Exploiting Linearity of Modular Multiplication

Hamdi Murat Yıldırım(✉)

Department of Computer Technology and Information Systems,
Bilkent University, 06800 Ankara, Turkey
hmurat@bilkent.edu.tr

Abstract. The XOR $\bigoplus$ and the addition $\boxplus$ operations have been widely used as building blocks for many cryptographic primitives. These operations and the multiplication $\odot$ operation are successively used in the design of IDEA and the MESH block ciphers. This work presents several interesting algebraic properties of the multiplication operation. By fixing one operand, we obtain vector valued function $\boldsymbol{g}_Z$ on $\mathbb{Z}_2^n$, associated with $\odot$. In this paper we show that the nonlinearity of $\boldsymbol{g}_Z$ remains the same under some transformations of Z and moreover we give an upper bound for the nonlinearity of $\boldsymbol{g}_Z$ when Z is a power of 2. Under weak-key assumptions, we furthermore present a list of new linear relations for 1-round IDEA cipher, some of directly derived and others algorithmically generated using these relations and known ones. We extend the largest linear weak key class for IDEA cipher with size 2^{23} to derive such a class with sizes 2^{24}. Under the independent key subblocks (subkeys) and weak-key assumptions we derive many linear relations for IDEA cipher using linear relations for 1-round IDEA cipher.

Keywords: IDEA cipher · Nonlinearity · Modular multiplication · Boolean functions · Cryptanalysis

1 Introduction

Block ciphers can be used to build other cryptographic primitives such as stream ciphers, hash functions, message authentication codes and cryptographically secure pseudorandom number generators. Both block ciphers and stream ciphers provide confidentiality, which ensures that information is accessible only to those authorized for access, one of the goals of information security. The addition modulo 2^n ($\boxplus$) and exclusive-OR (XOR) ($\bigoplus$, bitwise addition on modulo 2) are operations and have been widely used as building blocks in many cryptosystems: in RC6, Twofish, MARS, FEAL, SAFER as block ciphers and in ChaCha, Phelix, Snow as stream ciphers. The design of both the International Data Encryption Algorithm (IDEA) [4], the MESH block ciphers [9], WIDEA [3] cipher and RIDEA cipher [12] are based on the successive use of these operations and the multiplication modulo $2^{16}+1$ ($\odot$) operation. Extensive survey of such

D. Slamanig et al. (Eds.): MACIS 2019, LNCS 11989, pp. 249–269, 2020.
https://doi.org/10.1007/978-3-030-43120-4_19

block ciphers whose design following the Lai-Massey design paradigm and their analyses are provided by Nakahara [8]. IDEA was used in Pretty Good Privacy (PGP), which is a widely used computer program that provides confidentiality, authentication and data integrity. There are other applications of multiplication modulo $2^{16}+1$ ($\odot$), which are encountered in residue number systems and Fermat number transform and studies about improving its efficiency [1,6] Some algebraic properties of the operations $\boxplus$, $\odot$ and $\bigoplus$ have already been exploited to cryptanalyze the first 2-round of IDEA in [5]. 15 linear relations for 1-round IDEA cipher, which are derived by considering the linearity of both XOR $\bigoplus$ and the addition $\boxplus$ operation and also linearity of the multiplication $\odot$ for values 0 and 1, are used to derive the linear weak key class for IDEA cipher with size 2^{23} [2]. In this respect, nonlinearity is one of the well-known criterion for evaluating cryptographic Boolean functions. Note that the nonlinearity of both addition and multiplication is considered as high because of their polynomial expressions according to Theorem 3 and 4 in [4]. This is one of the reasons they are used in IDEA cipher. On the other hand, we consider the widely known and accepted measurement for nonlinearity based on the Hamming distance presented in [10] to study the nonlinearity of the multiplication operation. It is proved that this type of nonlinearity of $\odot$ is zero for six cases for $n \geq 2$ [12].

1.1 Contribution

In this paper we view each operation of IDEA cipher as a vector valued boolean function from $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$. Note that the designer of IDEA cipher just considers the case $n = 16$. We fix one operand of each operation to have a vector valued function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ and we use the nonlinearity measurement in [10]. We give an upper bound for its nonlinearity when $Z = 2^k$, $2 \leq k \leq \lceil (n-1)/2 \rceil$. This means that the nonlinearity of the operation $\odot$ is low for small values of k. In fact, it is expected that the nonlinearity of such building blocks of block ciphers should be high. In Sect. 3 for the operation $\odot$, we construct a family of transformations that leaves nonlinearity invariant. In Sect. 4, in addition to 15 linear relations holding with probability one for 1-round IDEA cipher given in [2], we use all cases making nonlinearity of IDEA cipher's operations zero in order to derive such extra 39 linear relations. Moreover, we devise an algorithm to derive 201 more such linear relation considering these 54 relations. Section 5 presents one linear weak key class for IDEA cipher with size 2^{24}, which is extended from a largest linear weak key class for IDEA cipher with size 2^{23} presented in [2] and a method for 438 linear relations for IDEA cipher considering subkeys chosen independently and 255 linear relations for 1-round IDEA cipher.

2 Preliminaries

We shall use the following notations throughout the rest of the paper:

- $x \oplus y = x + y \pmod 2$ for $x, y \in \mathbb{Z}_2$;
- $\mathbb{Z}_2^n = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$ (n-times) denotes the n-dimensional vector space over $\mathbb{Z}_2$;

- When $\boldsymbol{A} = (a_n, a_{n-1}, \ldots, a_1)$ and $\boldsymbol{X} = (x_n, x_{n-1}, \ldots, x_1) \in \mathbb{Z}_2^n$,
  - $\boldsymbol{A} \bigoplus \boldsymbol{X} = (a_n \oplus x_n, a_{n-1} \oplus + x_{n-1}, \ldots, a_1 \oplus x_1)$.
  - the dot product $\boldsymbol{A} \cdot \boldsymbol{X} = (\sum_{i=1}^{n} a_i x_i) \pmod 2 = a_n x_n \oplus a_{n-1} x_{n-1} \oplus \ldots \oplus a_1 x_1$.
  - for $\lambda \in \mathbb{Z}_2$, $l_{\boldsymbol{A},\lambda} : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be the function defined by $l_{\boldsymbol{A},\lambda}(\boldsymbol{X}) = \boldsymbol{A} \cdot \boldsymbol{X} \oplus \lambda$ is called an affine function (respectively linear) if $\lambda \neq 0$ (respectively $\lambda = 0$).

- $\mathcal{A} = \{l_{\boldsymbol{A},\lambda} \mid \boldsymbol{A} \in \mathbb{Z}_2^n, \lambda \in \mathbb{Z}_2\}$ denotes the set of all affine functions on $\mathbb{Z}_2^n$.
- $|S|$ denotes the cardinality of the set S.

It is easy to introduce the addition $\boxplus$, the multiplication $\odot$ and XOR $\oplus$ operations for any positive integer n as functions from $\mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$ (n-times) as follows:
Let $\mathbb{Z}_{2^n} = \{0, 1, \ldots, 2^n - 1\}$, $\mathbb{Z}_{2^n+1}^* = \{1, 2, \ldots, 2^n\}$, and let
$v : \mathbb{Z}_{2^n} \to \mathbb{Z}_2^n$ be a function defined by $v(X) = \boldsymbol{X}$,
where $\boldsymbol{X} = (x_n, \ldots, x_2, x_1)$ is a bit representation of $X = \sum_{i=1}^{n} x_i 2^{i-1} \in \mathbb{Z}_{2^n}$ and
$d : \mathbb{Z}_{2^n+1}^* \to \mathbb{Z}_{2^n}$ be a function defined by $d(X) = X$ if $X \neq 2^n$ and $d(2^n) = 0$.
With this convention, the addition $\pmod{2^n}$, $\boxplus$, the multiplication, $\odot$, $\pmod{2^n + 1}$ and the XOR $\bigoplus$ operations produce the three functions $\boldsymbol{f}$, $\boldsymbol{g}$ and $\boldsymbol{h} : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$:

The addition operation $\boxplus$; $\boldsymbol{f}(\boldsymbol{X}, \boldsymbol{Z}) = \boldsymbol{X} \boxplus \boldsymbol{Z} = v(X + Z \pmod{2^n})$.
The multiplication operation $\odot$; $\boldsymbol{g}(\boldsymbol{X}, \boldsymbol{Z}) = \boldsymbol{X} \odot \boldsymbol{Z} = v(d(d^{-1}(X) d^{-1}(Z) \pmod{2^n + 1}))$, where d^{-1} is the inverse d.
The XOR operation $\bigoplus$; $\boldsymbol{h}(\boldsymbol{X}, \boldsymbol{Z}) = \boldsymbol{X} \bigoplus \boldsymbol{Z} = (x_n \oplus z_n, x_{n-1} \oplus z_{n-1}, \ldots, x_1 \oplus z_1)$.

Notation: for any $Z \in \mathbb{Z}_{2^n}$, $v(Z) = \boldsymbol{Z} \in \mathbb{Z}_2^n$, we denote by $\boldsymbol{f}_Z$, $\boldsymbol{g}_Z$ and $\boldsymbol{h}_Z$ the following vector valued functions $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$: $\boldsymbol{f}_Z(\boldsymbol{X}) = f(\boldsymbol{X}, \boldsymbol{Z})$, $\boldsymbol{g}_Z(\boldsymbol{X}) = g(\boldsymbol{X}, \boldsymbol{Z})$ and $\boldsymbol{h}_Z(\boldsymbol{X}) = h(\boldsymbol{X}, \boldsymbol{Z})$.

