Linear Approximations of Addition Modulo 2^n-1 *

Chunfang Zhou[1,2], Xiutao Feng[1], Chuankun Wu[1]

[1] State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, 100190, China.
[2] Graduate University of the Chinese Academy of Science, Beijing, 100049, China.
{cfzhou, fengxt, ckwu}@is.iscas.ac.cn

Abstract. Addition modulo $2^{31} - 1$ is a basic arithmetic operation in the stream cipher ZUC. For evaluating ZUC's resistance against linear cryptanalysis, it is necessary to study properties of linear approximations of the addition modulo $2^{31} - 1$. In this paper we discuss linear approximations of the addition of k inputs modulo $2^n - 1$ for $n \geq 2$. As a result, an explicit expression of the correlations of linear approximations of the addition modulo $2^n - 1$ is given when $k = 2$, and an iterative expression when $k > 2$. For a class of special linear approximations with all masks being equal to 1, we further discuss the limit of their correlations when n goes to infinity. It is shown that when k is even, the limit is equal to zero, and when k is odd, the limit is bounded by a constant depending on k.

Key words: Linear approximation, modular additions, linear cryptanalysis.

1 Introduction

Linear cryptanalysis [1] is one of the most powerful and general cryptanalytic methods. Its main task is to find linear relations between the inputs and outputs of target functions. In block ciphers, we usually find some linear relations among keys, plaintexts and ciphertexts that hold with certain probability. If some plaintext/ciphertext pairs are known, some bits of the key can be recovered with high probability [1, 2]. In stream ciphers, linear cryptanalysis is usually combined with distinguishing cryptanalysis together, and its goal is to establish a linear distinguisher to distinguish the keystream generated by the target algorithm from a random sequence [3, 4].

For both block ciphers and stream ciphers, it is important to find an efficient method to evaluate their resistance against linear cryptanalysis. Most cryptographic algorithms are usually designed by composing distinct and well chosen components and operations. Hence we should calculate linear approximations of those components or operations. The addition modulo 2^n, especially when

* This work was supported by the Natural Science Foundation of China (Grant No. 60833008 and 60902024) and the National 973 Program (Grant No. 2007CB807902).

n is equal to the length of a computer word, e.g., 8, 16 or 32, is one of the most common operations, and is widely used in the design of cryptographic algorithms [5–8]. Many results on the addition modulo 2^n have been obtained, see [9–15].

The addition modulo $2^n - 1$ is another important arithmetic operation [16, 17]. Some properties of the addition modulo 2^n-1 have been explored in [18, 19]. However few results on linear approximations on the addition modulo 2^n-1 can be found from public literature. Recently a new stream cipher named ZUC [20], together with 128-EEA3 and 128-EIA3, has been proposed as the third suite of LTE encryption and integrity candidates, see [21] for details. In ZUC, the addition modulo $2^{31}-1$ is a basic operation since the linear feedback shift register (LFSR) of ZUC is defined over the prime field $\mathbb{F}_{2^{31}-1}$. For evaluating ZUC's resistance against linear cryptanalysis, it is necessary to study the properties of linear approximations of the addition modulo $2^{31} - 1$. In this paper, by means of known results on the addition modulo 2^n, we directly derive an expression for the correlations of arbitrary linear approximations of the addition modulo 2^n-1 with two inputs. For the case where more than two inputs are involved, we give an iterative expression. Moreover, for a class of special linear approximations with all masks being equal to 1, we discuss the limit of their correlations when n goes to infinity. Let k be the number of inputs of the addition modulo $2^n - 1$. It is shown that when k is even, the limit is equal to zero, and when k is odd, the limit is a constant depending on k.

The rest of the paper is organized as follows: in section 2, we give the definitions of linear approximations and their correlations and recall some properties of the addition modulo 2^n briefly. In section 3 some basic properties of linear approximation of the addition modulo $2^n - 1$ are given, and more properties for the case $k = 2$ are given in section 4. In section 5 we further discuss the limit of linear approximations with all masks being equal to 1. Finally we conclude in section 6.

2 Preliminaries

2.1 Linear approximation and its correlation

Let n be a positive integer. Denote Z_{2^n} the set of integers x such that $0 \le x \le 2^n - 1$. Given an integer $x \in Z_{2^n}$, let

$$x = x^{(n-1)}x^{(n-2)}\cdots x^{(0)} = \sum_{i=0}^{n-1} x^{(i)}2^i$$

be the binary representation of x, where $x^{(i)} \in \{0, 1\}$. We call $x^{(i)}$ the i-th bit of x, $0 \le i \le n - 1$. In the rest of the paper, without further specification, we always denote by $x^{(i)}$ the i-th bit of the integer x in its binary representation. For arbitrary two integers $w, x \in Z_{2^n}$, the inner product of w and x is defined

as

$$w \cdot x = \bigoplus_{i=0}^{n-1} w^{(i)} x^{(i)}.$$

Let J be a nonempty subset of Z_{2^n}, k be a positive integer and f be a function from J^k to J. Given $k+1$ constants $u, w_1, \cdots, w_k \in Z_{2^n}$, the linear approximation of the function f associated with $u, w_1, \cdots, w_k$ is an approximate relation of the form

$$u \cdot f(x_1, \cdots, x_k) = \bigoplus_{i=1}^{k} w_i \cdot x_i, \tag{1}$$

and the $(k+1)$-tuple $(u, w_1, \cdots, w_k)$ is called a *linear mask* of f. The efficiency of the linear approximation (1) is measured by its correlation which is defined as

$$\begin{aligned} \mathbf{cor}_f(u; w_1, \cdots, w_k) &= 2\Pr(u \cdot f(x_1, \cdots, x_k) = \bigoplus_{i=1}^{k} w_i \cdot x_i) - 1 \\ &= \frac{1}{|J|^k} \sum_{(x_1, \cdots, x_k) \in J^k} (-1)^{u \cdot f(x_1, \cdots, x_k) \oplus \bigoplus_{i=1}^{k} w_i \cdot x_i}, \end{aligned} \tag{2}$$

where the probability is taken over uniformly distributed $x_1, \cdots, x_k$ over J, and $|J|$ denotes the cardinality of the set J.

2.2 Linear approximations of the addition modulo 2^n

In this section we recall some properties of linear approximations of the addition modulo 2^n briefly, for more details please refer to [9, 10].

Denote by $\boxplus$ the addition modulo 2^n, that is, for any $x_1, x_2 \in Z_{2^n}$, we have $x_1 \boxplus x_2 = (x_1 + x_2) \mod 2^n$. Let (u, w_1, w_2) be a linear mask of the addition $\boxplus$, and denote by $\mathbf{cor}_{\boxplus}(u; w_1, w_2)$ the correlation of the linear approximation $u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$. From the linear mask (u, w_1, w_2) we derive a sequence $\underline{z} = z_{n-1} \cdots z_0$ as follows

$$z_i = u^{(i)} 2^2 + w_2^{(i)} 2 + w_1^{(i)}, \quad i = 0, 1, \cdots, n-1. \tag{3}$$

It's easy to see that $0 \le z_i \le 7$ for all $0 \le i \le n-1$. Define

$$M_n(u, w_1, w_2) = \prod_{i=0}^{n-1} A_{z_i}, \tag{4}$$

where A_j $(j = 0, 1, \cdots, 7)$ are constant matrices of size 2×2 and defined as follows

$$\begin{aligned} A_0 = \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}, A_1 = A_2 = -A_4 = \frac{1}{4}\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}, \\ -A_3 = A_5 = A_6 = \frac{1}{4}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, A_7 = \frac{1}{4}\begin{pmatrix} 3 & -1 \\ 1 & -3 \end{pmatrix}. \end{aligned}$$

Then we have

Theorem 1 ([9]). *For any given linear mask (u, w_1, w_2), let $M_n(u, w_1, w_2)$ be defined as above. Set $M_n(u, w_1, w_2) = (M_{i,j})_{0\le i,j\le 1}$. Then we have*

$$\begin{aligned} M_{i,j} = &\Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge c_n = i \wedge c_0 = j) \\ &- \Pr(u \cdot (x_1 \boxplus x_2) \neq w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge c_n = i \wedge c_0 = j), \end{aligned}$$

where c_0 is an initial carry bit, and c_n is the n-th carry bit of the addition of x_1 and x_2 with the initial carry bit c_0. By convention $c_0 = 0$, and we have

$$\mathbf{cor}_{\boxplus}(u; w_1, w_2) = M_{0,0} + M_{1,0}. \tag{5}$$

Note that for any integers x_1 and x_2, if $c_0 = 1$, then the addition of x_1 and x_2 modulo 2^n with the initial carry c_0 is equivalent to $(x_1 + x_2 + 1) \mod 2^n$. Therefore we get the following corollary.

