ALGEBRAIC PROPERTIES OF THE OPERATIONS USED IN BLOCK CIPHER IDEA

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

HAMDİ MURAT YILDIRIM

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF DOCTOR OF PHILOSOPHY
IN
MATHEMATICS

MARCH 2007

Approval of the Graduate School of Natural and Applied Sciences

Prof. Dr. Canan ÖZGEN
Director

I certify that this thesis satisfies all the requirements as a thesis degree of Doctor of Philosophy.

Prof. Dr. Zafer NURLU
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Doctor of Philosophy.

Prof. Dr. Ersan AKYILDIZ
Supervisor

Examining Committee Members

Assoc. Prof. Dr. Ali DOĞANAKSOY	(METU,MATH)	_____
Prof. Dr. Ersan AKYILDIZ	(METU,MATH)	_____
Assist. Prof. Dr. Emrah ÇAKÇAK	(METU,IAM)	_____
Assist. Prof. Dr. Ali Aydın SELÇUK	(Bilkent Univ.,CS)	_____
Assoc. Prof. Melek D. YÜCEL	(METU,EEE)	_____

I hearby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required, I have fully cited and referenced all material and results that are not original to this work.

Name Lastname : Hamdi Murat YILDIRIM

Signature :

ABSTRACT

ALGEBRAIC PROPERTIES OF THE OPERATIONS USED IN BLOCK CIPHER IDEA

Yıldırım, Hamdi Murat
Ph.D., Department of Mathematics
Supervisor: Prof. Dr. Ersan Akyıldız

March 2007, 68 pages

In this thesis we obtain several interesting algebraic properties of the operations used in the block cipher IDEA which are important for cryptographic analyzes. We view each of these operations as a function from $\mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$. By fixing one of variables $v(z) = \mathbf{Z}$ in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$, we define functions $\mathbf{f}_z$ and $\mathbf{g}_z$ from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$ for the addition $\boxplus$ and the multiplication $\odot$ operations, respectively. We first show that the nonlinearity of $\mathbf{g}_z$ remains the same under some transformations of z. We give an upper bound for the nonlinearity of $\mathbf{g}_{2^k}$, where $2 \leq k < n-1$. We list all linear relations which make the nonlinearity of $\mathbf{f}_z$ and $\mathbf{g}_z$ zero and furthermore, we present all linear relations for $\mathbf{g}_z$ having a high probability. We use these linear relations to derive many more linear relations for 1-round IDEA. We also devise also a new algorithm to find a set of new linear relations for 1-round IDEA based on known linear relations. Moreover, we extend the largest known linear class of weak keys with cardinality 2^{23} to two classes with cardinality 2^{24} and 2^{27}.

Finally, we obtain several interesting properties of the set $\{(\mathbf{X}, \mathbf{X} \bigoplus \mathbf{A}) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n \,|\, (\mathbf{X} \bowtie \mathbf{Z}) \bigoplus ((\mathbf{X} \bigoplus \mathbf{A}) \bowtie \mathbf{Z}) = \mathbf{B}\}$ for varying $\mathbf{A}, \mathbf{B}$ and $\mathbf{Z}$ in $\mathbb{Z}_2^n$, where $\bowtie \in \{\bigodot, \boxplus\}$. By using some of these properties, we present impossible differentials for 1-round IDEA and Pseudo-Hadamard Transform.

Keywords: Boolean Functions, Nonlinearity, Modular Arithmetic, Block Ciphers, Cryptanalysis.

ÖZ

IDEA BLOK ŞİFRELEME SİSTEMİNDE KULLANILAN İŞLEMLERİN CEBİRSEL ÖZELLİKLERİ

Yıldırım, Hamdi Murat
Doktora, Matematik Bölümü
Tez Danışmanı: Prof. Dr. Ersan Akyıldız
Mart 2007, 68 sayfa