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be any function and let $H(f)$ denote the Hamming distance from f to the set of all affine functions $\mathcal{A}$ on $\mathbb{Z}_2^n$. Namely,

$$H(f) = \min\{E_{\boldsymbol{A},\lambda}(f) \mid \boldsymbol{A} \in \mathbb{Z}_2^n, \lambda \in \mathbb{Z}_2\}$$

where $E_{\boldsymbol{A},\lambda}(f) = |\{\boldsymbol{X} \in \mathbb{Z}_2^n \mid f(\boldsymbol{X}) \neq l_{\boldsymbol{A},\lambda}(\boldsymbol{X}) = \boldsymbol{A} \cdot \boldsymbol{X} \oplus \lambda\}|$.
This non-negative integer $H(f)$ attached to $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ is called the nonlinearity of f.

It is clear that $H(f) = 0$ iff f is an affine function. The concept of nonlinearity of arbitrarily vector function $\boldsymbol{F} : \mathbb{Z}_2^n \to \mathbb{Z}_2^k$ was introduced in [10] as follows:
Let $\boldsymbol{F} = (f_k, \ldots, f_1)$, $f_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$, where $1 \leq i \leq k$.

Definition 1.

$$N(\boldsymbol{F}) = \min_{\boldsymbol{C} = (c_1, \ldots, c_k) \in \mathbb{Z}_2^k \setminus \{0\}} \{H(\boldsymbol{C} \cdot \boldsymbol{F} = c_k f_k \oplus c_{k-1} f_{k-1} \oplus \ldots \oplus c_1 f_1)\}$$

Definition 2. *Let f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$. The truth table of f is an ordered 2^n-tuple $(f(\boldsymbol{0}), f(\boldsymbol{1}), \ldots, f(\boldsymbol{2^n - 1})) \in \mathbb{Z}_2^{2^n}$, which is denoted by T_f.*

3 Nonlinearity of Multiplication Operation

It is a well-known fact that for every $Z \in \mathbb{Z}_{2^n}$, the nonlinearity $N(\boldsymbol{f}_Z)$ and $N(\boldsymbol{h}_Z)$ of $\boldsymbol{f}_Z$ and $\boldsymbol{h}_Z$ are equal to 0. However, the nonlinearity $N(\boldsymbol{g}_Z)$ of the vector function $\boldsymbol{g}_Z$ is not zero for every $Z \in \mathbb{Z}_{2^n}$. The following theorem, which is proved in [12], gives a list of Z values such that $N(\boldsymbol{g}_Z)$ is zero.

Theorem 1. *For $n \geq 2$, the nonlinearity $N(\boldsymbol{g}_Z)$ of the vector function $\boldsymbol{g}_Z(\boldsymbol{X}) = \boldsymbol{g}(\boldsymbol{X}, \boldsymbol{Z})$ is zero for $Z = 0,\ 1,\ 2,\ 2^{n-1},\ 2^{n-1}+1,\ 2^n - 1$.*

Remark 1. When $n \leq 12$, we checked that the values of Z in *Theorem 1* were the only ones for which $N(\boldsymbol{g}_Z) = 0$. It is an open problem whether this is the case for $n > 12$.

Using the following proposition, it is enough to calculate $N(\boldsymbol{g}_Z)$ for given Z value to determine one, two or three related values for the vector function of the multiplication operation having the same nonlinearity.

Proposition 1

(1) For $n \in \mathbb{Z}_+$ such that $\gcd(A, 2^n + 1) = 1$, we have $N(\boldsymbol{g}_A) = N(\boldsymbol{g}_B)$ when $AB \equiv 1 \pmod{2^n + 1}$.
(2) $N(\boldsymbol{g}_A) = N(\boldsymbol{g}_B)$ when $A + B \equiv 0 \pmod{2^n + 1}$.
(3) $N(\boldsymbol{g}_{2^k}) = N(\boldsymbol{g}_{2^s})$ when $k + s = n$ for $k, s \geq 0$.

Proof. For part 1, we have $\boldsymbol{g}_B(\boldsymbol{X}) = \boldsymbol{g}_{A^{-1}}(\boldsymbol{X})$ since $AB \equiv 1 \pmod{2^n + 1}$. $N(\boldsymbol{g}_A) = N((\boldsymbol{g}_A)^{-1}) = N(\boldsymbol{g}_B)$ follows from *Theorem 1* in [10].

For part 2, the case $A = B = 0$ is trivial. For other (A, B) pairs, one can use the obvious relation $v^{-1}(\boldsymbol{g}_A(\boldsymbol{X})) + v^{-1}(\boldsymbol{g}_B(\boldsymbol{X})) \equiv 0 \pmod{2^n + 1}$ to complete the proof of this part.

For part 3, for $k + s = n$, we obtain that $2^s(2^k + 2(2^s)^{-1}) \equiv 2^n + 2 \equiv 1 \pmod{2^n+1}$. Here $(2^s)^{-1} \equiv 2^k + 2(2^s)^{-1} \pmod{2^n+1}$ and we have $(2^s)^{-1} + 2^k \equiv 0 \pmod{2^n + 1}$. By part *2*, we get $N(\boldsymbol{g}_{(2^s)^{-1}}) = N(\boldsymbol{g}_{2^k})$. From *Theorem 1* in [10], we know that $N(\boldsymbol{g}_{(2^s)^{-1}}) = N(\boldsymbol{g}_{2^s})$. This completes the proof. □

Since there is no efficient algorithm to compute $N(\boldsymbol{g}_Z)$ in general, we can look for an upper bound for some values of Z. The following theorem gives a partial solution to the problem:

Theorem 2. *For $n \geq 3$ and $2 \leq k \leq \lceil (n-1)/2 \rceil$, we have $N(\boldsymbol{g}_Z) \leq 2^{k-1}$ when*

$$\text{(i) } Z = 2^k \text{ and } Z = 2^{n-k}.$$
$$\text{(ii) } Z + 2^k \equiv 0 \pmod{2^n + 1}.$$
$$\text{(iii) } Z2^k \equiv 1 \pmod{2^n + 1}.$$

Proof. Assume that $n \geq 3$ and $2 \leq k \leq \lceil (n-1)/2 \rceil$. For every $\boldsymbol{X} \in \mathbb{Z}_2^n$,

let $\boldsymbol{g}_{2^k}(\boldsymbol{X}) = (\boldsymbol{g}_{2^k}{}^{(n)}(\boldsymbol{X}), \ldots, \boldsymbol{g}_{2^k}{}^{(2)}(\boldsymbol{X}), \boldsymbol{g}_{2^k}{}^{(1)}(\boldsymbol{X}))$, and $\boldsymbol{g}_{2^k}{}^{(i)}(\boldsymbol{X})$ be i^{th} coordinate function of $\boldsymbol{g}_{2^k}(\boldsymbol{X})$.

Since $\boldsymbol{g}_2(0) = 2^n - 1$, $\boldsymbol{g}_2(2^{n-1}) = 0$ and $\boldsymbol{g}_2(2j)$ is even and $\boldsymbol{g}_2(2j+1)$ is odd for all $j \in \{1, \ldots, 2^{n-1} - 1\}$, the truth table of ${\boldsymbol{g}_2}^{(1)}$, $T_{{\boldsymbol{g}_2}^{(1)}} = S^{2^n}$, where $S^{2^n} = (s_{2^n}, \ldots, s_1) = (1, 0, \ldots, 0, 0, 1, \ldots, 1) \in \mathbb{Z}_2^{2^n}$, $s_{2^n} = 1$, $s_{2^{n-1}} = 0, s_{2^{n-1}+m} = 0$ and $s_{2^{n-1}-m} = 1$ for all $m \in \{1, \ldots, 2^{n-1} - 1\}$. Then the truth table of $T_{{\boldsymbol{g}_{2^k}}^{(1)}}$ becomes $(\underbrace{S^{2^{n-k+1}}, \ldots, S^{2^{n-k+1}}}_{(2^k-1)-times})$. Therefore, $\boldsymbol{g}_2^{(1)}(\boldsymbol{X}) = \overline{x_1}\,\overline{x_2} \ldots \overline{x_{n-1}} \oplus x_n$ and $\boldsymbol{g}_{2^k}^{(1)}(\boldsymbol{X}) = \overline{x_1}\,\overline{x_2} \ldots \overline{x_{n-k}} \oplus x_{n-k+1}$ according to their truth tables, where $\overline{x_i} = x_i \oplus 1$. We know that $\boldsymbol{g}_{2^k}^{(1)}(\boldsymbol{X}) \oplus \boldsymbol{g}_{2^k}^{(2)}(\boldsymbol{X}) = \boldsymbol{g}_{2^{k-1}}^{(1)}(\boldsymbol{X})$ since by the proof of *Theorem* 1, $y_2 \oplus y_1 = x_1$ for $\boldsymbol{g}_2(\boldsymbol{X}) = \boldsymbol{Y}$. The hamming distance between $\boldsymbol{g}_{2^k}^{(1)}(\boldsymbol{X})$ and x_{n-k+1} is 2^k.

This implies that $N(\boldsymbol{g}_{2^k}^{(1)}(\boldsymbol{X})) \leq 2^k$. By *Theorem 12* in [13], $2^k \leq N(\boldsymbol{g}_{2^k}^{(1)}(\boldsymbol{X}))$ since the term $x_1 \ldots x_{n-k}$ is not properly covered (see *Definition 9* in [13]) by any other terms in $\boldsymbol{g}_{2^k}^{(1)}(\boldsymbol{X})$. Then, $N({\boldsymbol{g}_{2^k}}^{(1)}(\boldsymbol{X})) = 2^k$ and we get $N({\boldsymbol{g}_{2^k}}^{(1)}(\boldsymbol{X}) \oplus {\boldsymbol{g}_{2^k}}^{(2)}(\boldsymbol{X})) = N({\boldsymbol{g}_{2^{k-1}}}^{(1)}(\boldsymbol{X})) = 2^{k-1}$. Hence, $N(\boldsymbol{g}_{2^k}(\boldsymbol{X})) \leq 2^{k-1}$ by using *Definition* 1.