Corollary 1. *Let $x_1 \overline{\boxplus} x_2 = x_1 \boxplus x_2 \boxplus 1$ and (u, w_1, w_2) be a linear mask of $\overline{\boxplus}$. Denote by $\mathbf{cor}_{\overline{\boxplus}}(u; w_1, w_2)$ the correlation of the linear approximation $u \cdot (x_1 \overline{\boxplus} x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$. Then we have*

$$\mathbf{cor}_{\overline{\boxplus}}(u; w_1, w_2) = M_{0,1} + M_{1,1}. \tag{6}$$

3 Some properties on linear approximations of the addition modulo $2^n - 1$

In this section we will discuss some properties of linear approximations of the addition modulo $2^n - 1$ with k inputs, where we always assume that $n \ge 2$ and $k \ge 2$. For consistency with the definition of the addition of the prime field $\mathbb{F}_{2^n-1}$ in ZUC [20], here we make the convention that the set of representatives of the residue class modulo $2^n - 1$ are $\{1, 2, \cdots, 2^n - 1\}$ instead of $\{0, 1, \cdots, 2^n - 2\}$. It should be pointed out that all results in this paper can induce the corresponding ones in $\{0, 1, \cdots, 2^n - 2\}$ directly.

Let $J = \{1, 2, \cdots, 2^n - 1\}$, and denote by $\hat{\boxplus}$ the addition modulo $2^n - 1$ as defined in ZUC, more precisely, for any $x_1, x_2 \in J$, we have

$$x_1 \hat{\boxplus} x_2 = \begin{cases} x_1 + x_2 & \text{if } x_1 + x_2 < 2^n, \\ (x_1 + x_2 + 1) \bmod 2^n & \text{if } x_1 + x_2 \ge 2^n. \end{cases} \tag{7}$$

For example, set $n = 3$, then $J = \{1, 2, \cdots, 7\}$, and $2 \hat{\boxplus} 6 = 1$, $3 \hat{\boxplus} 4 = 7$.

In the following we consider the addition modulo $2^n - 1$ over J with k inputs. For any given linear mask $(u, w_1, \cdots, w_k)$, we denote by $\mathbf{cor}_{\hat{\boxplus}}(u; w_1, \cdots, w_k)$ the correlation of the linear approximation

$$u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{i=1}^{k} w_i \cdot x_i.$$

For simplicity we write $\mathbf{cor}_{\hat{\boxplus}}(u; w_1, \cdots, w_k)$ as $\mathbf{cor}(u; w_1, \cdots, w_k)$.

The following two theorems can easily be derived.

Theorem 2. *For any given linear mask $(u, w_1, \cdots, w_k)$ and any permutation $(i_1, \cdots, i_k)$ of $(1, \cdots, k)$, we have*

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \mathbf{cor}(u; w_{i_1}, \cdots, w_{i_k}). \tag{8}$$

Proof. Define

$$J(u; w_1, \cdots, w_k) = \{\, (x_1, \cdots, x_k) \in J^k \mid u \cdot (x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_k) = \bigoplus_{i=1}^{k} w_i \cdot x_i \,\}.$$

By the definition of the correlation (see Eqn. (2)), we only need to prove that

$$|J(u; w_1, \cdots, w_k)| = |J(u; w_{i_1}, \cdots, w_{i_k})|. \tag{9}$$

For any $(x_1, \cdots, x_k) \in J(u; w_1, \cdots, w_k)$, we have

$$u \cdot (\hat{\boxplus}_{j=1}^{k} x_{i_j}) = u \cdot (\hat{\boxplus}_{i=1}^{k} x_i) = \bigoplus_{i=1}^{k} w_i \cdot x_i = \bigoplus_{j=1}^{k} w_{i_j} \cdot x_{i_j},$$

which shows $(x_{i_1}, \cdots, x_{i_k}) \in J(u; w_{i_1}, \cdots, w_{i_k})$, and vice versa. So Eqn. (9) holds. ■

Theorem 3. *For any given linear mask $(u, w_1, \cdots, w_k)$ and integer ℓ such that $1 \le \ell \le n-1$, we have*

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \mathbf{cor}(u \lll \ell; w_1 \lll \ell, \cdots, w_k \lll \ell), \tag{10}$$

where $x \lll \ell$ denotes the cyclic shift of x ℓ bits to the left .

Proof. Similarly to the proof of Theorem 2, we only need to prove that

$$|J(u; w_1, \cdots, w_k)| = |J(u \lll \ell; w_1 \lll \ell, \cdots, w_k \lll \ell)|. \tag{11}$$

It is easy to see that $x \lll \ell \equiv 2^\ell x \mod (2^n - 1)$ holds for any $x \in J$, which means that for any $x_1, \cdots, x_k \in J$, we have

$$(\sum_{i=1}^{k} x_i) \lll \ell \equiv 2^\ell \sum_{i=1}^{k} x_i \equiv \sum_{i=1}^{k} 2^\ell x_i \equiv \sum_{i=1}^{k} (x_i \lll \ell) \mod (2^n - 1),$$

namely, $(\hat{\boxplus}_{i=1}^{k} x_i) \lll \ell = \hat{\boxplus}_{i=1}^{k} (x_i \lll \ell)$.

So for any $(x_1, \cdots, x_k) \in J(u; w_1, \cdots, w_k)$, we have

$$\begin{aligned}(u \lll \ell) \cdot (\hat{\boxplus}_{i=1}^{k} (x_i \lll \ell)) &= (u \lll \ell) \cdot ((\hat{\boxplus}_{i=1}^{k} x_i) \lll \ell) = (u \cdot (\hat{\boxplus}_{i=1}^{k} x_i)) \lll \ell \\ &= (\bigoplus_{i=1}^{k} w_i \cdot x_i) \lll \ell = \bigoplus_{i=1}^{k} (w_i \lll \ell) \cdot (x_i \lll \ell).\end{aligned}$$

It follows that $(x_1 \lll \ell, \cdots, x_k \lll \ell) \in J(u \lll \ell; w_1 \lll \ell, \cdots, w_k \lll \ell)$, that is, $|J(u; w_1, \cdots, w_k)| \le |J(u \lll \ell; w_1 \lll \ell, \cdots, w_k \lll \ell)|$. Note that $(x \lll \ell) \lll (n - \ell) = x$ for any $x \in J$. By shifting each mask cyclicly $n - \ell$ bits to the left, we have

$$|J(u \lll \ell; w_1 \lll \ell, \cdots, w_k \lll \ell)| \le |J(u; w_1, \cdots, w_k)|.$$

So Eqn. (11) follows. ■

3.1 Addition of two inputs in $\mathbb{F}_{2^n-1}$

In this section we will derive an explicit expression of $\mathbf{cor}(u; w_1, w_2)$ for any linear mask (u, w_1, w_2) from Theorem 1. For any given linear mask (u, w_1, w_2), we keep the notations $\underline{z}$, $M_n(u, w_1, w_2)$ and $M_{i,j}$ $(0 \le i, j \le 1)$ defined in section 2.

