Statistical Properties of the Square Map Modulo a Power of Two

S. M. Dehnavi[1], A. Mahmoodi Rishakani[2], M. R. Mirzaee Shamsabad[3], Einollah Pasha[4]

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

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

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

[4] *Kharazmi University, Faculty of Mathematical and Computer Sciences, Tehran, Iran: pasha@khu.ac.ir*

Abstract: The square map is one of the functions that is used in cryptography. For instance, the square map is used in Rabin encryption scheme, block cipher RC6 and stream cipher Rabbit, in different forms. In this paper we study a special case of the square map, namely the square function modulo a power of two. We obtain probability distribution of the output of this map as a vectorial Boolean function. We find probability distribution of the component Boolean functions of this map. We present the joint probability distribution of the component Boolean functions of this function. We introduce a new function which is similar to the function that is used in Rabbit cipher and we compute the probability distribution of the component Boolean functions of this new map.

Key Words: Square map modulo a power of two, Vectorial Boolean function, Component Boolean function, Rabbit cipher

1. Introduction

The square map, like the operator of multiplication, has various applications in cryptography. For instance in asymmetric cryptography, RSA encryption scheme [1] makes use of multiplication and Rabin encryption scheme [1] applies the square map. In symmetric cryptography, some symmetric ciphers have the operator of multiplication or the square map in their design. For example block cipher Mars [2] uses the operator of multiplication and in design of block cipher RC6 [3] the square map (the operator of multiplication) is used. In designing some stream ciphers, the operator of multiplication and the square map is also used. For instance, the stream cipher Sosemanuk [4] uses the operator of multiplication and the stream cipher Rabbit [5] uses the square map. In all the aforementioned cases the operator of multiplication and the

square map is used in a variety of methods. In this paper we investigate a special case of the square map, i.e. the square map modulo a power of two and we study probability distribution of this map along with its component Boolean functions. In [6,7] we have studied some statistical and algebraic properties of the operator of multiplication modulo a power of two, but in this paper we study statistical properties of the square map modulo a power of two.

At first we consider the square map modulo a power of two as a vectorial Boolean function [8] and we obtain probability distribution of its output. Then, we investigate component Boolean functions of this map and we obtain the probability distribution of these component functions. After that, we consider the joint probability distribution of these component functions for the case of two component functions and we compute the joint probability distribution of these component functions. We introduce a new function similar to what is presented in Rabbit cipher and using joint probability distribution of component Boolean functions of the square map, we obtain the probability distribution of component Boolean functions of this new function[1].

In Section 2 we present the definitions and notations. Section 3 studies probability distribution of the output of the square map modulo a power of two as a vectorial Boolean function. In Section 4 we investigate probability distribution of the component Boolean functions of square map modulo a power of two. In Section 5 we obtain the joint probability distribution of the component Boolean functions of square map modulo a power of two for the case of two component Boolean functions and finally in Section 6 we conclude.

2. Notations and Definitions

In this article, the number of elements or cardinality 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 denoted by $f^{-1}(b)$ and is defined as $\{a \in A | f(a) = b\}$. The greatest power of 2 that divides a natural number a is denoted by $p_2(a)$ and the odd part of a or $a/2^{p_2(a)}$ is denoted by $\mathcal{O}_2(a)$.

Let $\mathbb{F}_2$ be the finite field with two elements. Each element of $\mathbb{F}_2^n$ (The Cartesian product of n copies of $\mathbb{F}_2$) can be considered as a vector of length n. Each function $f: \mathbb{F}_2^n \to \mathbb{F}_2$ is called a Boolean function and each function $f: \mathbb{F}_2^n \to \mathbb{F}_2^m$ with $m > 1$ is called a vectorial Boolean function; such a function can be viewed as a vector $(f_{m-1}, \dots, f_0)$ of f_i's, $0 \leq i < m$. Here, f_i's are Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. These Boolean functions are called component Boolean functions of the vectorial Boolean function f. Also, if $x \in \mathbb{F}_2^n$, then the i-th bit of x is denoted by x_i. Note that for each vectorial Boolean function $f: \mathbb{F}_2^n \to \mathbb{F}_2^m$ we have vectorial Boolean functions

$$f_{i,j}: \mathbb{F}_2^n \to \mathbb{F}_2^2, \qquad i > j,$$

[1] This Paper is an English version of a paper with the same title (in Persian) presented in ISCISC'14.

$$f_{i,j}(x) = \Big(f_i(x), f_j(x)\Big), \quad x \in \mathbb{F}_2^n.$$

We call these vectorial Boolean functions *joint Boolean functions* of f.