The remaining parts of this theorem can be easily proven by *Proposition* 1. □

Remark 2. When $n \leq 16$, we checked that the upper bound was tight, namely $N(\boldsymbol{g}_Z) = 2^{k-1}$, for the choices of Z above. It is an open problem whether this is the case when $n > 16$.

4 Linear Relations for 1-Round IDEA

4.1 Linear Relations for Operations

For a fixed operation $\bowtie \in \{\boxplus, \odot, \bigoplus\}$ and $z \in \mathbb{Z}_{2^n}$, we consider mapping $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ defined by $\mathbf{X} \to \mathbf{X} \bowtie \mathbf{Z} = \mathbf{Y}$ ($\mathbf{Z} = v(z)$).

We have discussed the nonlinearity of this vector valued multiplication function for some special cases. When $\bowtie$ is the XOR operation $\bigoplus$, it is clear that the dot product is distributive over $\bigoplus$, and therefore we get $\mathbf{A} \cdot (\mathbf{X} \bigoplus \mathbf{Z}) = \mathbf{A} \cdot \mathbf{X} \oplus \mathbf{A} \cdot \mathbf{Z} = \mathbf{A} \cdot \mathbf{Y}$, or equivalently

$$\mathbf{A} \cdot \mathbf{X} \oplus \mathbf{A} \cdot \mathbf{Y} \oplus \mathbf{A} \cdot \mathbf{Z} = 0 \text{ for every } \mathbf{A} \in \mathbb{Z}_2^n \tag{1}$$

Similarly for $\bowtie = \boxplus$, it is easy to see that $\mathbf{1} \cdot (\mathbf{X} \boxplus \mathbf{Z}) = \mathbf{1} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Z} = \mathbf{1} \cdot \mathbf{Y}$, or equivalently

$$\mathbf{1} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} = 0 \tag{2}$$

So for $\mathbf{X} \bowtie \mathbf{Z} = \mathbf{Y}$ it makes sense to search relations in the form

$$\mathbf{A} \cdot \mathbf{X} \oplus \mathbf{B} \cdot \mathbf{Y} \oplus \mathbf{C} \cdot \mathbf{Z} \oplus \lambda = 0 \text{ for some } \mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{Z}_2^n \text{ and } \lambda \in \mathbb{Z}_2. \tag{3}$$

As it can be seen from the proof of Theorem 1 [12], we get the following linear relations for every $\mathbf{X} = v(x) \in \mathbb{Z}_2^n$ such that $\mathbf{X} \odot \mathbf{Z} = \mathbf{Y}$:

$$\mathbf{1} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} \oplus 1 = 0 \text{ for } z \in \{0, 1\} \tag{4}$$

$$\mathbf{3} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} \oplus 1 = 0 \text{ for } z \in \{2^{n-1}, 2^{n-1}+1\} \tag{5}$$

$$\mathbf{1} \cdot \mathbf{X} \oplus \mathbf{3} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} = 0 \text{ for } z \in \{2, 2^n - 1\}, \tag{6}$$

where $v(z) = \mathbf{Z}$.

4.2 A New List of Linear Relations

For 1-round IDEA, 15 linear relations hold with probability one are derived due to the linearity of operations of IDEA (see equations in 1, 2, 4) in paper [2]. These relations marked by (*) are given in Table 1. Note that for each round of IDEA, four of the six 16-bit key subblocks $\mathbf{Z}_i$'s ($i = \{1, 4, 5, 6\}$) are involved by the multiplication operation $\odot$. In order to derive each of these linear relation, at least one of those key subblocks were restricted to take 0 and 1 (see Example 1 and Table 1). Additional key values, $2, 2^n - 1, 2^{n-1}$ and $2^{n-1} + 1$, making the nonlinearity of the vector valued function $\mathbf{g}_z$ of $\odot$ zero were discovered in [12]. Similar to the work in paper [2], we take into account 0, 1 or these key values as round multiplicative keys to derive extra 39 linear relations, which are not marked by (*) in Table 1. All these 54 linear relations (holding with probability one) with the related key subblocks restrictions are listed in Table 1. Notice that each linear relation for 1-round IDEA should be based on linear relations for the operations used in IDEA cipher. Hence under some round key subblocks restrictions (weak key assumptions), we can express a linear relation for 1-round IDEA as:

$$\phi \star Z \oplus \psi \star X \oplus \omega \star Y \oplus \lambda = 0$$

where Z, X and Y are round key, input and output of 1-round IDEA, respectively and $\lambda \in \mathbb{Z}_2$, $\phi \star Z = \boldsymbol{\phi}_1 \cdot \mathbf{Z}_1 \oplus \ldots \oplus \boldsymbol{\phi}_6 \cdot \mathbf{Z}_6$, $\psi \star X = \boldsymbol{\psi}_1 \cdot \mathbf{X}_1 \oplus \ldots \oplus \boldsymbol{\psi}_4 \cdot \mathbf{X}_4$ and $\omega \star Y = \boldsymbol{\omega}_1 \cdot \mathbf{Y}_1 \oplus \ldots \oplus \boldsymbol{\omega}_4 \cdot \mathbf{Y}_4$ such that $\phi = (\boldsymbol{\phi}_1, \ldots, \boldsymbol{\phi}_6)$, $\psi = (\boldsymbol{\psi}_1, \ldots, \boldsymbol{\psi}_4)$ and $\omega = (\boldsymbol{\omega}_1, \ldots, \boldsymbol{\omega}_4)$ for $\boldsymbol{\phi}_i$, $\boldsymbol{\psi}_i$ and $\boldsymbol{\omega}_i \in \mathbb{Z}_2^{16}$. Here $\boldsymbol{\phi}_i, \boldsymbol{\psi}_i$ and $\boldsymbol{\omega}_i$ are masks for $\mathbf{Z}_i = v(z_i), \mathbf{X}_i = v(x_i)$ and $\mathbf{Y}_i = v(y_i)$, respectively and $x_i, y_i, z_i \in \mathbb{Z}_{2^n}$.

For the sake of clarity, let us derive the 24th linear relation in Table 1, one of 15 linear relations found in [2]:

Example 1: Adding first two output of 1-round IDEA, namely $\mathbf{Y}_1$ and $\mathbf{Y}_2$ (see Fig. 2 in Appendix A), we have

$$\mathbf{Y}_1 \bigoplus \mathbf{Y}_2 = (\mathbf{X}_1 \bigoplus \mathbf{Z}_1) \bigoplus (\mathbf{X}_3 \boxplus \mathbf{Z}_3)$$

When $\mathbf{Z}_1 = (0, \ldots, 0)$ or $\mathbf{Z}_1 = (1, \ldots, 1)$, the least significant bit of $\mathbf{Y}_1 = \mathbf{X}_1 \odot \mathbf{Z}_1$ is $\mathbf{1} \cdot \mathbf{Y}_1 = \mathbf{1} \cdot \mathbf{X}_1 \oplus \mathbf{1} \cdot \mathbf{Z}_1 \oplus 1$ from the Eq. 4 and the least significant bit of $\mathbf{Y}_3 = \mathbf{X}_3 \boxplus \mathbf{Z}_3$ is $\mathbf{1} \cdot \mathbf{Y}_3 = \mathbf{1} \cdot \mathbf{X}_3 \oplus \mathbf{1} \cdot \mathbf{Z}_3$ from the Eq. 2. The addition of $\mathbf{1} \cdot \mathbf{Y}_1$ and $\mathbf{1} \cdot \mathbf{Y}_2$ becomes

$$\mathbf{1} \cdot \mathbf{Y}_1 \oplus \mathbf{1} \cdot \mathbf{Y}_2 = \mathbf{1} \cdot \mathbf{X}_1 \oplus \mathbf{1} \cdot \mathbf{Z}_1 \oplus \mathbf{1} \cdot \mathbf{X}_3 \oplus \mathbf{1} \cdot \mathbf{Z}_3 \oplus 1 \tag{7}$$

When $\mathbf{Z}_1 = (0, \ldots, 0)$ or $(1, \ldots, 1)$, one can represent this equation as a linear relation for 1-round IDEA

$$(\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{0}, \mathbf{0}) \star Z \oplus (\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}) \star X \oplus (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}) \star Y \oplus \mathbf{1} = 0$$

Table 1. List of linear relations for 1-round IDEA given in [2] (indicated by *) and derived. Here k is a non-negative integer, $-1 \equiv 0 \bmod (2^{16}+1)$, $-2^{15} \equiv 2^{15}+1 \bmod (2^{16}+1)$ and $-2 \equiv 2^{16}-1 \bmod (2^{16}+1)$.