One can notice that when $x_1 + x_2 < 2^n$, we have $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2$, and when $x_1 + x_2 \ge 2^n$, we have $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2 \boxplus 1$. Thus by Theorem 1 and Corollary 1, it seems that $\mathbf{cor}(u; w_1, w_2)$ is almost equal to $M_{0,0} + M_{1,1}$ if the difference between Z_{2^n} and J is ignored. Below we give an explicit expression for $\mathbf{cor}(u; w_1, w_2)$.

Theorem 4. *Let (u, w_1, w_2) be a linear mask of the addition $\hat{\boxplus}$ modulo $2^n - 1$, and $M_n(u, w_1, w_2) = (M_{i,j})_{0 \le i,j \le 1}$ be defined as above. Then we have*

$$\mathbf{cor}(u; w_1, w_2) = \frac{2^{2n}(M_{0,0} + M_{1,1}) + 2^n \cdot c + 1}{(2^n - 1)^2}, \tag{12}$$

where

$$c = \begin{cases} -3, & \text{if } u = w_1 = w_2 \text{ and } w_{\mathrm{H}}(w_2) \text{ is even}, \\ 1, & \text{if } u \ne w_1 = w_2 \text{ and } w_{\mathrm{H}}(w_2) \text{ is odd}, \\ 0, & \text{if } u, w_1 \text{ and } w_2 \text{ are pairwise different}, \\ -1, & \text{otherwise}, \end{cases}$$

and $w_{\mathrm{H}}(w_2)$ denotes the hamming weight of w_2 in its binary representation.

Proof. For any given $x_1, x_2 \in J$, we consider $x_1 \hat{\boxplus} x_2$ from the following two aspects.

First, when $0 < x_1 + x_2 < 2^n$, it is known that $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2$. By Theorem 1, we have

$$\begin{aligned} M_{0,0} = &\Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge 0 \le x_1 + x_2 < 2^n) \\ &- \Pr(u \cdot (x_1 \boxplus x_2) \ne w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge 0 \le x_1 + x_2 < 2^n). \end{aligned}$$

Since

$$\begin{aligned} &\Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge 0 \le x_1 + x_2 < 2^n) \\ &+ \Pr(u \cdot (x_1 \boxplus x_2) \ne w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge 0 \le x_1 + x_2 < 2^n) \\ &= \Pr(x_1 + x_2 < 2^n) = \frac{2^n + 1}{2^{n+1}}, \end{aligned}$$

thus we have

$$\Pr(u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2 \wedge 0 \le x_1 + x_2 < 2^n) = \frac{1}{2} M_{0,0} + \frac{2^n + 1}{2^{n+2}}.$$

It follows that there are $2^{n-2}(2^n + 1) + 2^{2n-1} M_{0,0}$ pairs (x_1, x_2) satisfying $u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$ and $0 \le x_1 + x_2 < 2^n$. We consider those pairs of the form $(0, x_2)$. When $x_1 = 0$, we get $(u \oplus w_2) \cdot x_2 = 0$ due to $u \cdot x_2 = w_2 \cdot x_2$.

It follows that there are 2^{n-1} solutions x_2 if $u \neq w_2$ and 2^n solutions if $u = w_2$. Hence there are 2^{n-1} pairs of the form $(0, x_2)$ among all the above pairs not in $J \times J$ if $u \neq w_2$ and 2^n pairs not in $J \times J$ if $u = w_2$. By the symmetric position of x_1 and x_2, we have the same conclusion for $x_2 = 0$. In addition, the pair $(0, 0)$ always satisfies $u \cdot (x_1 \boxplus x_2) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$ but is not in $J \times J$.

Second, when $x_1 + x_2 \geq 2^n$, we have $x_1 \hat{\boxplus} x_2 = x_1 \boxplus x_2 \boxplus 1$. Similar to the above case, there are totally $2^{n-2}(2^n + 1) + 2^{2n-1}M_{1,1}$ pairs (x_1, x_2) satisfying both $x_1 + x_2 + 1 \geq 2^n$ and $u \cdot (x_1 \boxplus x_2 \boxplus 1) = w_1 \cdot x_1 \oplus w_2 \cdot x_2$. Now we consider how to remove some pairs (x_1, x_2) satisfying $x_1 + x_2 + 1 = 2^n$ from the above pairs. Note that $x_1 \boxplus x_2 \boxplus 1 = 0$, thus we only need to count pairs (x_1, x_2) such that $x_1 + x_2 = 2^n - 1$ and $w_1 \cdot x_1 = w_2 \cdot x_2$. Since $x_1 + x_2 = 2^n - 1 = x_1 \oplus x_2$, it follows that

$$(w_1 \oplus w_2) \cdot x_1 = w_2 \cdot (2^n - 1). \tag{13}$$

If $w_1 \neq w_2$, Eqn. (13) has 2^{n-1} solutions; if $w_1 = w_2$, when $w_{\mathrm{H}}(w_2)$ is an odd number, Eqn. (13) has no solutions, and when $w_{\mathrm{H}}(w_2)$ is an even number, Eqn. (13) has 2^n solutions.

Denote by d the number of pairs $(x_1, x_2) \in Z_{2^n} \times Z_{2^n}$ which satisfy the linear approximation defined by mask (u, w_1, w_2) and $x_1 = 0$ or $x_2 = 0$ or $x_1 + x_2 = 2^n - 1$. Combine the above two cases, we have

$$d = \begin{cases} 3 \cdot 2^n - 1, & \text{if } u = w_1 = w_2 \text{ and } w_{\mathrm{H}}(w_2) \text{ is even,} \\ 2^n - 1, & \text{if } u \neq w_1 = w_2 \text{ and } w_{\mathrm{H}}(w_2) \text{ is odd,} \\ 3 \cdot 2^{n-1} - 1, & \text{if } u, w_1 \text{ and } w_2 \text{ are pairwise different,} \\ 2 \cdot 2^n - 1, & \text{otherwise.} \end{cases}$$

By the definition of correlation, we have

$$\begin{aligned} &\mathbf{cor}(u; w_1, w_2) \\ =&2 \cdot \frac{(2^{n-2}(2^n + 1) + 2^{2n-1}M_{0,0}) + (2^{n-2}(2^n + 1) + 2^{2n-1}M_{1,1}) - d}{(2^n - 1)^2} - 1 \\ =&\frac{2^{2n}(M_{0,0} + M_{1,1}) + 3 \cdot 2^n - 1 - 2d}{(2^n - 1)^2}. \end{aligned}$$

Then we can get the desired conclusion. ■

3.2 Addition of more than two inputs in $\mathbb{F}_{2^n-1}$

In this section we will derive an iterative expression of $\mathbf{cor}(u; w_1, \cdots, w_k)$ for any linear mask $(u, w_1, \cdots, w_k)$. The addition of k inputs $x_1, \cdots, x_k$ can be seen as the addition of $x_1 \hat{\boxplus} \cdots \hat{\boxplus} x_{k-1}$ and x_k.

