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

Statistical Properties of Multiplication mod 2^n

A. Mahmoodi Rishakani ·
S. M. Dehnavi ·
M. R. Mirzaee Shamsabad ·
Hamidreza Maimani ·
Einollah Pasha

Received: date / Accepted: date

Abstract In this paper, we investigate some statistical properties of multiplication mod 2^n for cryptographic use. For this purpose, we introduce a family of T-functions similar to modular multiplication, which we call M-functions. We obtain the probability distribution of M-functions as vectorial Boolean functions. At first, we determine the joint probability distribution of arbitrary number of the output of an M-function component bits. Then, we obtain the probability distribution of the component Boolean functions of combination of a linear transformation with an M-function. After that, using a new measure for computing the imbalance of maps, we show that the restriction of the output of an M-function to its upper bits is asymptotically balanced.

Keywords Modular multiplication · Boolean function · Joint probability distribution · T-function · Symmetric cryptography

1 Introduction

Cryptanalysis of the operations that have been used in various cryptosystems up to now or might be used in cryptosystems in future is important in two aspects; from the viewpoint of a cryptanalysist who wants to analyze a cryptosystem, a comprehensive knowledge of the components is crucial, and from the viewpoint of a designer who wants to design a cryptosystem, choosing components satisfying desired cryptographic properties is important. Since modular multiplication modulo 2^n is one of the basic operations (instructions) in modern microprocessors, our aim is to give some insight to a designer to choose either the operation of multiplication or some T-functions [6, 1] with

Shahid Rajaee Teacher Training University, Tehran, Iran: am.rishakani@srttu.edu
Kharazmi University, Tehran, Iran
Shahid Bahonar University, Kerman, Iran
Shahid Rajaee Teacher Training University, Tehran, Iran
Kharazmi University, Tehran, Iran

the same statistical properties as a component in a cryptosystem. We know that modular multiplication modulo 2^n is amongst the applied operations in cryptography, especially in symmetric cryptography; i.e. block ciphers, and stream ciphers. For example, modular multiplication is used in RC6 [8] and MARS [3] block ciphers and Sosemanuk [2] stream cipher.

In this paper, we investigate some statistical properties of a family of T-functions similar to modular multiplication modulo 2^n, which we call M-functions. We obtain the probability distribution of this family of functions as vectorial Boolean functions. In [7] we proposed an algorithm to calculate the joint probability distribution of any number of modular multiplication component bits. Here, we obtain a closed formula for the joint probability distribution of any number of an M-function (modular multiplication) component bits.

After that, we discuss the probability distribution of combination of the output of an M-function with a linear layer. As a consequence of this discussion, we show that the upper bits of an M-function play an important role in the probability distribution of an XOR of its component bits.Using a measure for computing the imbalance of functions, we show that the restriction of the output of an M-function to its upper bits is asymptotically balanced.

In Section 2, we present preliminary notations and definitions. Section 3 discusses statistical properties of an M-function component bits. Section 4 is devoted to the linear properties of modular multiplication. Section 5 discusses the imbalance of M-functions and Section 6 is the conclusion.

2 Preliminaries

In this paper, the number of elements (cardinal) of a finite set A is denoted by $|A|$. For a function $f : A \to B$, the preimage of an element $b \in B$ is defined as $\{a \in A | b = f(a)\}$ and denoted by $f^{-1}(b)$.

Let Z_{2^n} be the ring of integers modulo 2^n; there is a one-to-one correspondence between Z_{2^n} and Z_2^n (Cartesian product of n copies of Z_2).

$$\varphi : Z_2^n \to Z_{2^n},$$

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

The i-th bit of a natural number or a binary vector x is denoted by x_i. For every nonzero vector $a \in Z_2^n$, $p(a)$ is defined as the greatest power of 2 that divides $\varphi(a)$ in (1) and $p(0) := n + 1$.

Every function $f : Z_2^n \to Z_2$ is called a Boolean function, and every function $f : Z_2^n \to Z_2^m$ with $m > 1$ is called a vectorial Boolean function or an S-box [4]. Such a function can be represented as a vector of Boolean functions $(f_{m-1}, ..., f_0)$ where each f_i is a Boolean function $f_i : Z_2^n \to Z_2$ and is called the i-th component Boolean function.