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
1	* $(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	0	–	–	–	∓ 1	–	∓ 1	66
2	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	0	–	–	–	$\mp 2^{15}$	–	∓ 1	66
3	* $(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},1,\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	0	–	–	–	–	∓ 1	∓ 1	66
4	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	1	∓ 2	–	$2k$	–	$\mp 2^{15}$	∓ 2	48
5	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{3})$	1	∓ 2	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2	31
6	* $(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	0	–	–	–	∓ 1	∓ 1	–	66
7	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	0	–	–	–	$\mp 2^{15}$	∓ 1	–	66
8	* $(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	1	–	–	–	–	–	∓ 1	82
9	* $(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	1	–	–	–	∓ 1	–	–	81
10	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{3})$	0	–	$2k$	–	∓ 2	–	–	79
11	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{3})$	1	–	–	–	$\mp 2^{15}$	–	–	81
12	* $(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	1	–	–	–	–	∓ 1	–	81
13	* $(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	1	–	–	–	∓ 1	∓ 1	∓ 1	51
14	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{3})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	1	–	–	–	$\mp 2^{15}$	∓ 1	∓ 1	51
15	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	0	–	∓ 2	$2k$	∓ 1	$\mp 2^{15}$	∓ 2	33
16	* $(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	1	∓ 1	–	–	–	∓ 1	∓ 1	51
17	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	1	∓ 2	–	$2k$	–	$\mp 2^{15}$	∓ 1	49
18	* $(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	1	∓ 1	–	–	∓ 1	∓ 1	–	51
19	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	1	∓ 1	–	–	$\mp 2^{15}$	∓ 1	–	51
20	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	–	–	∓ 1	∓ 1	–	51
21	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	–	–	$\mp 2^{15}$	∓ 1	–	51
22	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 2	–	$2k$	∓ 1	$\mp 2^{15}$	–	49
23	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 2	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	–	49
24	* $(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 1	–	–	–	–	–	81
25	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 2	–	$2k$	–	–	–	79
26	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	–	–	–	–	–	81
27	* $(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	1	∓ 1	–	–	∓ 1	–	∓ 1	51
28	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	1	∓ 1	–	–	$\mp 2^{15}$	–	∓ 1	51
29	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{0})$	0	∓ 2	–	$2k$	∓ 1	–	∓ 1	49
30	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{0})$	0	∓ 2	–	$2k$	$\mp 2^{15}$	–	∓ 1	49
31	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	1	$\mp 2^{15}$	–	–	∓ 1	–	∓ 1	51
32	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	1	$\mp 2^{15}$	–	–	$\mp 2^{15}$	–	∓ 1	51
33	* $(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	0	∓ 1	–	–	–	∓ 1	–	66
34	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	–	–	–	∓ 1	–	66
35	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	1	∓ 2	–	$2k$	–	$\mp 2^{15}$	–	64
36	* $(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 1	–	–	∓ 1	∓ 1	∓ 1	36
37	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k$	∓ 1	$\mp 2^{15}$	∓ 1	34
38	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1	34
39	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	–	–	∓ 1	∓ 1	∓ 1	36

(*continued*)

Table 1. (*continued*)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
40	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	–	–	$\mp 2^{15}$	∓ 1	∓ 1	36
41	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 2	–	–	∓ 1	$\mp 2^{15}$	∓ 2	34
42	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 2	–	–	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2	34
43	* $(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 1	–	–	–	–	∓ 1	66
44	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	0	$\mp 2^{15}$	–	–	–	–	∓ 1	66
45	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 2	–	$2k$	–	–	∓ 1	64
46	* $(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 1	–	–	∓ 1	–	–	66
47	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{3})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 1	–	–	$\mp 2^{15}$	–	–	66
48	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	–	–	∓ 1	–	–	66
49	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{3})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	–	–	$\mp 2^{15}$	–	–	66
50	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	1	∓ 2	–	$2k$	∓ 1	–	–	64
51	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	1	∓ 2	–	$2k$	$\mp 2^{15}$	–	–	64
52	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	1	∓ 1	$2k$	–	∓ 2	–	–	64
53	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	1	$\mp 2^{15}$	$2k$	–	∓ 2	–	–	64
54	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	1	∓ 2	$2k$	$2k$	∓ 2	–	–	62

Example 2: From the Table 1, when $\mathbf{Z}_j = v(z_j), z_1 = \mp 2$, $z_4 = \mp 2^{15}$, $z_5 = \mp 2^{15}$ and $z_6 = \mp 2$ for $\phi = (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$, $\psi = (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$, $\omega = (\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$ and $\lambda = 0$ we have

$$\mathbf{1}\cdot\mathbf{Z}_1 \oplus \mathbf{1}\cdot\mathbf{Z}_2 \oplus \mathbf{1}\cdot\mathbf{Z}_4 \oplus \mathbf{1}\cdot\mathbf{Z}_5 \oplus \mathbf{1}\cdot\mathbf{Z}_6 \oplus \mathbf{1}\cdot\mathbf{X}_1 \oplus \mathbf{1}\cdot\mathbf{X}_2 \oplus \mathbf{3}\cdot\mathbf{X}_4 = \mathbf{3}\cdot\mathbf{Y}_2$$

This relation, one of new 39 linear relations derived, is the 42th linear relation in Table 1.

4.3 New Linear Relations Algorithmically Generated

Let us consider the 35th and the 45th linear relations for 1-round IDEA in Table 1 to obtain a new relation which is not listed in Table 1.

For the 35th linear relation $(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$ with key subblocks restrictions $z_1 = \mp 2$, $z_3 = 2k$ and $z_5 = \mp 2^{15}$ and the 45th linear relation $(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0}) \rightarrow (\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$ with restrictions $z_1 = \mp 2$, $z_3 = 2k$ and $z_6 = \mp 1$, we have two corresponding Eqs. (8) and (9) respectively

$$\mathbf{1}\cdot\mathbf{Z}_1 \oplus \mathbf{1}\cdot\mathbf{Z}_2 \oplus \mathbf{2}\cdot\mathbf{Z}_3 \oplus \mathbf{1}\cdot\mathbf{Z}_5 \oplus \mathbf{1}\cdot\mathbf{X}_1 \oplus \mathbf{1}\cdot\mathbf{X}_2 \oplus \mathbf{2}\cdot\mathbf{X}_3 \oplus \mathbf{1}\cdot\mathbf{Y}_2 \oplus \mathbf{1}\cdot\mathbf{Y}_3 \oplus \mathbf{1} = 0 \quad (8)$$

$$\mathbf{1}\cdot\mathbf{Z}_1 \oplus \mathbf{1}\cdot\mathbf{Z}_2 \oplus \mathbf{2}\cdot\mathbf{Z}_3 \oplus \mathbf{1}\cdot\mathbf{Z}_6 \oplus \mathbf{1}\cdot\mathbf{X}_1 \oplus \mathbf{1}\cdot\mathbf{X}_2 \oplus \mathbf{3}\cdot\mathbf{X}_3 \oplus \mathbf{3}\cdot\mathbf{Y}_1 \oplus \mathbf{3}\cdot\mathbf{Y}_2 \oplus \mathbf{1}\cdot\mathbf{Y}_4 \oplus \mathbf{1} = 0 \quad (9)$$

Equations (8) and (9) key subblocks restrictions do not give any conflicts and they can be combined (by adding them in mod 2) to obtain the following linear relation candidate:

$$\mathbf{1}\cdot\mathbf{Z}_5 \oplus \mathbf{1}\cdot\mathbf{Z}_6 \oplus \mathbf{1}\cdot\mathbf{X}_3 \oplus \mathbf{3}\cdot\mathbf{Y}_1 \oplus \mathbf{2}\cdot\mathbf{Y}_2 \oplus \mathbf{1}\cdot\mathbf{Y}_3 \oplus \mathbf{1}\cdot\mathbf{Y}_4 \oplus \mathbf{1} = 0 \quad (10)$$

We have used many inputs for 1-round IDEA to check that linear relation in (10) holds with probability one under the key subblocks restrictions $z_1 = \mp 2$, $z_3 = 2k$, $z_5 = \mp 2^{15}$ and $z_6 = \mp 1$. In fact, we have observed that only key restrictions $z_5 = \mp 2^{15}$ and $z_6 = \mp 1$ are enough to make this linear relation hold with probability one according to our experiments. Hence we have devised a new algorithm to find new linear relations for 1-round IDEA based on a set of 54 linear relations for 1-round IDEA in Table 1. Considering these known linear relations, we found additional 201 new linear relations for 1-round IDEA (see Table 5, Appendix B) using the following algorithm:

Algorithm 1. *An algorithm for finding new linear relations for 1-round IDEA based on existing linear ones:*

Let $\mathcal{S}$ be the set of linear relations with their key subblocks restrictions.
Step 1 All pair of $\mathcal{S}$ whose key subblocks values coincided are chosen.
Step 2 Any chosen pairs are also combined (directly added in mod 2).
Step 3 Each linear relation candidates in Step 2 is tested using 10 million test vectors to check whether it is a linear relation or not.
Step 4 The ones (i.e. candidate linear relations) passing Step 3 added to $\mathcal{S}$.
Step 5 Previous steps are repeated until there is no increase in the number of the elements of the set $\mathcal{S}$.
Step 6 Key restrictions of each linear relation in $\mathcal{S}$ are checked to remove unnecessary restrictions using 50000 test vectors.

We note that the last step has been added as a result of comments provided by Nakahara [7]. All 54 linear relations in Table 1 can be derived by hand calculation considering all combinations of subblock outputs of 1-round IDEA, $\mathbf{Y}_i$ and subblock keys of 1-round IDEA, $\mathbf{Z}_i$ which give us linear relations for the operations used in IDEA cipher. By using Algorithm 1, it is possible to obtain linear relations that can not be derived in this way.

5 Linear Weak Key Classes for IDEA

As indicated in Table 2, three linear relations, namely the 24th, the 33th and the 12th relations in Table 1 were successively used to find a linear relation for 8,5-round IDEA holding with probability one [2]. Because of key subblocks restrictions done in each round, this linear relation is satisfied for all 64-bit plaintexts provided that ranges of zero key bits' indices of a 128-bit master key bits are between 0–25, 29–71, and 75–110. Such key is a member of a class of weak keys with size 2^{23} since each of the remaining 23 bits of the master key can take 0 or 1.