Theorem 5. *For any given linear mask $(u, w_1, \cdots, w_k)$ and integer $k > 2$, we have*

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \frac{2^n - 1}{2^n} \sum_{w=0}^{2^n-1} \mathbf{cor}(w; w_1, \cdots, w_{k-1})\mathbf{cor}(u; w, w_k). \tag{14}$$

Proof. By Eqn. (2), we have

$$\mathbf{cor}(u; w_1, \cdots, w_k) = \frac{1}{(2^n-1)^k} \sum_{(x_1,\cdots,x_k)\in J^k} (-1)^{u\cdot(\hat{\boxplus}_{i=1}^k x_i)\oplus\bigoplus_{i=1}^k w_i\cdot x_i}.$$

Denote $y = x_1\hat{\boxplus}\cdots\hat{\boxplus}x_{k-1}$. Then we have

$$\begin{aligned}
&\sum_{w=0}^{2^n-1} \mathbf{cor}(w; w_1, \cdots, w_{k-1})\mathbf{cor}(u; w, w_k) \\
&= \frac{1}{(2^n-1)^{k+1}} \sum_{w=0}^{2^n-1} \sum_{\substack{(x_1,\cdots,x_{k-1})\in J^{k-1} \\ (z,x_k)\in J^2}} (-1)^{w\cdot y\oplus\bigoplus_{i=1}^{k-1} w_i\cdot x_i} (-1)^{u\cdot(z\hat{\boxplus}x_k)\oplus w\cdot z\oplus w_k\cdot x_k} \\
&= \frac{1}{(2^n-1)^{k+1}} \sum_{(x_1,\cdots,x_k,z)\in J^{k+1}} (-1)^{u\cdot(z\hat{\boxplus}x_k)\oplus\bigoplus_{i=1}^k w_i\cdot x_i} \sum_{w=0}^{2^n-1} (-1)^{w\cdot z\oplus w\cdot y}
\end{aligned}$$

Note that

$$\sum_{w=0}^{2^n-1} (-1)^{w\cdot z\oplus w\cdot y} = \begin{cases} 2^n, & \text{if } z = y, \\ 0, & \text{if } z \neq y. \end{cases}$$

Then we have

$$\begin{aligned}
&\sum_{w=0}^{2^n-1} \mathbf{cor}(w; w_1, \cdots, w_{k-1})\mathbf{cor}(u; w, w_k) \\
&= \frac{2^n}{(2^n-1)^{k+1}} \sum_{(x_1,\cdots,x_k)\in J^k} (-1)^{u\cdot(y\hat{\boxplus}x_k)\oplus\bigoplus_{i=1}^k w_i\cdot x_i} \\
&= \frac{2^n}{2^n-1}\mathbf{cor}(u; w_1, \cdots, w_k).
\end{aligned}$$

■

4 More properties of linear approximations of the addition modulo $2^n - 1$ with two inputs

In this section we will provide more properties of linear approximations of the addition modulo $2^n - 1$ with two inputs, that is, $k = 2$. First we introduce some notations and concepts.

Let $\mathbb{Q}$ be the rational field. Define

$$\mathrm{I} = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} | a, b \in \mathbb{Q} \right\},$$
$$\mathrm{II} = \left\{ \begin{pmatrix} a & -b \\ b & -a \end{pmatrix} | a, b \in \mathbb{Q} \right\},$$

and call a matrix in the set I (or II) to be type-I (or type-II). It is easy to see that $A_0, A_3, A_5, A_6 \in$ I and $A_1, A_2, A_4, A_7 \in$ II (which are defined in section 2). The following two properties can easily be verified.

Lemma 1. *The product of arbitrary two type-I (or type-II) matrices is a type-I matrix.*

Lemma 2. *The product of a type-I matrix and a type-II matrix is a type-II matrix.*

By the definition of $M_n(u, w_1, w_2)$ and Lemmas 1 and 2, we have

Lemma 3. *For any given linear mask (u, w_1, w_2), $M_n(u, w_1, w_2)$ is either type-I or type-II.*

For any given square matrix M, denote by $\mathbf{Tr}(M)$ the trace of the matrix M, that is, the sum of elements on the main diagonal of M. Since the trace of an arbitrary type-II matrix is zero, thus the following conclusions hold.

Corollary 2. *For any given linear mask (u, w_1, w_2), let $\underline{z} = z_{n-1} \cdots z_0$ be the sequence derived from (u, w_1, w_2) by the formula (3). If the number of elements z_i such that $z_i \in \{1, 2, 4, 7\}$ is odd, $i = 0, 1, \cdots, n-1$, then $\mathbf{Tr}(M_n(u, w_1, w_2)) = 0$.*

Corollary 3. *Let $u \in Z_{2^n}$ and $w_{\mathrm{H}}(u)$ be odd. Then $\mathbf{Tr}(M_n(u, u, u)) = 0$. Thus we have*

$$\mathbf{cor}(u; u, u) = -\frac{1}{2^n - 1}$$

and

$$\lim_{n\to\infty} \mathbf{cor}(u; u, u) = 0.$$

Corollary 4. *Let $u \in Z_{2^n}$ and $w_{\mathrm{H}}(u)$ be even. Then $M_n(u, u, u)$ is type-I, that is, $M_{0,0} = M_{1,1}$. Thus we have*

$$\mathbf{cor}(u; u, u) = \frac{2^{2n} \cdot 2M_{0,0} - 3 \cdot 2^n + 1}{(2^n - 1)^2}.$$

If all 1's of u in the binary representation are adjacent, then we have

$$\mathbf{cor}(u; u, u) = \frac{2^{2n} \cdot (2^{\frac{w_{\mathrm{H}}(u)}{2} - n} + 2^{-\frac{w_{\mathrm{H}}(u)}{2}}) - 3 \cdot 2^n + 1}{(2^n - 1)^2}$$

and

$$\lim_{n\to\infty} \mathbf{cor}(u; u, u) = 2^{-\frac{w_{\mathrm{H}}(u)}{2}}.$$

Proof. By Theorem 3, we only need to consider the masks whose binary expression be of the form $(\underbrace{0, \cdots, 0}_{n-w_{\mathrm{H}}(u)} \underbrace{1, \cdots, 1}_{w_{\mathrm{H}}(u)})$. Then $M_n(u, u, u) = A_0^{n-w_{\mathrm{H}}(u)} A_7^{w_{\mathrm{H}}(u)}$. Denote by $\mathbf{I}_2$ the 2×2 identity matrix. It is easy to see that $A_7^2 = \frac{1}{2}\mathbf{I}_2$. Since

$w_{\mathrm{H}}(u)$ is even, we have $A_7^{w_{\mathrm{H}}(u)} = 2^{-\frac{w_{\mathrm{H}}(u)}{2}}\mathbf{I}_2$. So $M_n(u,u,u) = 2^{-\frac{w_{\mathrm{H}}(u)}{2}}A_0^{n-w_{\mathrm{H}}(u)}$. Since A_0 is a symmetric matrix of the form $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, it is easily proved by induction that

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix}^t = \frac{1}{2}\begin{pmatrix} (a+b)^t + (a-b)^t & (a+b)^t - (a-b)^t \\ (a+b)^t - (a-b)^t & (a+b)^t + (a-b)^t \end{pmatrix}$$

for $t \geq 1$. Then we have $\mathbf{Tr}(A_0^{n-w_{\mathrm{H}}(u)}) = 1 + 2^{w_{\mathrm{H}}(u)-n}$. So $\mathbf{Tr}(M_n(u,u,u)) = 2^{-\frac{w_{\mathrm{H}}(u)}{2}}\mathbf{Tr}(A_0^{n-w_{\mathrm{H}}(u)}) = 2^{-\frac{w_{\mathrm{H}}(u)}{2}} + 2^{\frac{w_{\mathrm{H}}(u)}{2}-n}$, and the conclusion follows. ■

Below we give some facts on A_i, $0 \leq i \leq 7$, which will be used later.

Lemma 4. *1.* $A_0A_i = \frac{1}{2}A_i$, *for* $\forall\ i \in \{1,2,3,4,5,6\}$;
2. $A_iA_0 = A_i$ *if* $i \in \{1,2,4\}$ *and* $A_iA_0 = \frac{1}{2}A_i$ *if* $i \in \{3,5,6\}$;
3. $A_iA_j = 0$, $i \in \{1,2,4\}$ *and* $j \in \{1,2,3,4,5,6\}$;
4. $A_1A_7 = A_2A_7 = -A_4A_7 = A_6$.

Now we consider a class of special linear masks $(u,1,w)$. Let $\underline{z} = z_{n-1}\cdots z_0$ be the sequence derived from $(u,1,w)$. It is easy to see that $z_0 \in \{1,3,5,7\}$ and $z_i \in \{0,2,4,6\}$, $1 \leq i \leq n-1$. In the rest of the paper we simply write M instead of $M_n(u,1,w)$.