Bu tezde blok şifreleme sistemi IDEA da kullanılan işlemlerinin kriptografik analizler açısından önemli birçok ilginç cebirsel özelliklerini elde ediyoruz. Bu işlemlerden her birini $\mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$ ye bir fonksiyon olarak bakıyoruz. $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ daki değişkenlerden birisi olan z yi sabitleyip, $\mathbb{Z}_2^n$ den $\mathbb{Z}_2^n$ ye $\mathbf{f}_z$ and $\mathbf{g}_z$ fonksiyonlarını toplama $\boxplus$ and çarpma $\odot$ işlemleri için tanımlıyoruz. İlk $\mathbf{g}_z$ nin doğrusalsızlığının, z nin bazı dönüşümleri altında aynı kaldığını gösteriyoruz. $2 \leq k < n-1$ olduğunda, $\mathbf{g}_{2^k}$ nın doğrusalsızlığı için bir üst sınır veriyoruz. $\mathbf{f}_z$ ve $\mathbf{g}_z$ nin doğrusalsızlığını sıfır yapan tüm doğrusal bağıntılarını listeliyoruz ve ek olarak $\mathbf{g}_z$ nin yüksek bir olasılığa sahip tüm doğrusal bağıntılarını sunuyoruz. Bu doğrusal bağıntıları IDEA nın birçok 1-tur IDEA doğrusal bağıntılarını bulmak için kullanıyoruz. Ayrıca bilinen doğrusal bağıntılara dayalı, yeni doğrusal bağıntılar kümesi bulmak için yeni bir algoritma tasarlıyoruz. Üstelik 2^{23} elemanlı en büyük, bilinen doğrusal zayıf anahtar sınıfını 2^{24} ve 2^{27} elemanlı iki yeni bir sınıfa

genişletiyoruz.

Son olarak, $\mathbb{Z}_2^n$ elemanı, değişen $\mathbf{A}, \mathbf{B}$ and $\mathbf{Z}$ ve $\bowtie \in \{\bigodot, \boxplus\}$ için $\{(\mathbf{X}, \mathbf{X} \bigoplus \mathbf{A}) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n \,|\, (\mathbf{X} \bowtie \mathbf{Z}) \bigoplus ((\mathbf{X} \bigoplus \mathbf{A}) \bowtie \mathbf{Z}) = \mathbf{B}\}$ kümesinin bir kaç ilginç özelliklerini elde ediyoruz. Bu özelliklerden bazısını kullanarak 1-tur IDEA ve Pseudo-Hadamard Dönüşüm'leri için imkansız farkları sunuyoruz.

Anahtar Kelimeler: Boole Fonksiyonları, Doğrusalsızlık, Modüler Aritmetik, Blok Şifreleme, Kripto analiz.

ACKNOWLEDGEMENTS

I would like to express my deepest gratitude to my supervisor Prof. Dr. Ersan Akyıldız for his constant support, his stimulating not only scientific but also general advices, his encouragement and patient guidance helped me in all the time of my research and writing of this thesis.

My colleagues in the Department of Computer Technology and Information Systems at Bilkent University, my teachers in the Department of Mathematics at METU and my friends also deserve many thanks.

I would like to thank everybody who has been important to the successful realization of this thesis, as well as expressing my apology that I could not mention personally one by one.

All of my work would have never been done properly without continuous support and encouragement especially from my mother and my sister İnci.

Finally, I wish to give my special thanks to my dearest wife Pınar whose patient love enabled me to complete this thesis.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

International Data Encryption Algorithm (IDEA), is a block cipher designed by Xuejia Lai and James L. Massey [16], operates on 64-bit plaintext/ciphertext blocks, and 128-bit key and consists of 8 iterated rounds and a final transformation. The design of IDEA is completely based on the concept of mixing operations from different algebraic groups such as multiplication modulo $2^{16}+1$ ($\odot$), addition modulo 2^{16} ($\boxplus$) and bitwise exclusive-OR (XOR) ($\oplus$, bitwise addition on modulo 2) on 16 bit blocks. MESH ciphers introduced by Nakahara are also based on these operations [25],[26].