A function $f : A \to B$, with $|A| = n$, $|B| = m$ and $n = md$, is called balanced if and only if

$$\forall b \in B \quad |f^{-1}(b)| = d.$$

The following notation are used throughout this paper:

$\oplus$: The bit-wise XOR operation,

$x \gg m$ $(x \ll m)$: Shift of a vector x by m bits to the right (left),

$x >>> m$: Cyclic shift of a vector x by m bits to the right,

$x \cdot y$: The inner product of vectors x and y.

In all parts of this paper, by modular multiplication, we mean modular multiplication modulo a power of two, and the equivalence of Z_{2^n} and Z_2^n according to (1) shall be used frequently.

3 Statistical Properties

We use the methods and concepts of T-functions [6] in this section. Let's recall some definitions and theorems.

3.1 T-functions

For the first time, Shamir and Klimov [6] formally defined T-functions and mentioned their cryptographic applications. Their idea in definition of T-functions is somehow an extension of primitive operations like modular addition and multiplication modulo a power of two. These operations have the property that the i-th bit of the output, depends only on bits $0, ..., i$ of both inputs.

By $\mathcal{B}_{m,n}$ we mean all $m \times 1$ matrices with n-bit word entries or equivalently, all the $m \times n$ $(0, 1)$-matrices. So, for any $x \in \mathcal{B}_{m,n}$ we have these two representations,

$$x = \begin{pmatrix} x^0 \\ x^1 \\ \vdots \\ x^{m-1} \end{pmatrix} = \begin{pmatrix} x^0_{n-1} & \cdots & x^0_1 & x^0_0 \\ x^1_{n-1} & \cdots & x^1_1 & x^1_0 \\ \vdots & \ddots & \vdots & \vdots \\ x^{m-1}_{n-1} & \cdots & x^{m-1}_1 & x^{m-1}_0 \end{pmatrix}.$$

For every $x \in \mathcal{B}_{m,n}$, bitslice i of x, $0 \leq i < n$, is denoted by x_i and is defined as the column i of $m \times n$ matrix representation. In fact $x_i = \left(x^0_i, \cdots, x^{m-1}_i\right)^T$; here, the superindex T means transposition.

Definition 1 [6] A function,

$$f : \mathcal{B}_{m,n} \to \mathcal{B}_{l,n},$$

$$x \mapsto y = f(x),$$

is called a T-function if the i-th column of the output,

$$f_i(x) := (f(x))_i = \left(y_i^0, \cdots, y_i^{l-1}\right)^T$$

depends only on the first $i+1$ columns of the input $x_i, \cdots, x_0$.

Example 1 $f(x) = 2x \pmod{2^n}$ is a T-function, because,

$$f_{n-1}(x) = x_{n-2}, \cdots, f_1(x) = x_0, f_0(x) = 0.$$

In Example 1, we see that f_i does not depend on x_i; such T-functions are called *Parameters.*

Definition 2 [6] A parametric function is a function

$$g\left(x_1, \cdots, x_a; \alpha_1, \cdots, \alpha_b\right)$$

whose variables, are split by a semicolon into inputs (the x_i's) and parameters (the α_j's).

According to Definition 2, a parametric function is called invertible if and only if it is invertible for any values of parameter variables. In verifying the invertibility of T-functions, it is better to have a parametric function notion. We know that for a T-function f, f_i's inputs are $x_i, \cdots, x_0$. Therefore, we can assume x_i as input variable and $x_{i-1}, \cdots, x_0$ as parameter variables. Regarding to this notation we have the next theorem.

Theorem 1 *[6] A T-function f is invertible if and only if f_0 is invertible and for every $i \geq 1$, f_i is a parametric invertible function.*

3.2 Probability Distribution of M-functions

In this section, we present a family of T-functions with the same statistical properties to modular multiplication.