Lemma 5. *For any integers* $u, w \in Z_{2^n}$, *if* $\mathbf{Tr}(M) \neq 0$, *then the sequence* $\underline{z}$ *is of the form either* $\{0,6\}^{n-1}\{3,5\}$ *or* $\{0,6\}^*\{2,4\}0^*7$.

Proof. Let r be the number of z_i such that $z_i \in \{2,4\}$, $i = 1,2,\cdots,n-1$. We first prove that $r \leq 1$. Assume that $r > 1$. Then there exist two indexes i and j such that $z_i, z_j \in \{2,4\}$, $1 \leq i < j \leq n-1$. By Items 2 and 3 of Lemma 4, we have $A_{z_i}\cdots A_{z_j} = 0$. It follows that $M = 0$, which contradicts $\mathbf{Tr}(M) \neq 0$.

When $r = 0$, if $z_0 \in \{1,7\}$, by Corollary 2, it is known that the matrix M is of type-II, which contradicts $\mathbf{Tr}(M) \neq 0$ as well. Thus $z_0 \in \{3,5\}$. So $\underline{z}$ is of the form $\{0,6\}^{n-1}\{3,5\}$.

When $r = 1$, let $z_j \in \{2,4\}$, where $1 \leq j \leq n-1$. First we claim that $z_i = 0$ for all $1 \leq i < j$. If there exists some index i such that $z_i \neq 0$, by Items 2 and 3 of Lemma 4, we have $A_{z_i}\cdots A_{z_j} = 0$, furthermore $M = 0$, which is a contradiction. Second, if $z_0 \in \{1,3,5\}$, by Items 2 and 3 of Lemma 4, we have $A_{z_0}\cdots A_{z_i} = 0$. So $\underline{z}$ is of the form $\{0,6\}^*\{2,4\}0^*7$. ■

Theorem 6. *For any integers* $u, w \in Z_{2^n}$, $\mathbf{Tr}(M) \neq 0$ *if and only if* $u = w \oplus 2^i$, *where* $0 \leq i \leq LNB(w \oplus 1)$, $LNB(x)$ *denotes the least index where 1 appears in the binary representation of* x *if* $x \neq 0$, *and* $LNB(0) = n-1$.

Proof. The necessity follows directly from Lemma 5. Below we prove the sufficiency. First we prove that $\mathbf{Tr}(A_6^t) = 2^{-t}$ for any $t \geq 1$. In fact, it is easy to calculate two characteristic roots 0 and 2^{-1} of A_6. Thus we have $\mathbf{Tr}(A_6^t) = 0^t + (2^{-1})^t = 2^{-t}$.

If $i = 0$, i.e., $u = w \oplus 1$, then $\underline{z}$ is of the form $\{0,6\}^{n-1}\{3,5\}$. Let t be the number of z_i such that $z_i = 6$, $i = 1, 2, \cdots, n-1$. Then 0 occurs in $z_{n-1} \cdots z_1$ for $n-1-t$ times. Thus by Lemma 4, we have

$$\begin{aligned}\mathbf{Tr}(M) &= \mathbf{Tr}(A_{z_{n-1}} \cdot \cdots \cdot A_{z_0}) \\ &= \mathbf{Tr}(2^{-(n-1-t)} A_6^t A_{z_0}) \\ &= (-1)^w 2^{-(n-1-t)} \mathbf{Tr}(A_6^{t+1}) \\ &= (-1)^w 2^{-(n-1-t)} 2^{-(t+1)} \\ &= (-1)^w 2^{-n}.\end{aligned}$$

If $i > 0$, then $\underline{z}$ is of the form $\{0,6\}^*\{2,4\}0^*7$ and $z_i \in \{2, 4\}$. Let t be the number of repetitions of 6 appearing in $z_{n-1} \cdots z_{i+1}$. Then by Lemma 4, we have

$$\begin{aligned}\mathbf{Tr}(M) &= \mathbf{Tr}(A_{z_{n-1}} \cdot \cdots \cdot A_{z_0}) \\ &= \mathbf{Tr}(2^{-(n-1-i-t)} A_6^t A_{z_i} A_7) \\ &= (-1)^s 2^{-(n-1-i-t)} \mathbf{Tr}(A_6^{t+1}) \\ &= (-1)^s 2^{-(n-1-i-t)} 2^{-(t+1)} \\ &= (-1)^s 2^{-(n-i)},\end{aligned}$$

where $s = w^{(i)} \oplus 1$. ■

Theorem 6 gives a sufficient and necessary condition for judjing whether or not M is of type-II for any linear mask $(u, 1, w)$. From its proof we can get the following result.

Corollary 5. *For any integers $u, w \in Z_{2^n}$ such that $u = w \oplus 2^i$, where $0 \le i \le LNB(w \oplus 1)$, we have $\mathbf{Tr}(M) = (-1)^s 2^{-(n-i)}$, where*

$$s = \begin{cases} 0 & \text{if } i = 0 \text{ and } w^{(0)} = 0 \text{ or } i > 0 \text{ and } w^{(i)} = 1, \\ 1 & \text{otherwise.} \end{cases}$$

By Theorem 4 and Corollary 5, we can derive the following corollary.

Corollary 6. *The correlation of the linear approximation of addition in $\mathbb{F}_{2^n-1}$ with a mask of the form $(w, 1, 1)$ is given by*

$$\mathbf{cor}(w; 1, 1) = \begin{cases} \frac{1}{(2^n-1)^2} & \text{if } w = 0, \\ -\frac{1}{2^n-1} & \text{if } w = 1, \\ \frac{-2^{n+i}+2^n+1}{(2^n-1)^2} & \text{if } w = 2^i + 1, 1 \le i \le n-1, \\ \frac{2^n+1}{(2^n-1)^2} & \text{otherwise.} \end{cases}$$

When the mask is of the form $(1, w, 1)$, the correlation is given by

$$\mathbf{cor}(1; w, 1) = \begin{cases} \frac{1}{(2^n-1)^2} & \text{if } w = 0, \\ \frac{2^{n+i}-2^n+1}{(2^n-1)^2} & \text{if } w = 2^i + 1, 1 \le i \le n-1, \\ -\frac{1}{2^n-1} & \text{otherwise.} \end{cases}$$

Finally we give an upper bound of $|\mathbf{cor}(u;1,w)|$. For any given integer $x \in Z_{2^n}$, define

$$J_x = \{x \oplus 2^i | 1 \le i \le LNB(x \oplus 1)\}.$$

Theorem 7. *For any integers $u, w \in Z_{2^n}$, if $w \notin J_u$, then*

$$|\mathbf{cor}(u;1,w)| < \frac{3}{2^n - 1}. \tag{15}$$

Proof. If $w \neq u \oplus 1$, by Theorem 6, we have $\mathbf{Tr}(M) = 0$, that is, $M_{0,0} + M_{1,1} = 0$. If $u = w = 1$, Eqn. (15) follows directly from Corollary 6. If $u \neq w$, by Theorem 4 we have

$$|\mathbf{cor}(u;1,w)| \le \frac{2^n + 1}{(2^n - 1)^2} < \frac{3}{2^n - 1}.$$

If $w = u \oplus 1$, by Corollary 5 and Theorem 4, we have

$$|\mathbf{cor}(u;1,w)| \le \frac{2^{2n} \cdot 2^{-n} + 2^n + 1}{(2^n - 1)^2} = \frac{2 \cdot 2^n + 1}{(2^n - 1)^2} < \frac{3}{2^n - 1}.$$

■

5 The limit of $\mathbf{cor}(1;1^k)$ for the addition in $\mathbb{F}_{2^n-1}$ when $n \to \infty$

In this section we will discuss the limit of correlations $\mathbf{cor}(u;\underbrace{u,\cdots,u}_{k})$ when n goes to infinity, where $w_{\mathrm{H}}(u) = 1$. By Theorem 3, it is known that $\mathbf{cor}(u;\underbrace{u,\cdots,u}_{k})$ $= \mathbf{cor}(1;\underbrace{1,\cdots,1}_{k})$. So below we only consider $\mathbf{cor}(1;\underbrace{1,\cdots,1}_{k})$. For simplicity, we denote it by $\mathbf{cor}(1;1^k)$.