It is easy to introduce these 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 $v : \mathbb{Z}_{2^n} \to \mathbb{Z}_2^n$ and $d : \mathbb{Z}^*_{2^n+1} \to \mathbb{Z}_{2^n}$ be the invertible functions defined by: $v(x) = \mathbf{X}$, where $\mathbf{X} = (x_n, \ldots, x_2, x_1)$ is a bit representation of $x = \sum_{i=1}^{n} x_i 2^{i-1}$ and $d(x) = x$ if $x \neq 2^n$ and $d(2^n) = 0$. With this convention, the addition mod 2^n, $\boxplus$, the multiplication mod $(2^n + 1)$, $\odot$ and the XOR $\oplus$ operations produce the following functions $\mathbf{f}, \mathbf{g}, \mathbf{h} : \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to \mathbb{Z}_2^n$:

The addition operation $\boxplus$;

$\mathbf{f}(\mathbf{X}, \mathbf{Z}) = \mathbf{X} \boxplus \mathbf{Z} = v(x + z \bmod (2^n))$.

The multiplication operation $\odot$;

$\mathbf{g}(\mathbf{X}, \mathbf{Z}) = \mathbf{X} \odot \mathbf{Z} = v(d(d^{-1}(x)d^{-1}(z) \bmod (\ 2^n + 1)))$, where d^{-1} is the inverse d.

The XOR operation $\bigoplus$;

$\mathbf{h}(\mathbf{X},\mathbf{Z}) = \mathbf{X}\bigoplus\mathbf{Z} = (x_n,\ldots,x_1)\bigoplus(z_n,\ldots,z_1) = (x_n + z_n \bmod (2),\ldots,x_1+z_1 \bmod (2)) = (x_n \oplus z_n,\ldots,x_1\oplus z_1)$,
where $v(x)=\mathbf{X}$ and $v(z)=\mathbf{Z}$.

We now list some of the cryptographic and algebraic properties of these functions studied in [23] and [16]. For integer $n \geq 2$ and random vectors $\mathbf{A},\mathbf{B},\mathbf{C} \in \mathbb{Z}_2^n$,

i) $\mathbf{A}\bigodot(\mathbf{B}\boxplus\mathbf{C}) = (\mathbf{A}\bigodot\mathbf{B})\boxplus(\mathbf{A}\bigodot\mathbf{C})$ holds with probability about $1/4$ and

ii) $\mathbf{A}\bigodot(\mathbf{B}\boxplus\mathbf{1}) = (\mathbf{A}\bigodot\mathbf{B})\boxplus\mathbf{A}$ holds with probability $1/2-2^{-n-1}+2^{-2n} \approx 1/2$, where $v(1)=\mathbf{1}=(0,\ldots,0,1)$. and

iii) $\mathbf{A}\bigodot(\mathbf{B}\boxplus(1,\ldots,1)) = (\mathbf{A}\bigodot\mathbf{B})\boxplus(\mathbf{A}\bigodot(1,\ldots,1))$ holds with probability $2^{-n}-2^{-n-1}+2^{-2n} \approx 2^{-n}$.

iv) Any pair of these operations does not satisfy distributive law and a generalized associative law. That is, for $\triangleright$ and $\triangleleft \in \{\boxplus,\bigodot,\bigoplus\}$, there exist $\mathbf{A},\mathbf{B}$ and $\mathbf{C} \in \mathbb{Z}_2^n$ such that $\mathbf{A}\triangleright(\mathbf{B}\triangleleft\mathbf{C}) \neq (\mathbf{A}\triangleright\mathbf{B})\triangleleft(\mathbf{A}\triangleright\mathbf{C})$ and $\mathbf{A}\triangleright(\mathbf{B}\triangleleft\mathbf{C}) \neq (\mathbf{A}\triangleright\mathbf{B})\triangleleft\mathbf{C}$.

v) For a fixed $n \in \{1,2,4,8,16\}$ and $y \in \mathbb{Z}_{2^{n+1}}\backslash\{0,2^n\}$, let

$$\bar{f}(x,y) = \begin{cases} d^{-1}(d(x)+d(y) \bmod (2^n)) & \text{for all } x \text{ and } y \in \mathbb{Z}_{2^{n+1}} \\ 0 & \text{otherwise} \end{cases}$$

and let $\bar{g}(x,y) = d(d^{-1}(x)d^{-1}(y) \bmod (2^n+1))$ for all x and $y \in \mathbb{Z}_{2^n}$.