Definition 3 We define a T-function,

$$f : Z_2^n \times Z_2^n \to Z_2^n,$$

$$z = f(x, y),$$

with,

$$z_0 = x_0 y_0,$$

$$z_i = x_i y_0 \oplus x_0 y_i \oplus \gamma_i, \quad 0 < i < n,$$

$$f(x, 0) = 0,$$

$$f(x, (y \ll j)) = f(x, y) \ll j, \quad 0 < j < n;$$

where γ_i is a parameter depending on $x_{i-1}, \cdots, x_0$ and $y_{i-1}, \cdots, y_0$, an n-bit M-function.

In the sequel, we consider the inputs of M-functions are uniformly distributed.

Theorem 2 *Let f be an n-bit M-function*

$$f : Z_{2^n} \times Z_{2^n} \to Z_{2^n},$$

$$(x, y) \mapsto f(x, y).$$

Then, for every $a \in Z_2^n$ we have,

$$|f^{-1}(a)| = (p(a) + 1)2^{n-1}.$$

Proof Suppose that $M = [m_{i,j}]$ is the matrix of the outputs of f: a matrix with 2^n rows and 2^n columns numbered with $0, 1, \cdots, 2^n - 1$, and,

$$m_{i,j} = f(i, j), \quad 0 \leq i, j < 2^n.$$

We count the number of occurrences of each word in each column. If we fix the word $y = b$, $b \in Z_{2^n}$, the vector of the outputs of $f(x, b)$, $0 \leq x < 2^n$, is the b-th column of M. We distinguish three cases:
Case 1: *If $p(b) = 0$, then b is an odd number ($b_0 = 1$). From the assumptions, we have,*

$$f_0(x, b) = x_0 b_0 = x_0,$$

$$f_i(x, b) = x_i \oplus \beta_i, \quad 1 \leq i < n.$$

Here, β_i is a parameter. Now, f_0 is invertible and all f_i's, $i \geq 1$, are parametric invertible functions. So, according to Theorem 1, $f(x, b)$ is invertible. This means that every word in column b appears once.
Case 2: *If $p(b) = n + 1$, then $b = 0$. We have $f(x, 0) = 0$. Thus, the 0-th column is zero.*
Case 3: *If $p(b) = j$, $1 \leq j < n$, then there exists an odd number $\acute{b}$ of length $n - j$ bits such that $b = \acute{b} \ll j$:*

$$f(x, b) = f(x, \acute{b} \ll j) = f(x, \acute{b}) \ll j. \tag{2}$$

In this case, the outputs of f do not depend on $x_{n-j}, \cdots, x_{n-1}$ (this comes from (2) and the fact that f is a T-function) , so every output in the y-th column appears 2^j times. By the Case 1 and (2), the outputs of f in this case are the multiples of 2^j in Z_{2^n}.
Now, we should count the number of columns corresponding to $p(y)$. There are 2^{n-1} odd columns, and the number of columns indexed by the even number y with $p(y) = j$, $1 \leq j < n$, is equal to 2^{n-j-1}; there is just one column with $p(y) = n + 1$, i.e. column 0.
Now, let $A_{x,y}$ denote the number of occurrences of x in column y of matrix M; we have,

$$|f^{-1}(0)| = \sum_{y=0}^{2^n-1} A_{0,y} = A_{0,0} + \sum_{p(y)=0} A_{0,y} + \sum_{1 \leq p(y) < n} A_{0,y}$$

$$= 2^n + \sum_{p(y)=0} 1 + \sum_{p(y)=i,\, 1\le i<n} \left(2^{n-i-1}2^i\right)$$
$$= (n+2)2^{n-1};$$

and for every odd a,

$$|f^{-1}(a)| = \sum_{y=0}^{2^n-1} A_{a,y} = \sum_{p(y)=0} A_{a,y} = 2^{n-1}.$$

Now, for all even a's with the property $1 \le p(a) = i < n$*, we have,*

$$|f^{-1}(a)| = \sum_{y=0}^{2^n-1} A_{a,y} = \sum_{p(y)=0} A_{a,y} + \sum_{p(y)=s,\, 1\le s\le i} A_{a,y}$$
$$= 2^{n-1} + i2^{n-1}.$$

This ends the proof.