In this paper, we consider the complete set of remainders modulo 2^n as $\{0,1,\dots,2^n-1\}$ and denote it by $\mathbb{Z}_{2^n}$. We define the inverse parity function e_j as follows:

$$e_j = \begin{cases} 0 & j \ \ odd, \\ 1 & j \ \ even. \end{cases}$$

Let $(G,*)$ be a group and $\varphi: G \to G$ be a group endomorphism; we denote the kernel of φ by $\ker(\varphi)$ and the image of φ by $Im(\varphi)$.

In the sequel, by the square map (and its component Boolean functions) we mean the square map modulo a power of two.

3. Probability Distribution of the Square Map as a Vectorial Boolean Function

In this section, we consider the square map as a vectorial Boolean function and we obtain probability distribution of the output of this map. In Theorem 1, we employ some facts from group theory [9] and number theory. One of the results of this theorem is identifying the square numbers modulo a power of two.

We note that the square of each odd natural number is in the form of $8k+1$, but not every natural number in the form of $8k+1$ is a square number. Lemma 1 shows that in $\mathbb{Z}_{2^n}$ the square of each odd element is in the form of $8k+1$; the interesting point is that, based on Theorem 1, in $\mathbb{Z}_{2^n}$ every element in the form of $8k+1$ is also a square element.

Lemma 1: Let $a \in \mathbb{Z}_{2^n}$ be an odd element; we have $a^2 = 1 \ mod\ 8$.

Proof: Since a is odd, so there exists a $q \in \mathbb{Z}_{2^n}$ such that $a = 2q+1 \ \ mod\ 2^n$. Therefore,

$$\begin{aligned} a^2 &= 4q(q+1)+1 \\ &= 8\left(\tfrac{q(q+1)}{2}\right) + 1 \ \ mod \ \ 2^n \\ &= 1 \ mod\ 8. \end{aligned}$$

■

Theorem 1: Suppose that $n > 4$ and $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is defined as $f(x) = x^2 \ \ mod \ \ 2^n$; then we have:

a) For the case $a = 0$, the case $a = 2^{n-1}$ with $e_n = 0$, and the case $a = 2^{n-2}$ with $e_n = 1$:

$$|f^{-1}(a)| = 2^{\frac{n-1+e_n}{2}};$$

b) For the case $p_2(a)\ mod\ 2 \neq 0$ and the case $p_2(a)\ mod\ 2 = 0$ with $0 \leq p_2(a) \leq n-3$ and $\mathcal{O}_2(a)\ mod\ 8 \neq 1$:

$$|f^{-1}(a)| = 0;$$

c) For the case $p_2(a)\ mod\ 2 = 0$ with $0 \leq p_2(a) \leq n-3$ and $\mathcal{O}_2(a)\ mod\ 8 = 1$:

$$|f^{-1}(a)| = 2^{\frac{p_2(a)+4}{2}}.$$

Proof: a) Consider the equation $x^2 = 0\ \ mod\ \ 2^n$; on one hand, every $x \in \mathbb{Z}_{2^n}$ with $p_2(x) \geq \left\lceil \frac{n}{2} \right\rceil$ satisfies $x^2 = 0\ \ mod\ \ 2^n$. So, $|f^{-1}(0)|$ is at least $2^{n-\left\lceil \frac{n}{2} \right\rceil} = 2^{\left\lfloor \frac{n}{2} \right\rfloor} = 2^{\frac{n-1+e_n}{2}}$. On the other hand, for each $x \in \mathbb{Z}_{2^n}$ with $p_2(x) < \left\lceil \frac{n}{2} \right\rceil$ we have $x^2 \neq 0\ \ mod\ \ 2^n$. Thus, $|f^{-1}(0)| = 2^{\frac{n-1+e_n}{2}}$.