Lemma 6. *For any integers $n \ge 2$ and $k \ge 2$, we have*

$$\sum_{u \in Z_{2^n}} |\mathbf{cor}(u;1^k)| < (n+3)^{k-1}.$$

Proof. Note that $|J_x| \le n$ for all $x \in Z_{2^n}$. When $k = 2$, by Theorem 7, we have

$$\begin{aligned}\sum_{u \in Z_{2^n}} |\mathbf{cor}(u;1,1)| &= \sum_{u \in J_1} |\mathbf{cor}(u;1,1)| + \sum_{u \notin J_1} |\mathbf{cor}(u;1,1)| \\ &\le \sum_{u \in J_1} 1 + \frac{3}{2^n - 1} \sum_{u \notin J_1} 1 < n + 3.\end{aligned}$$

Suppose that when $k = k_0$, we have $\sum_{u \in Z_{2^n}} |\mathbf{cor}(u;1^{k_0})| < (n+3)^{k_0 - 1}$. Then

$$
\begin{aligned}
&\sum_{u\in Z_{2^n}} |\mathbf{cor}(u;1^{k_0+1})| \\
&= \frac{2^n-1}{2^n}\sum_{u\in Z_{2^n}} |\sum_{w\in Z_{2^n}} \mathbf{cor}(w;1^{k_0})\mathbf{cor}(u;w,1)| \\
&< \sum_{u\in Z_{2^n}}\sum_{w\in Z_{2^n}} |\mathbf{cor}(w;1^{k_0})\mathbf{cor}(u;w,1)| \\
&= \sum_{u\in Z_{2^n}} (\sum_{w\in J_u} |\mathbf{cor}(w;1^{k_0})\mathbf{cor}(u;w,1)| + \sum_{w\notin J_u} |\mathbf{cor}(w;1^{k_0})\mathbf{cor}(u;w,1)|) \\
&< \sum_{u\in Z_{2^n}}\sum_{w\in J_u} |\mathbf{cor}(w;1^{k_0})| + \frac{3}{2^n-1}\sum_{u\in Z_{2^n}}\sum_{w\notin J_u} |\mathbf{cor}(w;1^{k_0})| \\
&< n\cdot(n+3)^{k_0-1} + \frac{3}{2^n-1}\cdot(2^n-1)\cdot(n+3)^{k_0-1} \\
&= (n+3)^{k_0}.
\end{aligned}
$$

By induction the conclusion of the theorem holds. ■

Lemma 7. *For any integer $t \geq 1$ and $i \geq 2$, we have*

$$\lim_{n\to\infty} \sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}\sum_{u_t\notin J_{u_{t-1}}} \mathbf{cor}(u_t;1^i)\prod_{j=1}^{t}\mathbf{cor}(u_{j-1};u_j,1) = 0,$$

where $u_0 = 1$.

Proof. By Lemma 6 and Theorem 7, we have

$$
\begin{aligned}
&\left|\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}\sum_{u_t\notin J_{u_{t-1}}} \mathbf{cor}(u_t;1^i)\prod_{j=1}^{t}\mathbf{cor}(u_{j-1};u_j,1)\right| \\
&< \frac{3}{2^n-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}\sum_{u_t\notin J_{u_{t-1}}} |\mathbf{cor}(u_t;1^i)\prod_{j=1}^{t-1}\mathbf{cor}(u_{j-1};u_j,1)| \\
&\leq \frac{3}{2^n-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}}\sum_{u_t\notin J_{u_{t-1}}} |\mathbf{cor}(u_t;1^i)| \\
&< \frac{3}{2^n-1}(n+3)^{i-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{t-1}\in J_{u_{t-2}}} 1 \\
&< \frac{3}{2^n-1}(n+3)^{i-1}n^{t-1}.
\end{aligned}
$$

Since $\frac{3}{2^n-1}(n+3)^{i-1}n^{t-1}$ approaches 0 when n approaches infinity, thus the conclusion holds. ■

Lemma 8. *For any integer $k \geq 3$, if $\lim_{n\to\infty} \mathbf{cor}(1;1^k)$ exists, then*

$$\lim_{n\to\infty} \mathbf{cor}(1;1^k) = \lim_{n\to\infty} \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} \prod_{j=1}^{k-1} \mathbf{cor}(u_{j-1};u_j,1),$$

where $u_0 = u_{k-1} = 1$.

Proof.

$$\begin{aligned}
&\lim_{n\to\infty} \mathbf{cor}(1;1^k)\\
&= \lim_{n\to\infty} \sum_{u_1\in Z_{2^n}} \mathbf{cor}(u_1;1^{k-1})\mathbf{cor}(1;u_1,1)\\
&= \lim_{n\to\infty} (\sum_{u_1\in J_1} + \sum_{u_1\notin J_1})\mathbf{cor}(u_1;1^{k-1})\mathbf{cor}(1;u_1,1)\\
&= \lim_{n\to\infty} \sum_{u_1\in J_1} \mathbf{cor}(u_1;1^{k-1})\mathbf{cor}(1;u_1,1) \quad \text{(by Lemma 7)}\\
&= \lim_{n\to\infty} \sum_{u_1\in J_1} \sum_{u_2\in Z_{2^n}} \mathbf{cor}(u_2;1^{k-2})\mathbf{cor}(u_1;u_2,1)\mathbf{cor}(1;u_1,1)\\
&= \lim_{n\to\infty} \sum_{u_1\in J_1} (\sum_{u_2\in J_{u_1}} + \sum_{u_2\notin J_{u_1}})\mathbf{cor}(u_2;1^{k-2})\mathbf{cor}(u_1;u_2,1)\mathbf{cor}(1;u_1,1)\\
&= \lim_{n\to\infty} \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \mathbf{cor}(u_2;1^{k-2})\mathbf{cor}(u_1;u_2,1)\mathbf{cor}(1;u_1,1) \quad \text{(by Lemma 7)}\\
&= \lim_{n\to\infty} \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-2}\in J_{u_{k-3}}} \prod_{j=1}^{k-1} \mathbf{cor}(u_{j-1};u_j,1).
\end{aligned}$$

■

Theorem 8. *For any integer $k \geq 3$, if $\lim_{n\to\infty} \mathbf{cor}(1;1^k)$ exists, then*

$$\lim_{n\to\infty} \mathbf{cor}(1;1^k) = \lim_{n\to\infty} \sum_{u_1\in J_1} \sum_{u_2\in J_{u_1}} \cdots \sum_{u_{k-1}\in J_{u_{k-2}}} \prod_{j=1}^{k-1} \mathbf{Tr}(M_n(u_{j-1},u_j,1)),$$

where $u_0 = u_{k-1} = 1$.