Corollary 1 *Let f be an n-bit M-function with* $z = f(x, y)$*; then, for every* $a \in Z_2^n$ *we have,*

$$P(z = a) = \frac{p(a)+1}{2^{n+1}}.$$

In the following, we determine the joint probability distribution of any number of component bits of an M-function.

Theorem 3 *Let*

$$f : Z_2^n \times Z_2^n \to Z_2^n$$
$$z = f(x, y)$$

be an M-function. Then for every $0 \le i_0 < i_1 < \cdots < i_{k-1} < n$ *and* $a_0, \cdots, a_{k-1} \in Z_2$*, we have,*

$$P\left(z_{i_{k-1}} = a_{k-1}, \cdots, z_{i_0} = a_0\right) = \frac{1}{2^k} + \sum_{r=0}^{k-1} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+k-r+1}}. \quad (3)$$

Here we define $\prod_{s=0}^{-1}(1-a_s) := 1$*.*

Proof We take two steps,
Step 1: *A simple calculation shows that for every* $a = (a_{n-1}, \cdots, a_0) \in Z_2^n$*,* $p(a) = 1 + \sum_{r=0}^{n-1}(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)$*; so for every* $n \in N$*, for the case* $k = n$ *from Corollary 1, we have,*

$$P\left(z_{n-1} = a_{n-1}, \cdots, z_0 = a_0\right) = P(z = a)$$
$$= \frac{p(a)+1}{2^{n+1}}$$

$$= \frac{1}{2^n} + \sum_{r=0}^{n-1} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{n+1}}.$$

This proves the theorem in this case.

Step2: *For a fixed n, we show the theorem is true for any $1 \le k \le n$. We use reverse induction on k: from Step1, the theorem is true for $k = n$. Now suppose (3) is true for $k = t$, $2 \le t \le n$. We want to determine $P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0\right)$ for some $0 \le i_0 < i_1 < \cdots < i_{t-2} < n$ and $a_0, \cdots, a_{t-2} \in Z_2$.*

We distinguish three cases:

Case1: $i_0 > 0$*: by basic relations of probability theory and the reverse induction hypothesis, we have,*

$$P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0\right)$$

$$= P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0, z_0 = 0\right) + P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0, z_0 = 1\right)$$

$$= \left(\frac{1}{2^t} + \frac{1}{2^{t+1}} + \sum_{r=0}^{t-2} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r}}\right) + \left(\frac{1}{2^t} - \frac{1}{2^{t+1}}\right)$$

$$= \frac{1}{2^{t-1}} + \sum_{r=0}^{t-2} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r}}.$$

Case2: $i_{t-2} < n-1$*: by basic relations of probability theory and the reverse induction hypothesis, we have,*

$$P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0\right)$$

$$= P\left(z_{n-1} = 0, z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0\right) + P\left(z_{n-1} = 1, z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0\right)$$

$$= \left(\frac{1}{2^t} + \sum_{r=0}^{t-2} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r+1}} + \frac{\prod_{s=0}^{t-2}(1-a_s)}{2^{n+1}}\right)$$

$$+ \left(\frac{1}{2^t} + \sum_{r=0}^{t-2} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r+1}} - \frac{\prod_{s=0}^{t-2}(1-a_s)}{2^{n+1}}\right)$$

$$= \frac{1}{2^{t-1}} + \sum_{r=0}^{t-2} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r}}.$$

Case3: $i_0 = 0$, $i_{t-2} = n-1$*: in this case, there is an index $0 \le j < t-2$ such that $i_{j+1} - i_j > 1$; so there exists a number with the property $i_j < m < i_{j+1}$. Therefore, we have,*

$$P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_{i_0} = a_0\right)$$

$$= P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_m = 0, \cdots, z_{i_0} = a_0\right) + P\left(z_{i_{t-2}} = a_{t-2}, \cdots, z_m = 1, \cdots, z_{i_0} = a_0\right)$$

$$= \left(\frac{1}{2^t} + \sum_{r=0}^{j} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r+1}} + \frac{\prod_{s=0}^{j}(1-a_s)}{2^{m+t-j}} + \sum_{r=j+1}^{t-2} \frac{(-1)^{a_r} \prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r}}\right)$$

$$+\left(\frac{1}{2^t}+\sum_{r=0}^{j}\frac{(-1)^{a_r}\prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r+1}}-\frac{\prod_{s=0}^{j}(1-a_s)}{2^{m+t-j}}\right)$$
$$=\frac{1}{2^{t-1}}+\sum_{r=0}^{t-2}\frac{(-1)^{a_r}\prod_{s=0}^{r-1}(1-a_s)}{2^{i_r+t-r}}.$$

This ends the proof.