Suppose that n is odd and $p_2(a) = n-1$. So a equals to 2^{n-1}. Consider the equation $x^2 = 2^{n-1}\ \ mod\ \ 2^n$; let $x = 2^r q$ with q odd. We have

$$2^{2r}q^2 = 2^{n-1}\ \ mod\ \ 2^n.$$

So $r = \frac{n-1}{2}$, $1 \leq q \leq 2^{\frac{n+1}{2}} - 1$ and $q^2 = 1\ mod\ 2$. Thus, only odd q's satisfy the equation $x^2 = 2^{n-1}\ \ mod\ \ 2^n$; therefore, $|f^{-1}(a)| = 2^{\frac{n-1}{2}} = 2^{\frac{n-1+e_n}{2}}$.

Now suppose that n is even and $p_2(a) = n-2$. So $p_2(a) = n-2$ and $a = s2^{n-2}$, where $s \in \{1,3\}$. If $s = 1$, then we consider the equation $x^2 = 2^{n-2}\ \ mod\ \ 2^n$. Let $x = 2^r q$ with q odd. We have

$$2^{2r}q^2 = 2^{n-2}\ \ mod\ \ 2^n.$$

Hence $r = \frac{n-2}{2}$, $1 \leq q \leq 2^{\frac{n+2}{2}} - 1$ and $q^2 = 1\ \ mod\ \ 4$. So only half of odd q's satisfy the equation $x^2 = 2^{n-1}\ \ mod\ \ 2^n$; therefore, $|f^{-1}(a)| = 2^{\frac{n}{2}} = 2^{\frac{n-1+e_n}{2}}$.

b) Continuing the proof of the Case **a**, if $s = 3$, then considering the equation $x^2 = 2^{n-2}.3\ \ mod\ \ 2^n$ and supposing that $x = 2^r q$ with q odd, we have

$$2^{2r}q^2 = 2^{n-2}.3\ \ mod\ \ 2^n;$$

so, $r = \frac{n-2}{2}$ and $q^2 = 3\ \ mod\ \ 4$. Thus, according to Lemma 1, we conclude that $|f^{-1}(a)| = 0$.

Suppose that $p_2(a) = 1\ \ mod\ \ 2$. Consider the equation $x^2 = a\ \ mod\ \ 2^n$. Since the square of any odd element is an odd element, so only even elements $x \in \mathbb{Z}_{2^n}$ can satisfy

$x^2 = a \ mod \ 2^n$. Suppose that $x = 2^r q$ where $r \neq 0$ and q is odd. We have $p_2(x^2) = 2r$ which contradicts $p_2(a) = 1 \ mod \ 2$. Therefore, $|f^{-1}(a)| = 0$.

Now suppose that $p_2(a) = 0 \ mod \ 2$ and $\mathcal{O}_2(a) \ mod \ 8 \neq 1$; then $a = 2^{2j}t$, where $p_2(a) = 2j$ and $t = \mathcal{O}_2(a)$. Consider the equation $x^2 = a \ mod \ 2^n$. Let $x = 2^r q$ with q odd. We have

$$2^{2r}q^2 = 2^{2j}t \ mod \ 2^n.$$

Consequently, $r = j$ and $q^2 = t \ mod \ 2^{n-2j}$; therefore, regarding Lemma 1, we have $|f^{-1}(a)| = 0$.

c) We use Theorem 13.3 in [9] to prove this case. Suppose that $p_2(a) = 0$ and $a = 1 \ mod \ 8$; the algebraic structure $(G,*)$, where G is the subset of odd elements in $\mathbb{Z}_{2^n}$ and $*$ is the operator of multiplication modulo 2^n is a group structure. The function $\phi: G \to G$ with $\phi(g) = g * g$ is a group endomorphism on G. To compute $|ker(\phi)|$ we must count the number of solutions for the equation $x * x = 1_G$. In other words, we must count the number of solutions for the equation $x^2 = 1 \ mod \ 2^n$. We have

$$(x-1)(x+1) = 0 \ mod \ 2^n.$$

Since x is odd, for some $q \in \mathbb{Z}_{2^n}$ we have $x = 2q + 1$. So,

$$4q(q+1) = 0 \ mod \ 2^n.$$

Consequently, we have $q = 0$, $q = 2^{n-2}$, $q = 2^{n-1}$ or $q + 1 = 2^{n-1}$, $q + 1 = 2^{n-2}$, $q + 1 = 2^{n-1}$. Substituting the values of q, we have these solutions:

$$x_1 = 1,$$

$$x_2 = 2^n - 1,$$

$$x_3 = 2^{n-1} + 1,$$

$$x_4 = 2^{n-1} + 1.$$

Thus, $|ker(\phi)| = 4$ and since $|Im(\phi)| = \frac{|G|}{|\ker(\phi)|}$, we have