Note that this has been the largest known class of weak keys based on a linear relation for 8,5-round IDEA. Hence this linear relation can be regarded as the best linear relation for 8,5-round IDEA. Based on this linear relation, we have found a new class of weak keys with cardinality 2^{24}. For this construction, we replace the first round linear relation $(\mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{0}) \rightarrow (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0})$ with $(\{\mathbf{1}, \mathbf{3}\}, \mathbf{0}, \mathbf{1}, \mathbf{0}) \rightarrow (\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0})$ (see Table 3). For the former and latter relations, $\mathbf{Z}_1^{(1)}$ is chosen $\mathbf{0} = (0, \ldots, 0)$ or $\mathbf{1} = (1, \ldots, 1)$ and $\mathbf{Z}_1^{(1)}$ is restricted

Table 2. Each round linear relation and ranges for indices of zero key bits of IDEA master key are considered to derive the linear relation $(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$ for 8,5-round IDEA satisfied by a linear weak key class with cardinality 2^{23}.

Round i	Linear relation $\psi \rightarrow \omega$	$\mathbf{Z}_1^{(i)}$	$\mathbf{Z}_5^{(i)}$
1	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	0–14	–
2	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	96–110	57–71
3	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	–	50–64
4	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	82–96	–
5	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	75–89	11–25
6	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	–	4–18
7	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	36–50	–
8	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	29–44	93–107
8,5	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	–	–

Table 3. Each round linear relation and ranges for indices of zero key bits of IDEA master key are considered to derive the linear relation $(\{\mathbf{1},\mathbf{3}\},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$ for 8,5-round IDEA satisfied by a linear weak key class with cardinality 2^{24}.

Round i	Linear relation $\psi \rightarrow \omega$	$\mathbf{Z}_1^{(i)}$	$\mathbf{Z}_5^{(i)}$
1	$(\{\mathbf{1},\mathbf{3}\},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	1–15	–
2	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	96–110	57–71
3	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	–	50–64
4	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	82–96	–
5	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	75–89	11–25
6	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	–	4–18
7	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	36–50	–
8	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	29–44	93–107
8,5	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	–	–

to $\mathbf{0}$ or $\mathbf{2}^{15}$, respectively. Note that $(\{\mathbf{1},\mathbf{3}\},\mathbf{0},\mathbf{1},\mathbf{0}) = (\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$ (respectively $(\{\mathbf{1},\mathbf{3}\},\mathbf{0},\mathbf{1},\mathbf{0}) = (\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0})$) if $\mathbf{Z}_1^{(1)}$ is equal to $\mathbf{0}$ (respectively $\mathbf{Z}_1^{(1)} = \mathbf{2}^{15}$). Therefore, zero key bits' indices of a 128-bit key are between 1–25, 29–71, and 75–110. Then linear relation $(\{\mathbf{1},\mathbf{3}\},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$ for the 8,5-round IDEA holds with probability one (Table 3) and there are 2^{24} such keys. We haven't discovered other linear relations in Tables 1 and 5 similar to the best linear relation giving a large class of weak keys because of the following reasons:

- If we compare Table 1 with Table 5 in Appendix B, then it can be seen that for most cases, linear relations in Table 1 derived in [2] have less key restrictions than others.
- In Table 1, each of linear relations numbered with $8, 9, 12, 24, 26$ has one key subblock restriction and each of linear relations numbered with $1, 2, 3, 6, 7, 10,$

$25, 34, 43, 44, 46, 47, 48, 49$ has two key subblocks restrictions. There aren't any linear relations with one key subblock restriction in Table 5, but there are linear relations numbered with $98, 125, 159, 185$ and 216 having two key subblocks restrictions in Table 5. In order to find a linear relation for 8,5-round IDEA providing a large class of weak keys, it is better to use those relations (with less key subblocks restrictions) listed above. However, it is not possible to derive such linear relation for 8,5-round IDEA using these relations and linear relations with key subblocks ∓ 2 or $\mp 2^{15}$ restrictions other than those derived in [2] in both Tables 1 and 5. Because

(i) we faced with key subblocks restrictions giving conflicts, that is, some bits of the master 128-bit of IDEA are both 0 and 1 due to key subblocks restrictions of two linear relations considered for two different rounds, especially when a key subblock of one linear relation is equal to 0 or 1 and a key subblock of other one is chosen as ∓ 2 or $\mp 2^{15}$;

(ii) we haven't found successive linear relations for many linear relations with key subblock restriction like ∓ 2 or $\mp 2^{15}$ while deriving multi round linear relation. For example, for the 75th linear relation in Table 5, namely $(\mathbf{3}, \mathbf{3}, \mathbf{0}, \mathbf{1}) \rightarrow (\mathbf{2}, \mathbf{3}, \mathbf{2}, \mathbf{2})$ there aren't any linear relations whose input mask is equal to $(\mathbf{2}, \mathbf{3}, \mathbf{2}, \mathbf{2})$ in both Tables 1 and 5.

Because these limitations to derive new linear relations the block cipher, we assume that key subblocks (subkeys) are independent. Then under weak-key assumptions we consider each linear relation for 1-round IDEA cipher from Tables 1 and 5 as two vertices connected by a single edge having a direction. In this manner we have a directed graph and using suitable functions of Digraph module from *S*ageMath [11] we find many paths with length 8 and then consider last 0.5 round's relations in order to get 438 linear relations for 8.5-round IDEA cipher. In Table 6 (Appendix B), 50 of them with less number of key bits restriction for the master key, whose size is 832-bits (considering all 52 16-bit key subblocks) are listed. Note that second relation in this table $(\mathbf{1}, \mathbf{1}, \mathbf{0}, \mathbf{0}) \longrightarrow (\mathbf{3}, \mathbf{1}, \mathbf{0}, \mathbf{0})$ is a linear relation for 8.5-round IDEA cipher and associated with a class of weak keys with the cardinality 2^{586} whenever key subblocks (subkeys) are chosen independently. Note that the key space with size 2^{832} is extremely larger than this class.

6 Conclusion

In this paper we give several new properties on the nonlinearity of the multiplication operation $\odot$. Using its invariance properties, it is possible to calculate the nonlinearity just for one value of the associated vector function to learn one, two or three different values giving the same the nonlinearity. Furthermore, we give an upper bound for its nonlinearity when values are power of two. It is low for small powers. In fact, it is expected that the nonlinearity of such building blocks of block ciphers should be high. We devise an algorithm to find a new set of linear relations for 1-round IDEA using a set of linear relations directly derived and a set of known linear relations. We present one linear weak key class

slightly bigger than one known in the literature. Assuming that all key subblocks are chosen independently, we generate a new set of linear relations for full IDEA cipher using linear relations for 1-round IDEA. All these findings extend the related work done by Daemen et al. and they are meaningful to understand how properties of building components of a cipher are related to its security.

A Appendix: IDEA Block Cipher

The graph of the encryption of IDEA can be seen in Fig. 1. The key scheduling algorithm and the list of all 16-bit key subblocks (Table 4) are given in Appendix.

A.1 Key Schedule and Decryption Algorithm

For a given 128-bit key, 52 16-bit key subblocks are generated for the encryption. For the construction of these subblocks, the first step is to partition given 128-bit key into 8 pieces and assign them as the first 8 key subblocks of the 52 subblocks: $\mathbf{Z}_1^{(1)}, \mathbf{Z}_2^{(1)}, .., \mathbf{Z}_6^{(1)}, \mathbf{Z}_1^{(2)}, \mathbf{Z}_2^{(2)}, .., \mathbf{Z}_6^{(2)}, .., \mathbf{Z}_1^{(8)}, \mathbf{Z}_2^{(8)}, .., \mathbf{Z}_6^{(8)}, \mathbf{Z}_1^{(9)}, \mathbf{Z}_2^{(9)}, \mathbf{Z}_3^{(9)}, \mathbf{Z}_4^{(9)}$.

Then the key under the consideration is cyclically shifted to the left by 25 positions. The resulting key block is again partitioned into eight subblocks that are assigned to the next eight subblock keys. This process is repeated until all 52 subblock keys are derived.

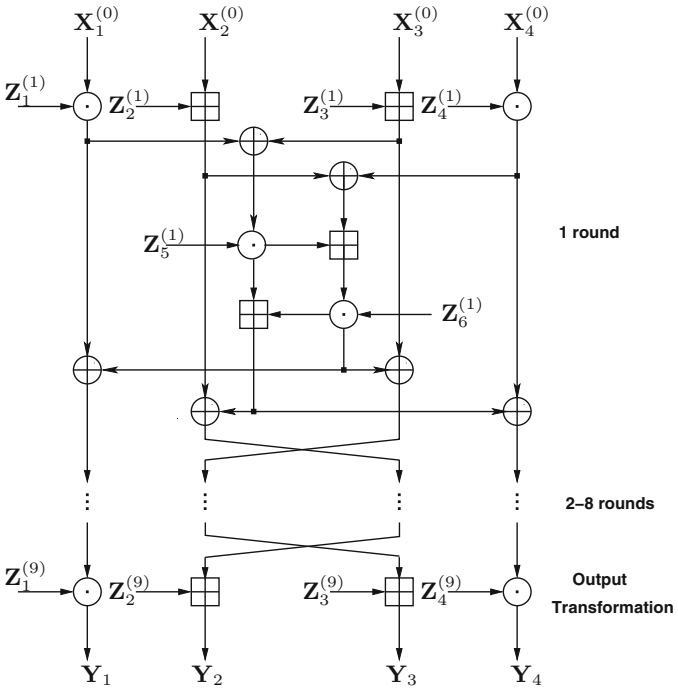

Fig. 1. Computational graph for the encryption process of the IDEA cipher

Table 4. 128-bit IDEA master key bits indices starts from 0 and ends with 127 (indexed left to right). Range of indices of this key used for each of 52 subblock keys generated by the key scheduling algorithm

r	$\mathbf{Z}_1$	$\mathbf{Z}_2$	$\mathbf{Z}_3$	$\mathbf{Z}_4$	$\mathbf{Z}_5$	$\mathbf{Z}_6$
1	0–15	16–31	32–47	48–63	64–79	80–95
2	96–111	112–127	25–40	41–56	57–72	73–88
3	89–104	105–120	121–8	9–24	50–65	66–81
4	82–97	98–113	114–1	2–17	18–33	34–49
5	75–90	91–106	107–122	123–10	11–26	27–42
6	43–58	59–74	100–115	116–3	4–19	20–35
7	36–51	52–67	68–83	84–99	125–12	13–28
8	29–44	45–60	61–76	77–92	93–108	109–124
9	22–37	38–53	54–69	70–85	–	–