Proof. Recall that $A_1 = A_2$ and $A_5 = A_6$, then it is easily proved that for arbitrary two integers $u, w \in Z_{2^n}$, the matrices sequence derived from $(u,1,w)$ is the same with the matrices sequence derived from $(u,w,1)$. So we have $M_n(u,1,w) = M_n(u,w,1)$. By Theorem 4, Theorem 6 and Corollary 5, we have

$$\mathbf{cor}(u;w,1) = \mathbf{Tr}(M_n(u,w,1)) + \frac{\delta(u,w,1)}{2^n-1},$$

where

$$\begin{aligned}|\delta(u,w,1)| &= \left|\frac{(2^{n+1}-1)\mathbf{Tr}(M_n(u,w,1))+2^n\cdot c+1}{2^n-1}\right| \\ &\le \frac{(2^{n+1}-1)|\mathbf{Tr}(M_n(u,1,w))|+2^n\cdot|c|+1}{2^n-1} \\ &\le \frac{(2^{n+1}-1)+2^n\cdot 3+1}{2^n-1} \\ &< 7.\end{aligned}$$

Then

$$\begin{aligned}&\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}\prod_{j=1}^{k-1}\mathbf{cor}(u_{j-1};u_j,1) \\ &=\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}(\mathbf{Tr}(M_n(u_0,u_1,1))+\frac{\delta(u_0,u_1,1)}{p})\prod_{j=2}^{k-1}\mathbf{cor}(u_{j-1};u_j,1) \\ &=A+B,\end{aligned}$$

where

$$A=\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}\mathbf{Tr}(M_n(u_0,u_1,1))\prod_{j=2}^{k-1}\mathbf{cor}(u_{j-1};u_j,1)$$

and

$$B=\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}\frac{\delta(u_0,u_1,1)}{2^n-1}\prod_{j=2}^{k-1}\mathbf{cor}(u_{j-1};u_j,1).$$

Since

$$\begin{aligned}|B| &\le \frac{7}{2^n-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}|\prod_{j=2}^{k-2}\mathbf{cor}(u_{j-1};u_j,1)| \\ &\le \frac{7}{2^n-1}\sum_{u_1\in J_1}\sum_{u_2\in J_{u_1}}\cdots\sum_{u_{k-2}\in J_{u_{k-3}}}1 \\ &\le \frac{7}{2^n-1}n^k \xrightarrow{n\to\infty} 0,\end{aligned}$$

thus we have

$$\lim_{n\to\infty}\mathbf{cor}(1;1^k)=\lim_{n\to\infty}A.$$

Repeat the above procedure, and we always strip $\frac{\delta(u_{j-1},u_j,1)}{2^n-1}$ from $\mathbf{cor}(u_{j-1};u_j,1)$, $j=2,3,\cdots,k-1$. Then finally we can get the desired conclusion. ■

Corollary 7. $\lim_{n\to\infty} \mathbf{cor}(1;1^2) = 0$ *and* $\lim_{n\to\infty} \mathbf{cor}(1;1^3) = -\frac{1}{3}$.

Proof. Since $M_n(1,1,1) = A_0^{n-1}A_7$ is of type-II, thus $\mathbf{Tr}(M_n(1,1,1)) = 0$, furthermore we have $\lim_{n\to\infty} \mathbf{cor}(1;1,1) = 0$. By Theorem 8 and Corollary 6, we have

$$\begin{aligned}
&\lim_{n\to\infty} \mathbf{cor}(1;1^3)\\
&= \lim_{n\to\infty} \sum_{u\in J_1} \mathbf{Tr}(M_n(u,1,1))\mathbf{Tr}(M_n(1,u,1))\\
&= \lim_{n\to\infty} \sum_{i=1}^{n-1} \mathbf{Tr}(M_n(2^i+1,1,1))\mathbf{Tr}(M_n(1,2^i+1,1))\\
&= \lim_{n\to\infty} \sum_{i=1}^{n-1} (-2^{-(n-i)}) \cdot 2^{-(n-i)}\\
&= -\lim_{n\to\infty} \sum_{i=1}^{n-1} 4^{-(n-i)} = -\frac{1}{3}.
\end{aligned}$$

■

In order to deal with the general case $\lim_{n\to\infty} \mathbf{cor}(1;1^k)$, for a given integer $k \geq 3$, we define

$$U_k = \{u_0u_1u_2\cdots u_{k-2}u_{k-1} | u_j \in J_{u_{j-1}}, 1 \leq j \leq k-1, u_{k-1} = u_0 = 1\}. \quad (16)$$

Then Theorem 8 can also be written as:

Theorem 9. *For given integer $k \geq 3$, if $\lim_{n\to\infty} \mathbf{cor}(1;1^k)$ exists, then*

$$\lim_{n\to\infty} \mathbf{cor}(1;1^k) = \lim_{n\to\infty} \sum_{u_0u_1\cdots u_{k-1}\in U_k} \prod_{j=1}^{k-1} \mathbf{Tr}(M_n(u_{j-1},u_j,1)).$$

For any string $u_0u_1u_2\cdots u_{k-2}u_{k-1} \in U_k$, by the definition of $J_{u_{j-1}}$, we have $u_j > 0$ for $0 \leq j \leq k-1$, and there is only one bit in u_j different from u_{j-1}, that is, $w_{\mathrm{H}}(u_{j-1}) - w_{\mathrm{H}}(u_j) = \pm 1$. Note that $w_{\mathrm{H}}(u_0) = 1$ is odd, thus $w_{\mathrm{H}}(u_2), w_{\mathrm{H}}(u_4), \cdots$ are all odd and $w_{\mathrm{H}}(u_1)$, $w_{\mathrm{H}}(u_3)$, $\cdots$ are all even.

When k is even, it is known that $w_{\mathrm{H}}(u_{k-1})$ is even, which contradicts $u_{k-1} = 1$. It follows that $U_k = \emptyset$. Hence we have the following conclusion.

Theorem 10. *For any even positive integer k, we have* $\lim_{n\to\infty} \mathbf{cor}(1;1^k) = 0$.

When k is odd, set $u_{2j} = 1$ and $u_{2j+1} = 2^{n-1} + 1$ for $0 \leq j \leq \frac{k-1}{2}$. Then $u_0\cdots u_{k-2}u_{k-1} \in U_k$. It shows that $U_k \neq \emptyset$. For all odd integer k, we define

$$\begin{aligned}
I_k &= \{i_1i_2\cdots i_{k-1} | 2^{i_j} = u_j \oplus u_{j-1}, u_0\cdots u_{k-2}u_{k-1} \in U_k\},\\
I_{k,d} &= \{i_1i_2\cdots i_{k-1} | d = \sum_{j=1}^{k-1} i_j, i_1i_2\cdots i_{k-1} \in I_k\},
\end{aligned}$$

and denote $N_{k,d} = |I_{k,d}|$.

Theorem 11. *For any odd integer $k \geq 3$, we have*

$$\sum_{u_0 u_1 \cdots u_{k-1} \in U_k} \prod_{j=1}^{k-1} \mathbf{Tr}(M_n(u_{j-1}, u_j, 1)) = (-1)^{\frac{k-1}{2}} \cdot 2^{-(k-1)n} \sum_{d=k-1}^{(k-1)(n-1)} N_{k,d} \cdot 2^d.$$

Proof. For any $u_0 \cdots u_{k-1} \in U_k$, by Corollary 5, when $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = 1$, the sign of $Tr(M_n(u_{j-1}, u_j, 1))$ is positive, and when $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = -1$, the sign of $Tr(M_n(u_{j-1}, u_j, 1))$ is negative. So the sign of $\prod_{j=1}^{k-1} Tr(M_n(u_{j-1}, u_j, 1))$ is the same as that of $\prod_{j=1}^{k-1}(w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}))$. Note that $\sum_{j=1}^{k-1}(w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1})) = 0$. It follows that the number of j such that $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = 1$ is equal to that of j such that $w_{\mathrm{H}}(u_j) - w_{\mathrm{H}}(u_{j-1}) = -1$. Thus the sign of $\prod_{j=1}^{k-1} Tr(M_n(u_{j-1}, u_j, 1))$ equals $(-1)^{\frac{k-1}{2}}$. Then we have

$$\begin{aligned}
&\sum_{u_0 \cdots u_{k-1} \in U_k} \prod_{j=1}^{k-1} Tr(M_n(u_{j-1}, u_j, 1)) \\
&= (-1)^{\frac{k-1}{2}} \sum_{i_1 i_2 \cdots i_{k-1} \in I_k} \prod_{j=1}^{k-1} 2^{-(n-i_j)} \\
&= (-1)^{\frac{k-1}{2}} \cdot 2^{-(k-1)n} \sum_{d=k-1}^{(k-1)(n-1)} N_{k,d} \cdot 2^d.
\end{aligned}$$

■

Theorem 12. *For any odd integer $k \geq 3$, if $\lim_{n\to\infty} \mathbf{cor}(1; 1^k)$ exists, then*

1. $\lim_{n\to\infty} \mathbf{cor}(1; 1^k) \geq \frac{1}{3} 2^{-(k-3)}$, *if* $k \equiv 1 \mod 4$;
2. $\lim_{n\to\infty} \mathbf{cor}(1; 1^k) \leq -\frac{1}{3} 2^{-(k-3)}$, *if* $k \equiv 3 \mod 4$.

