Since $2^{l_i} X_i$ has l_i zero bits in its least significant positions, Table A is modified to Figure 7. So the value of r is obtained as follows

$$n(2^r - 1) - \sum_{i=1}^{n} (2^{l_i} - 1) \leq 2^u < n(2^{r+1} - 1) - \sum_{i=1}^{n} (2^{l_i} - 1),$$

which is simplified to

$$r = \left\lfloor \log_2 (2^u + \sum_{i=1}^{n} 2^{l_i}) - \log_2 n \right\rfloor.$$

Since $n \leq 2^u$, so we have $\log_2 n \leq u$. Therefore, $r \geq 0$. If $\sum_{i=1}^{n} 2^{l_i} > 2^u$, then $r = 0$; and for j we have

$$n(2^r - 1) - \sum_{i=1}^{n} (2^{l_i} - 1) + (j-1)2^r < 2^u \leq n(2^r - 1) - \sum_{i=1}^{n} (2^{l_i} - 1) + j2^r,$$

which is simplified to

$$j = 2^{u-r} + [(\sum_{i=1}^{n} 2^{l_i}) / 2^r] - n + 1,$$

and X^* is equal to

$$X^* = n(2^r - 1) - \sum_{i=1}^{n} (2^{l_i} - 1) + j2^r - 2^u.$$

Thus the maximum Hamming weight is equal to

$$nr + j - wt(X^*) - \sum_{i=1}^{n} l_i \ . \qquad (18)$$

Example 6.1: Consider the transformation

$$Y_1 = 4X_1 + 2X_2 + 2X_3 + X_4,$$
$$Y_2 = 2X_1 + 2X_2 + X_3 + X_4,$$
$$Y_3 = 2X_1 + X_2 + 2X_3 + X_4,$$
$$Y_4 = X_1 + X_2 + X_3 + X_4,$$

on $(Z_{2^8})^4$ which is a generalized PHT. We have computed the algebraic degrees of the component Boolean functions of the outputs of this transformation. For Y_1, we have

(13,10,7,5,3,2,1,1).

For Y_2, we have

(16,13,10,7,5,3,2,1).

For Y_3, we have

(16,13,10,7,5,3,2,1);

and for Y_4, we have

(18,15,12,9,6,4,2,1).

These results are compatible with (18).

VII. Conclusion

Modular addition modulo a power of two, is one of the most applicable operators in symmetric cryptography; therefore, investigating cryptographic properties of this operator has a significant role in design and analysis of symmetric ciphers.

Algebraic properties of modular addition modulo a power of two have been studied for two operands by Braeken in fse'05. Also, the authors of this paper, have studied this operator, in some special cases, before. In this paper, taking advantage of previous researches in this area, we generalized algebraic properties of this operator for more than two operands. More precisely, we determined the algebraic degree of the component Boolean functions of modular addition of arbitrary number of summands modulo a power of two, as a vectorial Boolean function, along with the number of terms and variables in these component functions. As a result, algebraic degrees of the component Boolean functions of Generalized Pseudo-Hadamard Transforms were driven.

References

[1] Bluetoth SIG, "Specification of the Bluetooth System", Verson 1.1, 1 Febrary 22, 2001, available at http://www.bluetooth.com.

[2] R.L.Rivest, "The RC4 encryption algorithm," RSA Data Security, Inc., Mar., 1992.

[3] X. Lai and J. Massey. "A proposal for a new block encryption standard". In I. Damg_ard, editor, Advances in Cryptology , Eurocrypt'90: Workshop on the Theory and Application of Cryptographic Techniques,

Aarhus, Denmark, May 1990. Proceedings, volume 473 of LectureNotes in Computer Science, pages 389-404. Springer-Verlag, 1991.

[4] J. Jonsson and B. S. Kaliski, Jr, “RC6 block cipher”, Primitive submitted to NESSIE by RSA, Sept. 2000.

[5] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, “Twofish: A 128-Bit Block Cipher”, 1998, Available via http://www.counterpane.com/twofish.html.

[6] C. Burwick, D. Coppersmith, E. D'Avignon, R. Gennaro, S. Halevi, C. Jutla, S.M. Matyas Jr., L. O'Connor, M. Peyravian, D. Safford and N. Zunic, “MARS: a candidate cipher for AES”, Presented in the 1st AES conference, CA, USA, August 1998.

[7] A. Braeken, I. Semaef, “The ANF of Composition of Addition and Multiplication mod 2^n with a Boolean Function”, FSE’03, LNCS 2887, pp. 290-306, Springer-Verlag, 2003.

[8] Alireza Rahimipour, S. M. Dehnavi and Mehdi Alaeiyan,“Algebraic Properties of Modular Addition Modulo 2^t”, Southeast Asian Bulletin of Mathematics, 36: 125-134, 2012.