Corollary 2 *If $z=f(x,y)$ is an n-bit M-function, then for every $a\in Z_2$ and $0\leq i<n$, we have,*

$$P(z_i=a)=\frac{1}{2}+\frac{(-1)^a}{2^{i+2}}. \tag{4}$$

Equation (4) means that bitslices of any M-function is asymptotically balanced.

4 Linear Properties of Modular Multiplication

In this section, we investigate linear properties of modular multiplication. Consider the case that a symmetric cipher applies modular multiplication ($z=xy\ mod\ 2^n$) in a component. In linear cryptanalysis [8], computing the probability

$$P(a\cdot x\oplus b\cdot y=c\cdot z),$$

for any $a,b,c\in Z_2^n$ is crucial. So, as a special case, we solve the problem for the case $a=b=0$ and arbitrary c in Z_2^n. It is not hard to verify that modular multiplication mod 2^n is an n-bit M-function. So, we prove the theorem for M-functions.

Definition 4 We represent the n-bit *convolution* by $*$ and for every $x,y\in Z_2^n$ we write $z=x*y$ with

$$z_i=\bigoplus_{0\leq j\leq i}x_jy_{i-j},\quad 0\leq i<n.$$

Doing some simple calculations show that the convolution map is an M-function.

Theorem 4 *Let*

$$f:Z_2^n\times Z_2^n\to Z_2^n,$$
$$z=f(x,y),$$

be an M-function. Then for every $0\leq i_0<i_1<\cdots<i_{k-1}<n$, we have,

$$P\left(\bigoplus_{0\leq j<k}z_{i_j}=0\right)=\frac{1}{2}+\frac{1}{2^{i_{k-1}+2}}.$$

Proof It is sufficient to prove the assertion for the convolution map, because Theorem 3 is true for all M-functions. So, let f be the m-bit convolution map with $m = i_{k-1} + 1$. Then we construct a new T-function $g : Z_2^m \times Z_2^m \to Z_2^m$ with the following bitslices,

$$g_i = (t \gg (m - i - 1)).(z_{m-1}, \cdots, z_1, z_0) \quad 0 \leq i < m.$$

Here t is a $(0,1)$-vector of length m such that its j-th coordinate is 1 if and only if $j \in \{i_0, i_1, \cdots, i_{k-1}\}$. It is easy to check that g is an M-function; thus by Corollary 2 we have,

$$P\left(\bigoplus_{0 \leq j \leq k-1} z_{i_j} = 0\right) = P\left(g_{m-1} = 0\right) = \frac{1}{2} + \frac{1}{2^{m+1}}.$$

This ends the proof.

Theorem 4 shows that if we have a linear combination of the outputs of modular multiplication, then the probability distribution of the resulting Boolean function is the same as the probability distribution of the maximum indexed component bit in the linear combination.

Example 2 Let $x, y \in Z_{2^{32}}$ and $z = xy \pmod{2^{32}}$; if

$$w = f(z) = z \oplus (z >>> 8) \oplus (z >>> 15),$$

then the outputs of z and w, as an S-box, have the same probability distributions (because f is a one to one correspondence), more precisely,

$$\forall a \in Z_{2^{32}}, \quad P(z = a) = P(w = f(a)).$$

But, according to Theorem 4, the probability distribution of component bits of w is closer to the uniform distribution than the probability distribution of z:

$$\left|P(w_i = 0) - \frac{1}{2}\right| \leq \left|P(z_i = 0) - \frac{1}{2}\right|, \quad 0 \leq i < 31.$$

In this example,

$$\max_{0 \leq i < 32} \{P(w_i = 0)\} = \frac{1}{2} + \frac{1}{2^{17}}.$$

5 Imbalance

In the design and analysis of (vectorial) Boolean functions, one of the important properties to be studied is balancedness. Clearly, M-functions are not balanced. In this section, we give a criterion for computing the imbalance of maps.

Definition 5 [5] If P_1, P_2 are two probability distributions on a finite sample space χ, their distance is defined as,

$$D(P_1, P_2) = \sum_{x \in \chi} |P_1(x) - P_2(x)|.$$

Now, for a function $f : A \to B$, with $|A| = n$, $|B| = m$ and $n = md$, consider the probability distribution P_1 on B as,

$$\forall b \in B,\ P_1(b) = \frac{\left|f^{-1}(b)\right|}{n}, \tag{5}$$

and consider P_2 the uniform distribution on B:

$$\forall b \in B \quad P_2(b) = \frac{d}{n} = \frac{1}{m}. \tag{6}$$

According to the above discussion, we define the imbalance of the function f based on the distance between the probability distribution defined in (5) and the uniform distribution (6).

Definition 6 For a function $f : A \to B$, with $|A| = n$, $|B| = m$ and $n = md$, the imbalance of f is defined as,

$$D_f = \frac{m}{2(m-1)} D(P_1, P_2) = \frac{\sum_{b \in B} \left|\left|f^{-1}(b)\right| - d\right|}{2(m-1)d}. \tag{7}$$

An easy calculation leads to the next lemma.

Lemma 1 *For a function $f : A \to B$, with $|A| = n$, $|B| = m$ and $n = md$, we have $0 \leq D_f \leq 1$. Moreover, $D_f = 0$ if and only if f is balanced and $D_f = 1$ if and only if f is a constant map.*

In the sequel, we calculate the imbalance of some vectorial Boolean functions extracted from the outputs of modular multiplication. We prove the theorem in general case.

Theorem 5 *Assume that $f : Z_2^m \times Z_2^m \to Z_2^m$ is an M-function; we have,*

$$D_f = \frac{2^{m-2}}{2^m - 1}.$$

Proof According to the Definition 6, Theorem 2, and equations

$$\begin{aligned} \textstyle\sum_{k=0}^{m-1} k2^{-k} &= \tfrac{2^m - m - 1}{2^{m-1}}, \\ \textstyle\sum_{k=0}^{m-1} k2^{k} &= 2(m2^{m-1} - 2^m + 1), \end{aligned} \tag{8}$$

we have,

$$D_f = \frac{\sum_{b \in Z_2^m} \left|\left|f^{-1}(b)\right| - 2^m\right|}{2(2^m - 1)2^m}$$

$$= \frac{m2^{m-1} + 2^{2m-2} + \sum_{k=1}^{m-1} \left(2^{m-k-1}\right)(k-1)2^{m-1}}{2(2^m-1)2^m}$$
$$= \frac{2^{m-2}}{2^m-1}.$$

Theorem 6 *Assume that $f : Z_2^m \times Z_2^m \to Z_2^m$ is an M-function with component Boolean functions $(f_{m-1}, \cdots, f_0)$; then for the i-th component function $f_i : Z_2^m \to Z_2$, we have,*

$$D_{f_i} = \frac{1}{2^{i+1}}.$$

Proof According to Corollary 2, we have,

$$\left|f_i^{-1}(0)\right| = 2^{2m}P(f_i = 0) = 2^{2m-1} + 2^{2m-i-2},$$
$$\left|f_i^{-1}(1)\right| = 2^{2m}P(f_i = 1) = 2^{2m-1} - 2^{2m-i-2};$$

and consequently,

$$D_{f_i} = \frac{\left|\left|f_i^{-1}(0)\right| - 2^{2m-1}\right| + \left|\left|f_i^{-1}(1)\right| - 2^{2m-1}\right|}{2(2-1)2^{2m-1}} = \frac{1}{2^{i+1}}.$$

Theorem 5 shows that the imbalance of the output of modular multiplication is a decreasing function of m, and has the lower bound $\frac{1}{4}$. Additionally, increasing m has not a powerful effect on its imbalance.
Theorem 6 shows that the component Boolean functions of modular multiplication with upper indices are nearly balanced functions.

Theorem 7 *Let f be an n-bit M-function and $z = f(x, y)$; for every $1 \le k \le m$, the imbalance of k upper bits of z $(w = z \gg (m-k))$ equals to*

$$D_k = \frac{2^{2k-m-2}}{2^k-1}.$$

Proof According to Theorem 3 and some easy calculations, for every $a \in Z_2^k$, we have,

$$P(w = a) = \frac{1}{2^k} + \frac{p(a)-1}{2^{m+1}}.$$

According to Definition 6, we have,

$$D_k = \frac{2^k}{2(2^k-1)} \sum_{a \in Z_2^k} \left| P(w = a) - \frac{1}{2^k} \right|. \tag{9}$$

On the other hand, for every $0 \le i < k$, there are 2^{k-i-1} many $a \in Z_2^k$ such that $p(a) = i$. So, using (7),

$$\sum_{a \in Z_2^k} \left| P(w = a) - \frac{1}{2^k} \right| = \frac{k}{2^{m+1}} + \sum_{a \in Z_2^k,\, a \neq 0} \left| \frac{p(a)-1}{2^{m+1}} \right|$$

$$= \frac{k}{2^{m+1}} + \sum_{i=0}^{k-1} 2^{k-i-1} \left| \frac{i-1}{2^{m+1}} \right| = \frac{2^k}{2^{m+1}}.$$

This ends the proof.

In Theorem 7, if we put $k = \frac{m}{2}$, then,

$$D_{\frac{m}{2}} = \frac{2^{-2}}{2^{\frac{m}{2}} - 1}.$$

This shows that in 32-bit or 64-bit microprocessors, the upper half of the modular multiplication is nearly balanced.

6 Conclusion

It is well-known (though not proved) that the upper bits of the output of modular multiplication have good statistical properties. In this paper, we proved this fact from some viewpoints: we showed that the upper bits of modular multiplication are asymptotically balanced in spite of the fact that the asymptotic imbalance of the output of this operator is $\frac{1}{4}$, based upon the measure we proposed. In addition, we computed the probability of all linear combinations of the the output of modular multiplication, which is important in linear cryptanalysis of symmetric ciphers that apply the mentioned operation in their design.

References

1. V. Anashin, Uniformly distributed sequences of p-adic integers, Math. Notes 55, 1994, 109-133.
2. C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, H. Sibert, Sosemanuk: a fast software-oriented stream cipher, ECRYPT-Network of Excellence in Cryptology, Call for stream cipher Primitives- Phase 2, 2005.
3. C. Burwick, D. Coppersmith, E. D. Avingnon, R. Gennaro, Sh.Halevi, Ch.Jutla, S. M. Matyas Jr., L. O. Connor, M.Peyravian, D. Safford, N. Zunic: MARS - a Candidate Cipher for AES, proceeding of 1st Advanced Encryption Standard Candidate Conference, Venture, California, Aug.20-22 1998.
4. Claude Carlet. Vectorial boolean functions for cryptography. In Y. Crama and P. Hammer, editors, Boolean Methods and Models. Cambridge University Press: http://www.math.univ-paris13.fr/ carlet/chap-vectorial-fcts-corr.pdf
5. T. M. Cover and J. A. Thomas, Elements of Information Theory, Second Edition, John Wiley and Sons, 2006.
6. A. Klimov, A. Shamir, A New Class of Invertible Mappings, Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2002.
7. A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad, S. M. Dehnavi, Hamidreza Maimani, Einollah Pasha, Statistical Properties of Modular Multiplication Modulo a Power of Two, 9th International Conference on Information Security and Cryptology (ISCISC12), University of Tabriz, Tabriz, Iran, 2012.
8. R. L. Rivest, M. J. B. Robshaw, R. Sidney, Y.L. Yin: The RC6 Block Cipher, Proceeding of 1st dvanced Encryption Standard Candidate Conference,Venture, California, Aug.20-22 1998.