Proof. For any given $u_0 \cdots u_{k-1} \in U_k$, denote $2^{i_j} = u_j \oplus u_{j-1}$, $1 \leq j \leq k-1$. Then $i_1 i_2 \cdots i_{k-1} \in I_k$. Note that $2^{i_1} \oplus 2^{i_2} \oplus \cdots \oplus 2^{i_{k-1}} = \bigoplus_{j=1}^{k-1}(u_j \oplus u_{j-1}) = 0$, which means that $i_1, i_2, \cdots, i_{k-1}$ can be divided into two identical sets. So $d = \sum_{j=1}^{k-1} i_j$ is always even. Note that $1 \leq i_j \leq n-1$, thus $k-1 \leq d \leq (k-1)(d-1)$. In addition, by the definition of I_k and $I_{k,d}$, for any even integer $k-1 \leq d \leq (n-1)(k-1)$, it is easy to verify that there exist $i_1, i_2, \cdots, i_{k-1}$ such that $i_1 i_2 \cdots i_{k-1} \in I_{k,d}$, that is, $N_{k,d} \geq 1$. For example, when $d = k-1$, set $i_j = 1$ for $1 \leq j \leq k-1$, then $i_1 \cdots i_{k-1} \in I_{k,k-1}$; when $d = (k-1)(n-1)$, set $i_j = n-1$ for $1 \leq j \leq k-1$, then $i_1 \cdots i_{k-1} \in I_{k,(k-1)(n-1)}$. By Theorem 11,

we have

$$\begin{aligned}
&|\lim_{n\to\infty} \mathbf{cor}(1;1^k)| \\
&= \lim_{n\to\infty} 2^{-(k-1)n} \sum_{d=(k-1)/2}^{(k-1)(n-1)/2} N_{k,2d} 2^{2d} \\
&\geq \lim_{n\to\infty} 2^{-(k-1)n} \sum_{d=(k-1)/2}^{(k-1)(n-1)/2} 2^{2d} \\
&= \lim_{n\to\infty} 2^{-(k-1)n} \frac{2^{(k-1)(n-1)+2} - 2^{k-1}}{2^2 - 1} \\
&= \frac{1}{3} 2^{-(k-3)}.
\end{aligned}$$

■

6 Conclusion

In this paper we discussed some properties of linear approximations of the addition modulo $2^n - 1$. We presented an explicit expression for the case when two inputs are involved, and an iterative expression for the case when more than two inputs are involved. For a class of special linear approximations with all masks being equal to 1, we further discussed the limit of their correlations when n approaches infinity. More precisely, let k be the number of inputs of the addition modulo $2^n - 1$, we show that when k is even, the limit is equal to zero, and when k is odd, the limit is bounded by a constant depending on k.

Finally when both n and k approach infinity, we have a conjecture on $\mathbf{cor}(1;1^k)$.

Conjecture 1. $\lim_{k\to\infty}\lim_{n\to\infty} \mathbf{cor}(1;1^k) = 0$.

Acknowledgement

The authors are grateful to Marion Videau and the anonymous reviewers for their constructive comments. We also would like to thank professor Dengguo Feng and professor Dongdai Lin for their instructions.

References

1. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) Eurocrypt 1993. LNCS, vol. 765, pp. 386-397. Springer, Heidelberg (1994)
2. Nyberg, K.: Linear Approximation of Block Ciphers. In: De Santis, A. (ed.) Eurocrypt 1994. LNCS, vol. 950, pp. 439-444. Springer, Heidelberg (1995)
3. Coppersmith, D., Halevi, S., Jutla, C.: Cryptanalysis of Stream Ciphers with Linear Masking. In: Yung, M. (ed.) Crypto 2002. LNCS, vol. 2442, pp. 515-532. Springer, Heidelberg (2002)

4. Watanabe, D., Biryukov, A., Cannière, C.D.: A Distiguishing Attack of SNOW 2.0 with Linear Masking Method. In: Matsui, M., Zuccherato, R. (eds.) SAC 2003. LNCS, vol. 3006, pp. 222-233. Springer, Heidelberg (2004)
5. Lai, X.: On the Design and Security of Block Ciphers. ETH Series in Information Processing, Konstanz: Hartung-Gorre Verlag (1992)
6. GOST 28147-89. Cryptographic Protection for Data Processing Systems, Government Committee of the USSR for Standards (1989)
7. Rivest, R.: The MD5 Message-Digest Algorithm. RFC 1321, MIT and RSA Data Security, Inc., April (1992)
8. Ekdahl, P., Johansson, T.: A New Version of the Stream Cipher SNOW. In: Nyberg, K., Heys, H. (eds.) SAC 2002. LNCS, vol. 1233, pp. 37-46. Springer, Heidelberg (2002)
9. Nyberg, K., Wallén, J.: Improved Linear Distinguishers for SNOW 2.0. In: Robshaw, M.J.B. (ed.) FSE 2006. LNCS, vol. 4047, pp. 144-162. Springer, Heidelberg (2006)
10. Wallén, J.: Linear Approximations of Addition Modulo 2^n. In: Johansson, T. (ed.) FSE 2003. LNCS, vol. 2887, pp. 261-273. Springer, Heidelberg (2003)
11. Berson,T.A.: Differential Cryptanalysis Mod 2^{32} with Applications to MD5. In: Rueppel, R.A. (ed.) Eurocrypt 1992. LNCS, vol. 658, pp. 71-80. Springer, Heidelberg (1993)
12. Lipmaa, H., Moriai, S.: Efficient Algorithms for Computing Differential Properties of Addition. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, pp. 336-350. Springer, Heidelberg (2002)
13. Courtois, N.T., Debraize, B.: Algebraic Description and Simultaneous Linear Approximations of Addition in Snow 2.0. In: Chen, L., Ryan, M.D., Wang, G. (eds.) ICICS 2008. LNCS, vol. 5308, pp. 328-344. Springer, Heidelberg (2008)
14. Maximov, A., Johansson, T.: Fast Computation of Large Distributions and Its Cryptographic Applications. In: Roy, B. (ed.) Asiacrypt 2005. LNCS, vol. 3788, pp. 313-332. Springer, Heidelberg (2005)
15. Nyberg, K.: Correlation Theorems in Cryptanalysis. In Discrete Applied Mathematics, vol. 111, iss. 1-2, pp. 177-188 (2001)
16. Tu, Z., Deng, Y.A.: A Conjecture on Binary String and Its Applications on Constructing Boolean Functions of Optimal Algebraic Immunity. Cryptology ePrint Archive, Report 2009/272 (2009), http://eprint.iacr.org/2009/272
17. Tu, Z., Deng, Y.A.: A Class of 1-Resilient Function with High Nonlinearity and Algebraic Immunity. Cryptology ePrint Archive, Report 2010/179 (2010), http://eprint.iacr.org/2010/179
18. Zimmermann, R.: Efficient VLSI Implementation of Modulo $2^n \pm 1$ Addition and Multiplication. In Proceedings of 14th IEEE Symposium on Computer Arithmetic, pp. 158-167. (1999)
19. Flori, J.P., Randriam, H., Cohen, G., Mesnager, S.: On a Conjecture about Binary Strings Distribution. In: Carlet, C., Pott, A. (eds.) SETA 2010. LNCS, vol. 6338, pp. 346-358. Springer, Heidelberg (2010)
20. Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3, Document 2: ZUC Specification, http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm
21. GSM Algorithms, http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm