

# A More Explicit Formula for Linear Probabilities of Modular Addition Modulo a Power of Two

S. M. Dehnavi<sup>1</sup>, A. Mahmoodi Rishakani<sup>2</sup>, M. R. Mirzaee Shamsabad<sup>3</sup>

<sup>1</sup> Kharazmi University, Faculty of Mathematical and Computer Sciences, Tehran, Iran  
std\_dehnavism@khu.ac.ir

<sup>2</sup> Shahid Rajaee Teacher Training University, Faculty of Sciences, Tehran, Iran  
am.rishakani@srttu.edu

<sup>3</sup> Shahid Bahonar University, Faculty of Mathematics and Computer Science, Kerman, Iran  
mohammadmirzaeesh@yahoo.com

**Abstract:** Linear approximations of modular addition modulo a power of two was studied by Wallen in 2003. He presented an efficient algorithm for computing linear probabilities of modular addition. In 2013 Schulte-Geers investigated the problem from another viewpoint and derived a somewhat explicit formula for these probabilities. In this note we give a closed formula for linear probabilities of modular addition modulo a power of two, based on what Schulte-Geers presented: our closed formula gives a better insight on these probabilities and more information can be extracted from it.

**Key Words:** Modular addition modulo a power of two, Linear probability, Symmetric cipher, Linear cryptanalysis

## 1. Introduction

Linear cryptanalysis is a strong tool in cryptanalysis of symmetric ciphers. In [1] linear approximations of modular addition modulo a power of two is investigated and an efficient algorithm for computing these probabilities is given. A somewhat explicit formula for linear probabilities of this operator is also given in [2]. In this note, we propose a closed formula for linear probabilities of modular addition modulo a power of two based on the algorithm presented in [2]. Our closed formula exhibits a better insight for these probabilities and more information can be derived from it.

In this note, we use the following notations:

$w(x)$ : Hamming weight of a binary vector  $x = (x_{n-1}, \dots, x_0)$ ,

$\cdot$ : Standard dot product,

$\oplus$ : Bitwise XOR operator,

$|B|$ : Number of symbols in a block  $B$ ,

$\bar{\alpha}$ : Complement of a bit  $\alpha$ ,

$o$ -block: A block of symbols 1,2 or 4,

$e$ -block: A block of symbols 3,5 or 6,

0-block: A block of symbol 0,

7-block: A block of symbol 7,

$[cond]$ : 1 if  $cond = true$  and 0 otherwise.

## 2. A Closed Formula for Linear Probabilities of Modular Addition

Suppose that the input masks  $(a_{n-1}, \dots, a_0)$  and  $(b_{n-1}, \dots, b_0)$  and the output mask  $(c_{n-1}, \dots, c_0)$  are given. We wish to compute

$$\left| P(a \cdot x \oplus b \cdot y = c \cdot r) - \frac{1}{2} \right|, \quad (1)$$

where

$$r = x + y \text{ mod } 2^n,$$

$x = (x_{n-1}, \dots, x_0)$ ,  $y = (y_{n-1}, \dots, y_0)$  and  $r = (r_{n-1}, \dots, r_0)$ . To compute (1), we recall the algorithm presented in [2]: put

$$s_i = a_{n-1-i} \oplus b_{n-1-i} \oplus c_{n-1-i}, \quad 0 \leq i < n.$$

Now put  $z_0 = 0$  and

$$z_{i+1} = z_i \oplus s_i, \quad 0 \leq i < n - 1.$$

The bias (1) is zero if there exists an  $0 \leq i < n$  such that  $z_i = 0$  holds and  $a_i = b_i = c_i$  does not hold. Otherwise, we have

$$\left| P(a \cdot x \oplus b \cdot y = c \cdot r) - \frac{1}{2} \right| = 2^{-(w(z)+1)}, \quad z = (z_{n-1}, \dots, z_0).$$

We can reformulate the above algorithm in this form: put

$$S_i = a_{n-1-i} + 2b_{n-1-i} + 4c_{n-1-i}, \quad 0 \leq i < n.$$

So we have a sequence  $S_0, \dots, S_{n-1}$  of symbols in  $\{0, \dots, 7\}$ . Is not hard to see that (1) can be computed by means of the (informal) automata of Picture 1. We begin by state 0 in the automata and traverse the diagram symbol by symbol. If we meet “halt” then (1) is equal to zero, and otherwise (1) is equal to  $2^{-w}$ . We illustrate our algorithm through some examples:

**Example 1.** Let  $n = 9$  and

$$(a_8, \dots, a_0) = (0, 1, 1, 0, 1, 1, 1, 0, 0),$$

$$(b_8, \dots, b_0) = (0, 1, 1, 0, 1, 1, 0, 0, 0),$$

$$(c_8, \dots, c_0) = (0, 1, 1, 0, 1, 0, 1, 0, 1).$$

Then we have

$$S_0 \dots S_8 = 077073504.$$

Traversing the diagram, we get the bias  $2^{-5}$ .

**Example 2.** Let  $n = 11$  and

$$(a_{10}, \dots, a_0) = (0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1),$$

$$(b_{10}, \dots, b_0) = (0, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1),$$

$$(c_{10}, \dots, c_0) = (0, 0, 1, 1, 1, 0, 0, 1, 0, 1, 1).$$

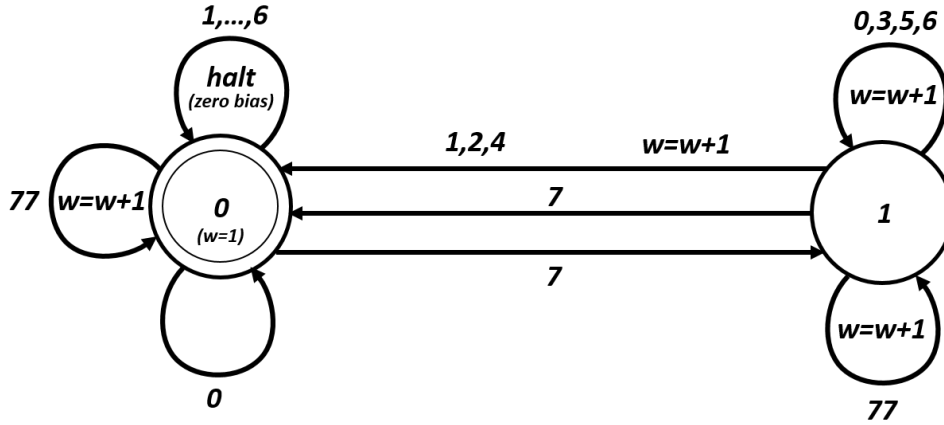
Then we have

$$S_0 \dots S_{10} = 00777015267.$$

Traversing the diagram, we get the bias 0.

In the appendix we have presented a pseudo-code for computing (1). It can be easily checked that the algorithm is very fast.

With the aid of Picture (1) which is by itself derived from [2], the proof of following theorem is straightforward:



Picture 1

**Theorem 1.** Notations as before, let

$$S_0, \dots, S_{n-1} = B_1 \dots B_m.$$

Here,  $B_i$ 's,  $1 \leq i \leq m$ , are  $o$ -blocks,  $e$ -blocks,  $0$ -blocks or  $7$ -blocks. Define  $\alpha_1 = 0$  and for  $1 < i \leq m$

$$\alpha_i = \begin{cases} 1 & \# \{B_j: 1 \leq j < i, B_j \text{ is } 7\text{-block of odd length}\} + \# \{B_j: 1 \leq j < i, B_j \text{ is } o\text{-block}\} \text{ is odd,} \\ 0 & \# \{B_j: 1 \leq j < i, B_j \text{ is } 7\text{-block of odd length}\} + \# \{B_j: 1 \leq j < i, B_j \text{ is } o\text{-block}\} \text{ is even.} \end{cases}$$

Then (1) is equal to

$$\frac{q}{2^w},$$

where

$$q = \prod_{i=1}^m (1 - \bar{\alpha}_i [B_i \text{ is } o\text{-block or } e\text{-block}]),$$

and

$$w = 1 + \sum_{B_i \text{ is } o\text{-block or } e\text{-block}} |B_i| + \sum_{B_i \text{ is } 7\text{-block}} \frac{|B_i|}{2} + \sum_{B_i \text{ is } 0\text{-block}} \alpha_i |B_i|.$$

We state some of the direct consequences of Theorem 1 here:

- If (1) is not zero, then we cannot see a symbol in  $\{1,2,4\}$  followed by some blocks which are not 7-blocks followed by a symbol in  $\{1, \dots, 6\}$ : as a special case, there cannot be a symbol in  $\{1,2,4\}$  before a symbol in  $\{1, \dots, 6\}$ .
- If (1) is not zero, then it is less than or equal to  $2^{-(d+1)}$  where  $d$  is the total number of symbols in  $\{1, \dots, 6\}$ .
- If (1) is not zero, then there are (at least)  $3^f 4^g - 1$  other sequences with the same probability, where

$$f = \sum_{B_i \text{ is } o\text{-block or } e\text{-block}} |B_i|,$$

$$g = \sum_{B_i \text{ is } 0\text{-block}} \alpha_i |B_i|.$$

- If (1) is zero, then there are (at least)  $3^f 4^g - 1$  other sequences with zero bias, where

$$f = \sum_{B_i \text{ is } o\text{-block or } e\text{-block}} |B_i|,$$

$$g = \sum_{B_i \text{ is } 0\text{-block}} |B_i|.$$

## References

- [1] Johan Wallén: Linear Approximations of Addition Modulo  $2^n$ . FSE 2003: 261-273
- [2] Ernst Schulte-Geers: On CCZ-equivalence of addition mod  $2^n$ . Des. Codes Cryptography 66(1-3): 111-127 (2013)

## Appendix

**Input:**  $S[0], \dots, S[n-1]$

**Output:** halt (zero bias) or  $w$  (value of the exponent)

$i=0, s=0, w=1$

```
while (i<n) do
  index=i
  j=0
  if (S[index]=7)
    while (S[i]=7)
      j=j+1
      i=i+1
    end (while)
    if (j is odd) s=1-s
    w = w + (j div 2)
  else if (S[index]=0)
    i=i+1
    if (s=1) w=w+1
  else if (S[index] is in {1,2,4})
    if (s=0) halt
    s=1-s
    w=w+1
    i=i+1
  else if (S[index] is in {3,5,6})
    if (s=0) halt
    else
      w=w+1
      i=i+1
    end (if)
  end (if)
end (while)
```