$$|Im(\phi)| = \frac{2^{n-1}}{4} = 2^{n-3}.$$

On the other hand, according to Lemma 1 and since the number of elements in $\mathbb{Z}_{2^n}$ in the form of $8q + 1$ is equal to 2^{n-3} and $|Im(\phi)| = 2^{n-3}$, so every element in the form of $8q + 1$ in $\mathbb{Z}_{2^n}$ is a square element. Therefore, the equation $x^2 = a \ mod \ 2^n$ at least has a solution $x_1 = t$. It is not hard to verify that

$$x_2 = t.(2^n - 1) \ mod \ 2^n,$$

$$x_3 = t.(2^{n-1} - 1) \ mod \ 2^n,$$

and

$$x_4 = t.(2^{n-1} + 1) \ mod \ 2^n,$$

are the only other solutions for the equation. Consequently, we have

$$|f^{-1}(a)| = |ker(\phi)| = 4 = 2^{\frac{p_2(a)+4}{2}}.$$

Now suppose that $p_2(a) = 0 \ mod 2$ with $2 \leq p_2(a) \leq n-3$ and $\mathcal{O}_2(a) \ mod \ 8 = 1$. In this case, we have $a = 2^{2j}t$ with $p_2(a) = 2j$ and $t = \mathcal{O}_2(a)$. Consider the equation $x^2 = a \ mod \ 2^n$. Let $x = 2^r q$ with q odd. We have

$$2^{2r}q^2 = 2^{2j}t \ mod \ 2^n;$$

so, $r = j$ and $q^2 = t \ mod \ 2^{n-2j}$. Regarding Lemma 1 and the proof of Case **b**, this equation has four solutions with $0 \leq q \leq 2^{n-2j} - 1$. For each of these solutions we present 2^j solutions

$$x = 2^j\left(s2^{n-2j+1} + q\right), \quad 0 \leq s \leq 2^j - 1.$$

We have

$$\begin{aligned} x^2 &= 2^{2j}\left(s^2 2^{2n-4j+2} + q^2 + 2sq2^{n-2j+1}\right) \\ &= s^2 2^{2n-2j+2} + 2^{2j}q^2 + sq2^{n+2} \\ &= 2^{2j}q^2 \ \ mod \ \ 2^n. \end{aligned}$$

In fact, regarding the inequality $2j \leq n-3$, we have $2n - 2j \geq n + 3$. Thus,

$$|f^{-1}(a)| = 2^{\frac{p_2(a)}{2}+2} = 2^{\frac{p_2(a)+4}{2}}. \qquad \blacksquare$$

4. Probability Distribution of Component Boolean Functions of the Square Map

In this section, we study the component Boolean functions of square map and we find the probability distribution of these component functions. Theorem 2 has been proved in [10] with the help of some concepts in T-function theory. Here, we reprove this theorem using Theorem 1.

Theorem 2: Suppose that $n > 4$ and the function $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is defined as $z = f(x) = \ x^2 \ mod \ 2^n$; then we have

$$P(z_i = 0) = \begin{cases} \frac{1}{2} & i = 0 \\ \frac{1}{2} + 2^{-\left\lfloor \frac{i+2}{2} \right\rfloor} & 1 \le i < n \end{cases}$$

Proof: The cases $i = 0,1$ are obvious. Suppose that $1 < i < n-2$ and i is odd; the number of elements a with $p_2(a) = 2j$ is equal to 2^{n-2j-1} and the number of a's with $p_2(a) = 2j$ and $\mathcal{O}_2(a)\ mod\ 8 \neq 1$ is equal to 2^{n-2j-3}. By Theorem 1,

$$P(z_i = 1) = \sum_{\substack{0 \le p_2(a) < i \\ p_2(a)\ mod\ 2 = 0 \\ a_i = 1}} \frac{|f^{-1}(a)|}{2^n}$$