A.2 The MA-Structure and 1-Round IDEA Cipher

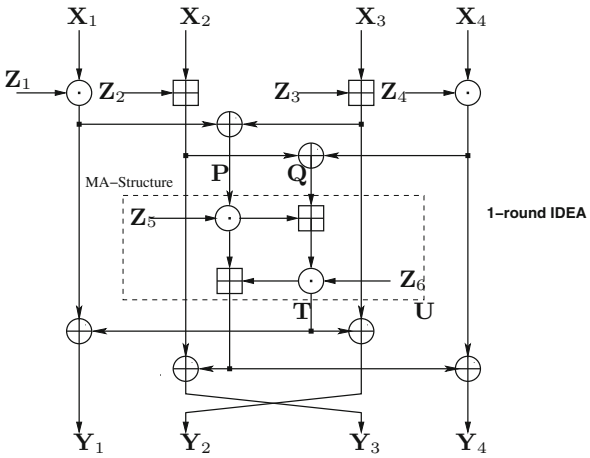

Fig. 2. Computational graph for the encryption process of 1-round IDEA cipher

Let us denote round key, input and output for the 1-round IDEA block cipher (see Fig. 2) as $Z = (\mathbf{Z}_1, \ldots, \mathbf{Z}_6)$, $X = (\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4)$ and $Y = (\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Y}_3, \mathbf{Y}_4)$, where $\mathbf{Z}_i$, $\mathbf{X}_i$, $\mathbf{Y}_i \in \mathbb{Z}_2^{16}$, respectively. Then we have:

$$\begin{aligned} \mathbf{Y}_1 &= (\mathbf{X}_1 \odot \mathbf{Z}_1) \oplus \mathbf{T}. \qquad & \mathbf{Y}_2 &= (\mathbf{X}_3 \boxplus \mathbf{Z}_3) \oplus \mathbf{T}. \\ \mathbf{Y}_3 &= (\mathbf{X}_2 \boxplus \mathbf{Z}_2) \oplus \mathbf{U}. \qquad & \mathbf{Y}_4 &= (\mathbf{X}_4 \odot \mathbf{Z}_4) \oplus \mathbf{U}. \end{aligned} \tag{11}$$

We have the following equations for two input subblocks of the MA-structure $\mathbf{P}$ and $\mathbf{Q}$ and two output subblocks of the MA-structure $\mathbf{U}$ and $\mathbf{T}$ (see Fig. 2):

$$\mathbf{P} = (\mathbf{X}_1 \odot \mathbf{Z}_1) \oplus (\mathbf{X}_3 \boxplus \mathbf{Z}_3) \text{ and } \mathbf{Q} = (\mathbf{X}_2 \boxplus \mathbf{Z}_2) \oplus (\mathbf{X}_4 \odot \mathbf{Z}_4). \tag{12}$$

$$\mathbf{U} = (\mathbf{P} \odot \mathbf{Z}_5) \boxplus \mathbf{T} \text{ and } \mathbf{T} = [(\mathbf{P} \odot \mathbf{Z}_5) \boxplus \mathbf{Q}] \odot \mathbf{Z}_6. \tag{13}$$

It is easy to see that $\mathbf{Y}_1 \oplus \mathbf{Y}_2 = \mathbf{P}$ and $\mathbf{Y}_3 \oplus \mathbf{Y}_4 = \mathbf{Q}$.

B Appendix: New Linear Relations for 1-Round IDEA and 8.5-Round IDEA

Table 5. List of new linear relations for 1-round IDEA, based on linear relations of Table 1, generated by Algorithm 1. Here k is a non-negative integer, $-1 \equiv 0 \bmod (2^{16}+1)$, $-2^{15} \equiv 2^{15}+1 \bmod (2^{16}+1)$ and $-2 \equiv 2^{16}-1 \bmod (2^{16}+1)$.

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
55	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	–	–	62
56	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{0})$	1	–	–	$2k$	∓ 1	$\mp 2^{15}$	∓ 1	50
57	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	–	$2k+1$	∓ 1	∓ 1	∓ 2	34
58	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	–	–	$2k$	∓ 1	∓ 1	∓ 2	49
59	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1	35
60	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	–	∓ 2	46
61	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1})$	1	–	–	$2k+1$	–	$\mp 2^{15}$	∓ 1	65
62	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k+1$	∓ 1	∓ 1	∓ 2	33
63	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	–	$2k$	–	$\mp 2^{15}$	∓ 2	49
64	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	1	–	–	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 2	49
65	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2	32
66	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	1	∓ 2	$2k$	$2k+1$	∓ 2	–	–	62
67	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k+1$	$2k$	∓ 2	∓ 1	∓ 1	32
68	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k$	$2k$	∓ 2	∓ 1	∓ 1	32
69	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	–	–	$2k+1$	∓ 1	–	∓ 2	64
70	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	1	–	–	$2k+1$	∓ 1	$\mp 2^{15}$	–	65
71	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	–	$2k$	$\mp 2^{15}$	–	∓ 2	49
72	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 2	–	$2k$	$\mp 2^{15}$	∓ 1	–	49
73	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 1	–	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 2	34
74	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1	33
75	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1	33
76	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2	32
77	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	$\mp 2^{15}$	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	–	50
78	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	0	–	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2	49

(*continued*)

Table 5. (*continued*)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
79	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	–	$2k$	$\mp 2^{15}$	∓ 1	∓ 2	34
80	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	–	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 1	35
81	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 1	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	–	48
82	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k$	$2k+1$	∓ 2	∓ 1	–	47
83	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	1	∓ 2	–	$2k$	–	∓ 1	∓ 2	48
84	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	1	∓ 2	–	$2k$	–	∓ 1	–	64
85	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1	32
86	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	0	∓ 2	–	$2k+1$	∓ 1	–	∓ 2	48
87	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	–	–	$2k$	$\mp 2^{15}$	–	∓ 2	64
88	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	–	$2k+1$	∓ 1	∓ 1	∓ 2	34
89	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	∓ 1	$2k+1$	–	∓ 2	∓ 1	–	49
90	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	∓ 1	$2k$	$2k+1$	∓ 2	–	∓ 2	47
91	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	1	$\mp 2^{15}$	–	$2k+1$	–	$\mp 2^{15}$	–	65
92	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 2	–	$2k+1$	∓ 1	–	–	64
93	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2	32
94	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	–	–	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2	49
95	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2	32
96	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 2	–	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 1	34
97	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	1	∓ 1	–	$2k$	–	$\mp 2^{15}$	∓ 1	50
98	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{3})$	1	–	$2k+1$	–	∓ 2	–	–	79
99	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	1	–	$2k$	–	∓ 2	∓ 1	–	64
100	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	–	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 2	34
101	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k+1$	$2k$	∓ 2	–	∓ 1	47
102	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k$	∓ 1	∓ 1	∓ 1	34
103	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	0	∓ 1	$2k$	–	∓ 2	–	∓ 1	49
104	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	1	∓ 2	–	$2k+1$	–	$\mp 2^{15}$	–	64
105	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	–	$2k+1$	–	–	∓ 2	64
106	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	–	$2k$	∓ 1	$\mp 2^{15}$	–	50
107	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	–	$2k$	$\mp 2^{15}$	∓ 1	∓ 2	34
108	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k$	$2k+1$	∓ 2	–	∓ 1	47
109	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	–	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 1	35
110	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	0	$\mp 2^{15}$	$2k+1$	–	∓ 2	–	–	64
111	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	–	48
112	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k$	$2k$	∓ 2	–	∓ 2	46
113	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 1	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	–	48
114	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1	32
115	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 2	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	–	49
116	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	–	∓ 2	47
117	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{2})$	1	–	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1	48

(*continued*)

Table 5. (*continued*)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
118	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{2})$	1	–	$2k$	–	∓ 2	–	∓ 1	64
119	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 2	–	$2k+1$	–	–	∓ 1	64
120	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{3})$	1	–	$2k$	$2k$	∓ 2	$\mp 2^{15}$	–	63
121	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2	32
122	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	–	–	$2k+1$	$\mp 2^{15}$	–	∓ 2	64
123	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 1	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2	34
124	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 2	–	$2k$	–	–	∓ 2	63
125	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0})$	0	–	–	$2k+1$	–	$\mp 2^{15}$	–	80
126	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	1	$\mp 2^{15}$	–	$2k$	–	$\mp 2^{15}$	∓ 1	50
127	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	1	–	–	$2k+1$	–	∓ 1	∓ 2	64
128	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	–	∓ 2	–	∓ 1	49
129	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2	31
130	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	–	$2k+1$	–	–	∓ 2	64
131	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	–	$2k$	∓ 1	$\mp 2^{15}$	–	50
132	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 1	–	$2k$	–	∓ 1	∓ 2	49
133	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	1	$\mp 2^{15}$	–	–	–	∓ 1	∓ 1	51
134	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	∓ 1	$2k$	$2k$	∓ 2	–	∓ 2	47
135	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{0})$	1	–	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1	50
136	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	0	∓ 2	–	$2k+1$	$\mp 2^{15}$	–	∓ 2	48
137	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{2})$	0	–	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1	48
138	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	–	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2	34
139	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k$	$2k$	∓ 2	∓ 1	∓ 2	31
140	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	–	–	$2k$	$\mp 2^{15}$	∓ 1	∓ 2	49
141	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 1	$2k+1$	$2k+1$	∓ 2	–	∓ 2	47
142	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2	33
143	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	1	–	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2	49
144	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k+1$	$2k+1$	∓ 2	∓ 1	–	47
145	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1	33
146	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{2})$	0	–	$2k$	$2k$	∓ 2	–	∓ 2	62
147	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	$\mp 2^{15}$	$2k+1$	–	∓ 2	∓ 1	–	49
148	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 1	34
149	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2	32
150	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	1	–	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	–	65
151	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k$	$2k$	∓ 2	$\mp 2^{15}$	–	47
152	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2	34
153	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	–	$2k$	–	–	∓ 2	64
154	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	0	–	$2k+1$	–	∓ 2	∓ 1	–	64
155	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 1	–	$2k$	∓ 1	$\mp 2^{15}$	∓ 2	34
156	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1	33