$$= \sum_{j=0}^{\frac{i-3}{2}} \frac{2^{n-2j-3} 2^{j+2}}{2^n . 2}$$

$$= \frac{1}{2}\left(1 - 2^{-\frac{i-1}{2}}\right)$$

$$= \tfrac{1}{2} - 2^{-\left\lfloor \frac{i+2}{2} \right\rfloor}.$$

Suppose that $1 < i < n-2$ and i is even; the number of elements a with $p_2(a) = 2j$ is equal to 2^{n-2j-1} and the number of a's with $p_2(a) = 2j$ and $\mathcal{O}_2(a)\ mod\ 8 \neq 1$ is equal to 2^{n-2j-3}. By Theorem 1,

$$P(z_i = 1) = \sum_{\substack{0 \le p_2(a) < i \\ p_2(a)\ mod\ 2 = 0 \\ a_i = 1}} \frac{|f^{-1}(a)|}{2^n}$$

$$= \sum_{j=0}^{\frac{i-1}{2}} \frac{2^{n-2j-3} 2^{j+2}}{2^n . 2}$$

$$= \tfrac{1}{2}\left(1 - 2^{-\frac{i}{2}}\right)$$

$$= \tfrac{1}{2} - 2^{-\left\lfloor \frac{i+2}{2} \right\rfloor}.$$

Now suppose that $i = n-2$ and i is even; we have

$$P(z_{n-2}=1)=\sum_{\substack{0\le p_2(a)<n-2\\ p_2(a)\ mod\ 2=0\\ a_{n-2}=1}}\frac{|f^{-1}(a)|}{2^n}$$

$$=\frac{|f^{-1}(2^{n-2})|}{2^n}+\sum_{j=0}^{\frac{n-6}{2}}\frac{2^{n-2j-3}2^{j+2}}{2^n.2}$$

$$=\frac{1}{2}-\frac{1}{2^{\frac{n}{2}}}$$

$$=\frac{1}{2}-2^{-\left\lfloor\frac{i+2}{2}\right\rfloor}.$$

Now if $i=n-2$ and i is odd, then we have

$$P(z_{n-2}=1)=\sum_{\substack{0\le p_2(a)<n-2\\ p_2(a)\ mod\ 2=0\\ a_{n-2}=1}}\frac{|f^{-1}(a)|}{2^n}$$

$$=\sum_{j=0}^{\frac{n-5}{2}}\frac{2^{n-2j-3}2^{j+2}}{2^n.2}$$

$$=\frac{1}{2}-2^{-\left\lfloor\frac{i+2}{2}\right\rfloor}.$$

Now if $i=n-1$ and i is even, then we have

$$P(z_{n-1}=1)=\sum_{\substack{0\le p_2(a)<n-1\\ p_2(a)\ mod\ 2=0\\ a_{n-1}=1}}\frac{|f^{-1}(a)|}{2^n}$$

$$=\sum_{j=0}^{\frac{n-3}{2}}\frac{2^{n-2j-3}2^{j+2}}{2^n.2}$$

$$=\frac{1}{2}-2^{-\left\lfloor\frac{i+2}{2}\right\rfloor}.$$

Finally, if $i=n-1$ and i is odd, then we have

$$P(z_i = 1) = \sum_{\substack{0 \le p_2(a) < i \\ p_2(a)\ mod\ 2 = 0 \\ a_i = 1}} \frac{|f^{-1}(a)|}{2^n}$$

$$= \sum_{j=0}^{\frac{n-4}{2}} \frac{2^{n-2j-3} 2^{j+2}}{2^n . 2}$$

$$= \frac{1}{2} - 2^{-\left\lfloor \frac{i+2}{2} \right\rfloor}$$ ■

5. Joint Probability Distribution of Component Boolean Functions of the Square Map

In this section, we investigate the joint component Boolean functions of square map and we obtain the joint probability distribution of these component functions. Then, using these distributions, we introduce a new map similar to what is presented in Rabbit cipher and we find the probability distribution of component Boolean functions of this new map.

Theorem 3: Suppose that $n > 4$ and the function $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is defined as $z = f(x) = x^2 \ mod\ 2^n$; we have:

a) For $j + 2 < i$,

$$P(z_i = b, z_j = a) = \begin{cases} \frac{1}{4} + \frac{(-1)^a}{2^{\left\lfloor \frac{j}{2} \right\rfloor + 2}} + (1 - a)\frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}} & j \neq 0, \\ \frac{1}{4} + (1 - a)\frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}} & j = 0. \end{cases}$$