(*continued*)

Table 5. (*continued*)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
157	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	–	50
158	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1	35
159	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	0	–	–	$2k$	–	–	∓ 2	79
160	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	–	$2k$	–	∓ 1	∓ 2	49
161	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	1	∓ 2	–	$2k+1$	–	∓ 1	∓ 1	49
162	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	–	$2k$	–	$\mp 2^{15}$	–	65
163	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k$	–	∓ 2	∓ 1	∓ 1	34
164	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	1	∓ 1	$2k+1$	–	∓ 2	–	∓ 1	49
165	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	$2k$	∓ 2	–	∓ 2	47
166	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k$	$2k$	∓ 2	∓ 1	–	47
167	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	–	$2k+1$	∓ 1	–	∓ 2	49
168	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 1	–	$2k+1$	–	∓ 1	∓ 2	49
169	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 2	–	$2k+1$	∓ 1	∓ 1	–	49
170	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	–	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2	34
171	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{2})$	1	∓ 2	$2k+1$	$2k+1$	∓ 2	–	∓ 1	47
172	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	–	∓ 2	47
173	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	–	48
174	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 2	–	$2k+1$	$\mp 2^{15}$	–	–	64
175	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	0	–	–	$2k+1$	–	$\mp 2^{15}$	∓ 2	64
176	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{2})$	0	–	$2k+1$	–	∓ 2	–	∓ 1	64
177	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{3})$	0	–	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	–	63
178	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	1	–	–	$2k$	–	∓ 1	∓ 2	64
179	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	–	$2k$	–	–	∓ 2	64
180	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{2})$	0	–	$2k$	$2k+1$	∓ 2	–	∓ 2	62
181	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k$	$\mp 2^{15}$	∓ 1	∓ 1	34
182	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k+1$	–	∓ 2	∓ 1	∓ 1	34
183	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	–	$2k$	∓ 1	$\mp 2^{15}$	∓ 2	34
184	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	–	47
185	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k+1$	–	–	–	79
186	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	1	∓ 1	–	$2k+1$	–	$\mp 2^{15}$	∓ 2	49
187	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{2})$	0	–	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2	47
188	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k$	$2k$	∓ 2	∓ 1	∓ 2	32
189	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 1	$2k+1$	$2k$	∓ 2	–	∓ 2	47
190	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 2	–	$2k$	–	$\mp 2^{15}$	∓ 1	49
191	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	–	∓ 2	–	∓ 1	49
192	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0})$	1	∓ 2	–	$2k+1$	∓ 1	–	∓ 1	49
193	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	–	$2k+1$	∓ 1	–	∓ 2	49
194	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	–	$2k+1$	–	∓ 1	∓ 2	49

(*continued*)

Table 5. (*continued*)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
195	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{2})$	1	–	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2	47
196	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	–	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1	34
197	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	–	47
198	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k+1$	–	∓ 2	$\mp 2^{15}$	∓ 2	32
199	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{2})$	0	–	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 2	47
200	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 1	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2	34
201	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 2	–	$2k$	–	∓ 1	∓ 1	49
202	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{2})$	1	–	$2k+1$	$2k$	∓ 2	–	∓ 2	62
203	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	–	∓ 2	∓ 1	∓ 1	34
204	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k$	–	∓ 2	$\mp 2^{15}$	∓ 2	32
205	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{2})$	1	–	$2k$	$2k+1$	∓ 2	∓ 1	∓ 2	47
206	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	–	$2k$	∓ 1	–	∓ 2	49
207	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	1	$\mp 2^{15}$	–	$2k+1$	–	$\mp 2^{15}$	∓ 2	49
208	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2	32
209	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k$	$2k+1$	∓ 2	∓ 1	∓ 1	32
210	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	$2k$	∓ 2	∓ 1	∓ 2	32
211	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k+1$	$2k$	∓ 2	∓ 1	–	47
212	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	–	$2k+1$	$\mp 2^{15}$	–	∓ 2	49
213	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	–	∓ 2	47
214	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	–	∓ 2	∓ 1	∓ 1	34
215	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	1	∓ 2	$2k+1$	$2k$	∓ 2	–	–	62
216	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	0	–	–	$2k+1$	–	–	∓ 2	79
217	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k$	$2k+1$	∓ 2	∓ 1	∓ 2	32
218	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{2})$	0	–	$2k$	–	∓ 2	∓ 1	∓ 1	49
219	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 2	–	$2k+1$	–	∓ 1	–	64
220	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{2})$	1	–	$2k+1$	–	∓ 2	∓ 1	∓ 1	49
221	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	–	–	$2k$	∓ 1	–	∓ 2	64
222	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 1	–	$2k$	–	$\mp 2^{15}$	∓ 2	49
223	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	–	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2	34
224	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	–	47
225	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 1	32
226	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	–	–	$2k+1$	∓ 1	∓ 1	∓ 2	49
227	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2	32
228	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	–	$2k$	∓ 1	–	∓ 2	49
229	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 2	–	$2k$	∓ 1	∓ 1	–	49
230	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0})$	1	∓ 2	–	$2k+1$	$\mp 2^{15}$	–	∓ 1	49
231	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	–	$2k+1$	$\mp 2^{15}$	–	∓ 2	49
232	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2	32
233	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 2	–	$2k+1$	$\mp 2^{15}$	∓ 1	–	49

(*continued*)

Table 5. (*continued*)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6	# of free bits
234	$(\mathbf{1,2,2,1,1,1})$	$(\mathbf{1,2,3,1})$	$(\mathbf{0,3,2,2})$	1	∓ 1	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 2	32
235	$(\mathbf{1,1,2,1,1,1})$	$(\mathbf{1,1,2,1})$	$(\mathbf{0,3,0,0})$	1	∓ 1	–	$2k$	∓ 1	∓ 1	∓ 2	34
236	$(\mathbf{1,3,0,1,1,0})$	$(\mathbf{1,2,0,1})$	$(\mathbf{0,1,2,3})$	0	∓ 1	$2k$	–	∓ 2	∓ 1	–	49
237	$(\mathbf{0,2,3,1,1,1})$	$(\mathbf{0,2,3,1})$	$(\mathbf{1,2,2,2})$	0	–	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2	47
238	$(\mathbf{1,0,2,0,1,1})$	$(\mathbf{1,0,3,0})$	$(\mathbf{0,1,1,1})$	0	∓ 2	–	$2k+1$	–	$\mp 2^{15}$	∓ 1	49
239	$(\mathbf{0,2,2,1,1,1})$	$(\mathbf{0,2,2,1})$	$(\mathbf{3,0,2,2})$	1	–	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2	47
240	$(\mathbf{0,2,2,1,1,1})$	$(\mathbf{0,3,2,1})$	$(\mathbf{3,0,2,2})$	0	–	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2	47
241	$(\mathbf{0,2,3,1,1,1})$	$(\mathbf{0,3,3,1})$	$(\mathbf{1,2,2,2})$	1	–	$2k$	$2k$	∓ 2	∓ 1	∓ 2	47
242	$(\mathbf{1,0,2,1,1,0})$	$(\mathbf{1,0,3,1})$	$(\mathbf{0,1,0,1})$	0	∓ 2	–	$2k+1$	∓ 1	$\mp 2^{15}$	–	49
243	$(\mathbf{1,2,3,1,1,1})$	$(\mathbf{1,2,3,1})$	$(\mathbf{2,1,2,2})$	0	∓ 1	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2	32
244	$(\mathbf{1,0,3,1,0,1})$	$(\mathbf{1,0,3,3})$	$(\mathbf{1,3,1,0})$	0	∓ 1	–	$2k$	$\mp 2^{15}$	–	∓ 2	49
245	$(\mathbf{1,1,0,1,1,1})$	$(\mathbf{1,1,0,3})$	$(\mathbf{0,1,0,0})$	0	∓ 1	–	–	$\mp 2^{15}$	∓ 1	∓ 1	36
246	$(\mathbf{0,3,2,1,0,1})$	$(\mathbf{0,3,3,1})$	$(\mathbf{0,2,3,2})$	1	–	$2k+1$	$2k+1$	∓ 2	–	∓ 2	62
247	$(\mathbf{1,1,3,1,1,1})$	$(\mathbf{1,1,3,1})$	$(\mathbf{2,3,0,0})$	0	∓ 2	–	$2k+1$	∓ 1	∓ 1	∓ 1	34
248	$(\mathbf{1,3,2,1,0,1})$	$(\mathbf{1,2,3,1})$	$(\mathbf{3,3,3,2})$	1	∓ 2	$2k$	$2k$	∓ 2	–	∓ 1	47
249	$(\mathbf{1,2,2,1,1,1})$	$(\mathbf{1,3,2,1})$	$(\mathbf{0,1,2,2})$	0	∓ 2	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1	32
250	$(\mathbf{1,2,2,1,1,1})$	$(\mathbf{1,2,2,1})$	$(\mathbf{0,1,2,2})$	1	∓ 2	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1	32
251	$(\mathbf{1,2,1,1,0,0})$	$(\mathbf{1,2,1,1})$	$(\mathbf{1,1,3,3})$	0	∓ 1	$2k+1$	–	∓ 2	–	–	64
252	$(\mathbf{1,2,2,1,1,1})$	$(\mathbf{3,3,3,1})$	$(\mathbf{0,3,2,2})$	0	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	∓ 1	∓ 2	32
253	$(\mathbf{1,1,2,1,1,1})$	$(\mathbf{3,1,2,1})$	$(\mathbf{0,3,0,0})$	1	$\mp 2^{15}$	–	$2k$	∓ 1	∓ 1	∓ 2	34
254	$(\mathbf{1,2,2,1,1,1})$	$(\mathbf{3,2,3,1})$	$(\mathbf{0,3,2,2})$	1	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 2	32
255	$(\mathbf{1,3,0,1,1,0})$	$(\mathbf{3,2,0,1})$	$(\mathbf{0,1,2,3})$	0	$\mp 2^{15}$	$2k$	–	∓ 2	∓ 1	–	49

Table 6. 50 linear relations with less number of key bits restriction for 8.5-round IDEA cipher. Here each row is associated with one such relation, a linear mask for each round input and one for the last round output, namely ciphertext are provided. Last column shows the number of key bits from the master key that are not restricted, that is, each such bit can be either 0 or 1. Note that mask $(\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d})$ is denoted by abcd. When $832 - 556 = 276$ key bits are restricted according to Tables 1 and 2, twenty second row of this table gives a linear relation for 8.5-round IDEA cipher involving plaintext bit $(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0}) \star (\mathbf{X}_1^0, \mathbf{X}_2^0, \mathbf{X}_3^0, \mathbf{X}_4^0) = \mathbf{1} \cdot \mathbf{X}_2^0$ and ciphertext bits added $(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{3}) \star (\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Y}_3, \mathbf{Y}_4) = \mathbf{1} \cdot \mathbf{Y}_1 \oplus \mathbf{2} \cdot \mathbf{Y}_2 \oplus \mathbf{1} \cdot \mathbf{Y}_3 \oplus \mathbf{3} \cdot \mathbf{Y}_4$ (see Sect. 4.2 and Fig. 1 in Appendix A).

#	1st round's input mask	2nd round's input mask	3rd round's input mask	4th round's input mask	5th round's input mask	6th round's input mask	7th round's input mask	8th round's input mask	Last 0.5 round's input mask	*Cipher text* mask	# of free key bits
1	1100	0110	0110	1010	1100	0110	1010	1100	0110	0110	586
2	1010	1100	0110	0110	1010	1100	0110	1010	1100	3100	586
3	1010	1100	0110	0110	1010	1100	0110	1010	1100	1100	586
4	0110	1010	1100	0110	0110	1010	1100	0110	1010	1010	586
5	0110	1010	1100	0110	0110	1010	1100	0110	1010	3010	585

(*continued*)

Table 6. (*continued*)

#	1st round's input mask	2nd round's input mask	3rd round's input mask	4th round's input mask	5th round's input mask	6th round's input mask	7th round's input mask	8th round's input mask	Last 0.5 round's input mask	*Cipher text* mask	# of free key bits
6	0100	0001	0010	1011	1110	1101	0100	0001	0010	0010	579
7	1001	0101	0011	1001	0101	0011	1001	0101	0011	0011	577
8	0101	0011	1001	0101	0011	1001	0101	0011	1001	1001	577
9	1001	0101	0011	1001	0101	0011	1001	0101	0011	0013	576
10	0101	0011	1001	0101	0011	1001	0101	0011	1001	3001	576
11	0101	0011	1001	0101	0011	1001	0101	0011	1001	1003	576
12	0100	0001	0010	1011	1110	3101	0100	0001	0010	0010	576
13	0101	0011	1001	0101	0011	1001	0101	0011	1001	3003	575
14	1111	1111	1111	1111	1111	1111	1111	1111	1111	1111	562
15	0011	1001	0101	0011	1001	0101	0011	1001	0101	0101	562
16	1111	1111	1111	1111	1111	1111	1111	1111	1111	3111	561
17	1111	1111	1111	1111	1111	1111	1111	1111	1111	1113	561
18	0011	1001	0101	0011	1001	0101	0011	1001	0101	0103	561
19	1111	1111	1111	1111	1111	1111	1111	1111	1111	3113	560
20	1133	0100	0001	0010	3211	1133	0100	0001	0010	0010	557
21	0100	0001	0010	3211	1133	0100	0001	0010	3211	1211	557
22	0100	0001	0010	3211	1133	0100	0001	0010	3211	1213	556
23	3311	1133	3311	1133	3311	1133	3311	1133	3311	1311	545
24	1133	3311	1133	3311	1133	3311	1133	3311	1133	1131	545
25	3311	1133	3311	1133	3311	1133	3311	1133	3311	1313	544
26	1133	3311	1133	3311	1133	3311	1133	3311	1133	3133	544
27	3211	1133	0100	0001	0010	3211	1133	0100	0001	0001	540
28	3211	1133	0100	0001	0010	3211	1133	0100	0001	0003	539
29	0001	0010	3211	1133	0100	0001	0010	3211	1133	1131	539
30	0010	3211	1133	0100	0001	0010	3211	1133	0100	0100	538
31	0001	0010	3211	1133	0100	0001	0010	3211	1133	3133	538
32	1101	0100	0001	0010	1011	1110	1101	0100	0001	0001	534
33	1110	1101	0100	0001	0010	1011	1110	1101	0100	0100	533
34	1101	0100	0001	0010	1011	1110	1101	0100	0001	0003	533
35	0010	1011	1110	1101	0100	0001	0010	1011	1110	1110	533
36	0001	0010	1011	1110	1101	0100	0001	0010	1011	1011	533
37	0010	1011	1110	1101	0100	0001	0010	1011	1110	3110	532
38	0001	0010	1011	1110	1101	0100	0001	0010	1011	3011	532
39	0001	0010	1011	1110	1101	0100	0001	0010	1011	1013	532
40	3101	0100	0001	0010	1011	1110	3101	0100	0001	0001	531
41	0001	0010	1011	1110	1101	0100	0001	0010	1011	3013	531
42	3101	0100	0001	0010	1011	1110	3101	0100	0001	0003	530
43	0010	1011	1110	3101	0100	0001	0010	1011	1110	1110	530
44	0001	0010	1011	3110	1101	0100	0001	0010	1011	1011	530
45	0001	0010	1011	1110	3101	0100	0001	0010	1011	1011	530
46	0010	1011	1110	3101	0100	0001	0010	1011	1110	3110	529
47	0001	0010	1011	3110	1101	0100	0001	0010	1011	3011	529
48	0001	0010	1011	3110	1101	0100	0001	0010	1011	1013	529
49	0001	0010	1011	1110	3101	0100	0001	0010	1011	3011	529
50	0001	0010	1011	1110	3101	0100	0001	0010	1011	1013	529

References

1. Chaves, R., Sousa, L.: Improving residue number system multiplication with more balanced moduli sets and enhanced modular arithmetic structures. IET Comput. Digital Tech. **1**(5), 472–480 (2007)
2. Daemen, J., Govaerts, R., Vandewalle, J.: Weak keys for IDEA. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 224–231. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48329-2_20
3. Junod, P., Macchetti, M.: Revisiting the IDEA philosophy. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 277–295. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03317-9_17
4. Lai, X.: On the Design and Security of Block Cipher. ETH Series in Information Processing, vol. 1. Hartung-Gorre Verlag, Konstanz (1992)
5. Meier, W.: On the security of the IDEA block cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 371–385. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48285-7_32
6. Modugu, R., Choi, M., Park, N.: A fast low-power modulo $2^n + 1$ multiplier design. In: IEEE Instrumentation and Measurement Technology Conference, I2MTC 2009, pp. 951–956. IEEE (2009)
7. Nakahara Jr., J.: Personal communication, November 2004
8. Nakahara Jr., J.: Lai-Massey Cipher Designs: History. Design Criteria and Cryptanalysis. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-68273-0
9. Nakahara Jr., J., Rijmen, V., Preneel, B., Vandewalle, J.: The MESH block ciphers. In: Chae, K.-J., Yung, M. (eds.) WISA 2003. LNCS, vol. 2908, pp. 458–473. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24591-9_34
10. Nyberg, K.: On the construction of highly nonlinear permutations. In: Rueppel, R.A. (ed.) EUROCRYPT 1992. LNCS, vol. 658, pp. 92–98. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-47555-9_8
11. SageMath, the Sage Mathematics Software System (Version 6.7). The Sage Developers (2015). http://www.sagemath.org
12. Yıldırım, H.M.: Nonlinearity properties of the mixing operations of the block cipher IDEA. In: Johansson, T., Maitra, S. (eds.) INDOCRYPT 2003. LNCS, vol. 2904, pp. 68–81. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-24582-7_5
13. Zhang, X.-M., Zheng, Y., Imai, H.: Duality of Boolean functions and its cryptographic significance. In: Han, Y., Okamoto, T., Qing, S. (eds.) ICICS 1997. LNCS, vol. 1334, pp. 159–169. Springer, Heidelberg (1997). https://doi.org/10.1007/BFb0028472