b) For $j < i \le j + 2$ with $j > 2$,

$$P(z_i = b, z_j = a) = \frac{1}{4} - \frac{1}{2^{\left\lfloor \frac{j+3}{2} \right\rfloor}} + \frac{e_j(a \oplus b)}{2^{\left\lfloor \frac{j+2}{2} \right\rfloor}} + \frac{e_a}{2^{\left\lfloor \frac{j+2}{2} \right\rfloor}} + \frac{e_a(-1)^b}{2^{\left\lfloor \frac{i+2}{2} \right\rfloor}}.$$

c) For the other cases,

$$P(z_i = b, z_j = a) = \begin{cases} \frac{1}{4} + (1 - e_a e_{i+j})\frac{(-1)^b}{4} & j = 0, i = 1,2 \\ (1-a)\left(\frac{1}{2} + \frac{(-1)^b}{4}\right) & j = 1, i = 2,3 \\ \frac{1}{2^{a+1}} - \frac{b}{4} & j = 2, i = 3 \\ \frac{3e_a}{8} + \frac{ae_b}{4} & j = 2, i = 4. \end{cases}$$

(These probabilities for $n \leq 4$ is also presented in the Appendix.)

Proof: At first, suppose that $j \neq 0$ is even; or $j = 2r, r > 0$. We have

$$P(z_i = b, z_{2r} = 1) = \sum_{c_i = b, c_{2r} = 1} P(z = c) = \sum_{\substack{0 \leq p_2(c) \leq 2r \\ p_2(c) \bmod 2 = 0 \\ c_i = b, c_{2r} = 1}} P(z = c). \quad (1)$$

In summation (1), if $p_2(c) = 2k$, $0 \leq k \leq r-2$, then binary representation of c is in this form:

$$c = \left(*, \dots, *, \underbrace{b}_{i}, *, \dots, *, \underbrace{1}_{2r}, *, \dots, *, \underbrace{0}_{2k+2}, \underbrace{0}_{2k+1}, \underbrace{1}_{2k}, 0, \dots, 0\right).$$

Consequently, $2k + 5$ bits are determined and so we have 2^{n-2k-5} nonzero summands, the probability of each is equal to $\frac{2^{\frac{p_2(c)+4}{2}}}{2^n}$, by Theorem 1. Thus, the contribution of this case in (1) is equal to $2^{-(k+3)}$. We note that the case $k = r-1$ contradicts Theorem 1. For the case $k = r$, $2r + 4$ bits are determined, and so we have 2^{n-2r-4} nonzero summands, the probability of each equals to $\frac{2^{\frac{p_2(c)+4}{2}}}{2^n}$ by Theorem 1. Therefore, the contribution of this case in (1) is equal to $2^{-(r+2)}$. Hence,

$$P(z_i = b, z_{2r} = 1) = \left(\sum_{k=0}^{r-2} 2^{-(k+3)}\right) + 2^{-(r+2)}$$

$$= \frac{1}{4} - \frac{1}{2^{r+2}}. \quad (2)$$

Now, using basic probability theory and Theorem 2 and (2), we have

$$P(z_i = b, z_{2r} = 0) = 1 - P(z_i = b \oplus 1) - P(z_{2r} = 1) + P(z_i = b \oplus 1, z_{2r} = 1)$$

$$= \frac{1}{4} + \frac{1}{2^{r+2}} + \frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}}.$$

So,

$$P(z_i = b, z_{2r} = a) = \frac{1}{4} + \frac{(-1)^a}{2^{r+2}} + (1-a)\frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}}.$$

At this point, suppose that $j \neq 0$ is odd; i.e. $j = 2r + 1, r \geq 0$. We have

$$P(z_i = b, z_{2r+1} = 1) = \sum_{c_i = b, c_{2r+1} = 1} P(z = c)$$

$$= \sum_{\substack{0 \leq p_2(c) \leq 2r+1 \\ p_2(c) \ mod \ 2 = 0 \\ c_i = b, c_{2r+1} = 1}} P(z = c). \quad (3)$$

In (3), according to Theorem 1, $p_2(c)$ can be $0, 2, \ldots, 2r - 2$. Similar to the previous case,

$$P(z_i = b, z_{2r+1} = 1) = \frac{1}{4} - \frac{1}{2^{r+2}},$$

and

$$P(z_i = b, z_{2r+1} = 0) = \frac{1}{4} + \frac{1}{2^{r+2}} + \frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}}.$$

So,

$$P(z_i = b, z_{2r+1} = a) = \frac{1}{4} + \frac{(-1)^a}{2^{r+2}} + (1-a)\frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}}.$$

Thus, in the case $j \neq 0$, we have

$$P\big(z_i = b, z_j = a\big) = \frac{1}{4} + \frac{(-1)^a}{2^{\left\lfloor \frac{j}{2} \right\rfloor + 2}} + (1-a)\frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}}.$$

Now, suppose that $j = 0$:

$$P(z_i = b, z_0 = 1) = \sum_{c_i = b, c_0 = 1} P(z = c)$$

$$= \sum_{p_2(c) = 0, c_i = b} P(z = c). \quad (4)$$

In (4), four bits are determined and so we have 2^{n-4} summands, the probability of each is equal to $\frac{2^2}{2^n}$ by Theorem 1. Hence,

$$P(z_i = b, z_0 = 1) = 2^{n-4}.\frac{2^2}{2^n} = \frac{1}{4},$$

and similarly,

$$P(z_i = b, z_0 = 0) = 1 - P(z_i = b \oplus 1) - P(z_0 = 1) + P(z_i = b \oplus 1, z_0 = 1)$$

$$= \frac{1}{4} + \frac{(-1)^b}{2^{\left\lfloor \frac{i+2}{2} \right\rfloor}}.$$

So, for the case $j = 0$, we have

$$P(z_i = b, z_0 = a) = \frac{1}{4} + (1-a)\frac{(-1)^b}{2^{\left\lfloor \frac{i}{2} \right\rfloor + 1}}.$$

b) For $2 < j$ and $i = j + 1$ or $= j + 2$, we have

$$P\big(z_i = b, z_j = 1\big) = \sum_{c_i = b, c_j = 1} P(z = c)$$

$$= \sum_{\substack{0 \le p_2(c) \le 2\left\lfloor \frac{j}{2} \right\rfloor \\ p_2(c) \bmod 2 = 0 \\ c_i = b, c_j = 1}} P(z = c).$$

According to the proof of Case **a** and regarding the binary representation of *c*, for the even and odd cases of *j*, we have

$$P\big(z_i = b, z_j = 1\big) = 2^{n-5}\frac{2^2}{2^n} + 2^{n-7}\frac{2^3}{2^n} + \cdots + 2^{n-\left(2\left\lfloor \frac{j+1}{2} \right\rfloor + 1\right)}\frac{2^{\left\lfloor \frac{j+1}{2} \right\rfloor}}{2^n} + e_j e_b 2^{n-(j+3)}\frac{2^{\frac{j+4}{2}}}{2^n}$$

$$= \frac{1}{4} - \frac{1}{2^{\left\lfloor \frac{j+3}{2} \right\rfloor}} + \frac{e_j e_b}{2^{\frac{j+2}{2}}}.$$

and

$$P\big(z_i = b, z_j = 0\big) = 1 - \Big(P(z_i = b \oplus 1) + P\big(z_j = 1\big) - P\big(z_i = b \oplus 1, z_j = 1\big)\Big)$$

$$= \frac{1}{4} + \frac{2^{\left\lfloor \frac{j+3}{2} \right\rfloor} - 2^{\left\lfloor \frac{j+2}{2} \right\rfloor}}{2^{j+2}} + \frac{(-1)^b}{2^{\left\lfloor \frac{i+2}{2} \right\rfloor}} + \frac{be_j}{2^{\frac{j+2}{2}}}.$$

So, for $j < i \leq j + 2$ and $j > 2$, we have

$$P(z_i = b, z_j = a) = \frac{1}{4} - \frac{1}{2^{\left\lfloor \frac{j+3}{2} \right\rfloor}} + \frac{e_j(a \oplus b)}{2^{\frac{j+2}{2}}} + \frac{e_a}{2^{\left\lfloor \frac{j+2}{2} \right\rfloor}} + \frac{e_a(-1)^b}{2^{\left\lfloor \frac{i+2}{2} \right\rfloor}}.$$

c) All the cases are simple. ■

Now, we introduce a new function similar to what is presented in stream cipher Rabbit and we obtain the probability distribution of its component Boolean functions.

Theorem 4: Suppose that $n \geq 8$ is an even natural number, the function $f: \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ is defined as $z = f(x) = x^2 \ mod \ 2^n$ and $w = g(x) = x^2 \oplus (x^2 \gg \frac{n}{2}) \ mod \ 2^n$. Here, $\gg$ is the bitwise right shift operator and $\oplus$ means the bitwise XOR. We have

$$P(w_i = 0) = \frac{1}{2} + 2^{-\left| \frac{i}{2} + \frac{n}{4}\left(1 - \left\lfloor \frac{2i}{n} \right\rfloor\right) \right|}, \qquad 0 \leq i < n.$$

Proof: According to Theorem 3, we have

$$\begin{aligned} P(w_0 = 0) &= P(z_0 \oplus z_{n/2} = 0) \\ &= P(z_0 = 0, z_{n/2} = 0) + P(z_0 = 1, z_{n/2} = 1) \\ &= \frac{1}{2} + 2^{-\left\lfloor \frac{n+4}{4} \right\rfloor}, \end{aligned}$$

and for $0 < i < \frac{n}{2}$,

$$\begin{aligned} P(w_i = 0) &= P(z_i \oplus z_{i+(n/2)} = 0) \\ &= P(z_i = 0, z_{i+(n/2)} = 0) + P(z_i = 1, z_{i+(n/2)} = 1) \\ &= \frac{1}{2} + 2^{-\left\lfloor \frac{2i+n+4}{4} \right\rfloor}. \end{aligned}$$

For $\geq \frac{n}{2}$, according to Theorem 2, we have

$$P(w_i = 0) = \frac{1}{2} + 2^{-\left\lfloor \frac{2i+n+4}{4} \right\rfloor}.$$

Therefore,

$$P(w_i = 0) = \frac{1}{2} + 2^{-\left| \frac{i}{2} + \frac{n}{4}\left(1 - \left\lfloor \frac{2i}{n} \right\rfloor\right) \right|}.$$

■

References

[1] D.R. STINSON, “Cryptography - Theory and Practice”, 3rd edn. Chapman & Hall/CRC, Boca Raton, 2003.

[2] 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.

[3] R. L. Rivest, M. J. B. Robshaw, R. Sidney, Y.L. Yin: “The RC6 Block Cipher”, Proceeding of 1st Advanced Encryption Standard Candidate Conference, Venture, California, Aug. 20-22 1998.

[4] C. Berbain, O. Billet, A. Canteaut, N. Courtois, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Pornin, and H. Sibert, “*Sosemanuk, a Fast Software-Oriented Stream Cipher”*, submitted to Ecrypt, 2005.

[5] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, and O. Scavenius, “Rabbit: A New High-Performance Stream Cipher”, in *Fast Software Encryption (FSE’03)*, LNCS 2887, pp. 307-329, Springer-Verlag, 2003.

[6] 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 (ISCISC’12), University of Tabriz, Tabriz, Iran, 2012

[7] S. M. Dehnavi, A. Mahmoodi Rishakani, M. R. Mirzaee Shamsabad, Einollah Pasha, “Cryptographic Properties of Modular Multiplication Modulo a Power of Two”, Kharazmi Journal of Science, **No**. 12-1, **pp**. 327-338, 2013 (In Persian)

[8] Claude Carlet, “Boolean functions for Cryptography and Error Correcting Codes”, available via http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.107.2986&rep=rep1&type=pdf

[9] J. B. Fraleigh. “A First Course in Abstract Algebra”, Sixth edition, ADDISON-WESLEY publishing company Inc, 1999.

[10] A. Klimov and A. Shamir, “A New Class of Invertible Mappings,” Workshop on Cryptographic Hardware and Embedded Systems (CHES), 2002.

Appendix

In the following tables, the probability corresponding to the i-th column and the j-th row is equal to $P(z_i = b, z_j = a)$.

$a = 0$ $b = 0$	0	1	2	3
0	–	$1/2$	$1/4$	$1/2$
1	–	–	$3/4$	$3/4$
2	–	–	–	$1/2$

$a = 0$ $b = 1$	0	1	2	3
0	–	0	$1/4$	0
1	–	–	$1/4$	$1/4$
2	–	–	–	$1/4$

$a = 1$ $b = 0$	0	1	2	3
0	–	$1/2$	$1/2$	$1/4$
1	–	–	0	0
2	–	–	–	$1/4$

$a = 1$ $b = 1$	0	1	2	3
0	–	0	0	$1/4$
1	–	–	0	0
2	–	–	–	0