Then $\bar{f}(x,y)$ is a polynomial over the ring $\mathbb{Z}_{2^{n+1}}$ with degree 2^n-1 and $\bar{g}(x,y)$ can not be written as a polynomial in x over the ring $\mathbb{Z}_{2^n}$.

The properties *i*), *ii*) and *iii*) were exploited to cryptanalyze the first 2-round of IDEA in [23] and the property *v*) leads to the author in [16] to conclude that the operations $\boxplus$ and $\bigodot$ are highly nonlinear.

By fixing one of the variables in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$, namely $\mathbf{Z} = v(z)$ we obtain vector valued functions $\mathbf{f}_z$ and $\mathbf{g}_z$: $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$, where $\mathbf{f}_z(\mathbf{X}) = \mathbf{f}(\mathbf{X}, \mathbf{Z}) = \mathbf{X} \boxplus \mathbf{Z}$ and $\mathbf{g}_z(\mathbf{X}) = \mathbf{g}(\mathbf{X}, \mathbf{Z}) = \mathbf{X} \odot \mathbf{Z}$. In Section 3.2 and 3.3, using the nonlinearity measurement based on the Hamming distance [29], we find

- those transformation of z's such that the nonlinearity of $\mathbf{g}_z$ remains the same,
- an upper bound for the nonlinearity of $\mathbf{g}_{2^k}$, where $2 \leq k < n-1$,
- many linear relations associated with the set of those z above making the nonlinearity of $\mathbf{f}_z$ and $\mathbf{g}_z$ zero, and
- many linear relations for $\mathbf{g}_z$ holding with a high probability.

Nonlinearity criteria is an important issue for the linear cryptanalysis [22]. In fact, it is well known that there exists a linear relation among the inputs and outputs of a vector valued function if and only if its nonlinearity is zero. In this respect for any $\mathbf{X} = (x_n, x_{n-1}, \ldots, x_1)$, $\mathbf{Y} = (y_n, y_{n-1}, \ldots, y_1)$ and $\mathbf{Z} = (z_n, z_{n-1}, \ldots, z_1) \in \mathbb{Z}_2^n$, there exists a trivial linear relation with probability one for both functions $\mathbf{f}_z$ and $\mathbf{h}_z$, namely

$$x_1 \oplus z_1 = y_1.$$

On the other hand, for any $\mathbf{X}, \mathbf{Y} \in \mathbb{Z}_2^n$ and $\mathbf{Z} \in \{(0, \ldots, 0), (1, \ldots, 1)\}$, there exists a linear relation with probability one for the function $\mathbf{g}_z$, namely

$$x_1 \oplus z_1 \oplus 1 = y_1.$$

Daemen et al. used these linear relations to derive 15 linear relations for 1-round IDEA [8] . For $z \in \{2, 2^{n-1}, 2^{n-1}+1, 2^n - 1\}$, it was shown that the nonlinearity of $\mathbf{g}_z$ is zero [35]. Due to this fact, two additional linear relations for $\mathbf{g}_z$ can be derived. These two and the previous linear

relations were used to derive 39 linear relations for 1-round IDEA in [34]. In Section 3.4.2, we present a new algorithm to find new 242 linear relations (holding with probability one) based on these 54 linear relations. Daemen et al. successively used 3 of their 15 linear relations for 1-round IDEA to find a linear relation for 8,5-round IDEA satisfied by each member of a class of weak keys with cardinality 2^{23}. Based on that linear relation, we extend this linear weak keys class with cardinality 2^{23} to two classes with cardinality 2^{24} and 2^{27} in Section 3.6.

Differential cryptanalysis is an another powerful technique to analyze symmetric ciphers and hash functions [1]. In [8], this technique was applied to find a class of weak keys with cardinality 2^{35} and then it was extended to find another class of weak keys with cardinality 2^{51}. In this study, the basic idea was the following difference properties of the IDEA operations:

For $\mathbf{X}$ and $v(a) = \mathbf{A} \in \mathbb{Z}_2^n$, let $\mathbf{X}_a = \mathbf{X} \bigoplus \mathbf{A}$. Then we have
$(\mathbf{X} \bigodot \mathbf{Z}) \bigoplus (\mathbf{X}_{2^{n-1}} \bigodot \mathbf{Z}) = \mathbf{2^{n-1}}$ for $\mathbf{Z} \in \{v(0), v(1)\}$, and
$(\mathbf{X} \boxplus \mathbf{Z}) \bigoplus (\mathbf{X}_{2^{n-1}} \boxplus \mathbf{Z}) = \mathbf{2^{n-1}}$ and $(\mathbf{X} \bigoplus \mathbf{Z}) \bigoplus (\mathbf{X}_a \bigoplus \mathbf{Z}) = \mathbf{A}$ for all $v(a) = \mathbf{A}$ and $\mathbf{Z} \in \mathbb{Z}_2^n$.

One can view these results as properties of the operations $\{\bigodot, \bigoplus\}$ and $\{\boxplus, \bigoplus\}$ applied to the pair $\{\mathbf{X}, \mathbf{X}_a\}$ for varying a and $v(z) = \mathbf{Z}$. Therefore it would be interesting to study the possible similar properties of the operations $\{\boxplus, \bigodot\}$. For $a, b, z \in \mathbb{Z}_{2^n}$ and $\bowtie \in \{\boxplus, \bigodot\}$, let $\mathbf{D}_{\bowtie,z}(a, b) = \{(\mathbf{X}, \mathbf{X}_a) \,|\, (\mathbf{X} \bowtie \mathbf{Z}) \bigoplus (\mathbf{X}_a \bowtie \mathbf{Z}) = \mathbf{B}\}$, where $v(z) = \mathbf{Z}$ and $v(b) = \mathbf{B}$. In Section 4.1 we prove that $|\mathbf{D}_{\boxplus,z}(a, b)| = |\mathbf{D}_{\boxplus,z}(b, a)|$, $|\mathbf{D}_{\boxplus,z}(a, b)| = |\mathbf{D}_{\boxplus,-z}(b, a)|$, where $|S|$ stands for the cardinality of the set S, $-z$ is the additive inverse of z in $\mathbb{Z}_{2^n}$. Furthermore, for all a, b and $z \in \mathbb{Z}_{2^n}$ such that $\gcd(z, 2^n + 1) = 1$, we show that $|\mathbf{D}_{\bigodot,z}(a, b)| = |\mathbf{D}_{\bigodot,z^{-1}}(b, a)|$, where z^{-1} is the multiplicative inverse of z mod $(2^n + 1)$. In this section we

also find those a's and b's such that $|\mathbf{D}_{\boxplus,z}(a,b)| = 2^{n-1}$. On the other hand for all z, we list a, b and $\bowtie$ such that $|\mathbf{D}_{\bowtie,z}(a,b)| = 0$. In Sections 4.3 and 4.4 we use this list to obtain impossible differentials for 1-round IDEA and Pseudo-Hadamard Transform.

This thesis is organized as follows: In Chapter 2 we explain the linear cryptanalysis, the differential cryptanalysis, the block cipher IDEA and its security. In Chapter 3 we discuss the nonlinearity properties and linear relations of the IDEA operations. In Chapter 4 we present our work on the difference properties of these operations, 1-round IDEA and Pseudo-Hadamard Transform.

CHAPTER 2

BLOCK CIPHERS

2.1 Introduction

In this chapter we shall first give basics for the block ciphers, the linear and differential cryptanalysis. Then we will introduce the block cipher IDEA and discuss its security.

Definition 2.1.1. *An n-bit block cipher is a function* $E : \mathbb{Z}_2^n \times K \rightarrow \mathbb{Z}_2^n$ *such that for every* $k \in K$, $E(\mathbf{P}, k)$ *is an invertible function of* $\mathbf{P}$ *from* $\mathbb{Z}_2^n$ *to* $\mathbb{Z}_2^n$. *This function is called encryption function. The inverse of the encryption function* $E(\mathbf{P}, k)$ *is called the decryption function which is denoted by* $D(\mathbf{C}, k)$ *(i.e.* $\mathbf{C} = E(\mathbf{P}, k)$*). Here* K *is an arbitrary finite set.*

The encryption function E is based on a simple function repeatedly applied. Each repetition is called a *round*. Each round uses the previous round's output and the subkey derived from the secret key by an algorithm. For a 128-bit secret key, Rijndael is an example of 10-round block cipher which was selected as Advanced Encryption Standard (AES) by the US National Institute of Standards and Technology (NIST) in 2000 [9].

The following two sections descibe two well-known cryptanalysis techniques that have been extensively studied and applied to many block ciphers.

2.1.1 Differential Cryptanalysis

Differential cryptanalysis is the very well-known attack on iterative block ciphers, initially introduced by Murphy [24] and then it was improved by Eli Biham and Adi Shamir in 1990. Differential cryptanalysis is a chosen plaintext attack and analyzes the effect of the difference of a pair of plaintexts on the difference of ciphertext pairs which are the outputs of rounds in an iterative cipher. In 1992, Eli Biham and Adi Shamir represented the improved version of the differential cryptanalysis to attack the full 16−round DES in 2^{37} time and by analyzing 2^{36} ciphertexts obtained from 2^{47} chosen plaintexts [2]. Differential cryptanalysis is also successfully applied to analyze more recent block ciphers such as FEAL, Khafre, REDOC-II, LOKI and Lucifer.

Differential cryptanalysis is mainly focus on a round of an iterated $n-$round cipher. In fact, $\triangle\mathbf{X}$ represents the difference $\mathbf{X} \otimes (\mathbf{X}')^{-\mathbf{1}}$ between plaintexts (ciphertexts) pair, $\mathbf{X}$ and $\mathbf{X}'$, where $\otimes$ is the group operation on the set of plaintexts (ciphertexts) and $(\mathbf{X}')^{-\mathbf{1}}$ is the inverse element of $\mathbf{X}'$ in that group. This difference does not contain the key value. For DES-like cryptosystems, the difference is taken as a fixed exclusive-or (bitwise addition over modulo 2) of the two plaintexts (ciphertexts). For others, it may change according to their structure. To analyze differential behaviour of a round function, the difference distribution table can be constructed according to difference of every plaintext and ciphertext pairs. For the extension of the single round analysis to other rounds, the notion of characteristic was introduced by Biham and Shamir [1]. An $n-$round characteristic is a tuple $(\boldsymbol{\alpha}_0, \boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_n)$ containing series of differences, where $\boldsymbol{\alpha}_0 = \triangle\mathbf{P}$ is the chosen difference of a pair of plaintext $\mathbf{P}_0$ and $\mathbf{P}_0'$ which are the inputs of the first round, $\boldsymbol{\alpha}_i$ is the difference of a pair of ciphertext that are the outputs of i^{th} round related to plaintext $\mathbf{P}_0$ and $\mathbf{P}_0'$. The probability of an $i-$round

characteristic is the following conditional probability:

$$P(\triangle \mathbf{C}_i = \boldsymbol{\alpha}_i, \triangle \mathbf{C}_{i-1} = \boldsymbol{\alpha}_{i-1}, \ldots, \triangle \mathbf{C}_1 = \boldsymbol{\alpha}_1 \mid \triangle \mathbf{P} = \boldsymbol{\alpha}_0)$$

Here, an $i-$round characteristic can be either the combination of one or more round characteristic or iteration of some fixed characteristic (iterative characteristic). The details of the characteristics were given in [3]. In the differential cryptanalysis, when such probabilities are computed, it is assumed that all subkeys are independent and uniformly random. A plaintext $\mathbf{P}, \mathbf{P}'$ with difference $\triangle \mathbf{P}$ is a *right pair* with respect to an $n-$round characteristic and an independent key K if they satisfy the differences in characteristic when they are encrypted. Every pair which is not a right pair with respect to the characteristic and the independent key is called a *wrong pair*. The first step of the chosen plaintext attack, differential cryptanalysis on an $n-$round is to find the subkey of the last round by determining $n-1$ round characteristic ($\triangle \mathbf{P} = \boldsymbol{\alpha}_0, \triangle \mathbf{C}_1 = \boldsymbol{\alpha}_1, \ldots, \triangle \mathbf{C}_{n-1} = \boldsymbol{\alpha}_{n-1}$) which holds $\triangle \mathbf{C}_{n-1}$ completely or partially with high, or nearly high probability. For every right pair $\mathbf{P}$ and $\mathbf{P}'$ with difference $\boldsymbol{\alpha}_0$, the occurence of candidate subkey for the last round key is counted if ciphertext pair $\mathbf{C}_{r-1}$ and $\mathbf{C}'_{r-1}$ with difference $\boldsymbol{\alpha}_{r-1}$ is obtained from the last round ciphertext $\mathbf{C}_r$ and $\mathbf{C}'_r$ by that key. For sufficiently many chosen plaintext pairs, the above steps are repeated. Finally, the most appeared subkey(s) is taken as the actual subkey of the last round.

The notion of *differential* was introduced by Lai et al. [16]. Here is its definition:

Definition 2.1.2. [16]*: An $i-$round differential is a couple $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, where $\boldsymbol{\alpha}$ is the difference of a pair distinct plaintext $\mathbf{P}$ and $\mathbf{P}'$ and where $\boldsymbol{\beta}$ is a possible difference for the resulting i^{th} round outputs $\mathbf{C}_i$ and $\mathbf{C}'_i$. The probability of an $i-$round differential $(\boldsymbol{\alpha}, \boldsymbol{\beta})$ is the conditional probability*

that $\boldsymbol{\beta}$ *is the difference* $\triangle \mathbf{C}_i$ *of the ciphertext pair after* i *rounds given that the plaintext pair* $(\mathbf{P}, \mathbf{P}')$ *has difference* $\triangle \mathbf{P} = \boldsymbol{\alpha}$ *when the plaintext* $\mathbf{P}$ *and the subkeys* $\mathbf{K}_1, \ldots, \mathbf{K}_i$ *are independent and uniformly random. We denote this differential probability by* $P(\triangle \mathbf{C}_i = \boldsymbol{\beta} \mid \triangle \mathbf{P} = \boldsymbol{\alpha})$.

Lai et al. preferred to use differentials instead of characteristic in the differential cryptanalysis for an $n-$round cipher. Their reason is that the indeterminate differences is not important. This is due to the fact that only $n-1$ round difference is needed to find the last round key of $n-$round cipher. Note that the probabilities of differentials are greater than characteristics and for this reason, it was used to derive a lower bound on the complexity of the differential cryptanalysis in [16]. The probability of an $i-$round differential with input difference $\boldsymbol{\alpha}$ and output difference $\boldsymbol{\beta}$ is the sum of the probabilities of all $i-$round characteristics with the corresponding input and output difference.

Lai presented a definition of higher order derivatives of discrete cryptographic functions that is analogous to the definition of differentiation in calculus [18]. Knudsen used higher order differentials to cryptanalyze ciphers probably secure aganist a differential attack using first order differentials and he showed the existence of the ciphers which are probably secure aganist a differential attack [14].

Knudsen introduced the notion truncated differentials (partial differentials). For an $2n$ bit Feistel cipher, Unlike $i-$round differentials with difference $(\boldsymbol{\alpha}, \boldsymbol{\beta})$, $i-$round truncated differentials predicts only subsequence of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$, namely $\boldsymbol{\alpha}'$ and $\boldsymbol{\beta}'$. Truncated differentials are used to analyze 6-round DES with complexity of about 46 chosen plaintexts and a running time about time of 3500 encryptions. It is noted that this type of attacks seems to be useful for ciphers that have a relatively small number of rounds.

To immunize against differential cryptanalysis, the difference distribution tables of the S-boxes of a DES-like iterated block cipher must not contain entries with large values except for the first entry of the first row. In other words, the values of the difference distribution table of S-Boxes must be uniformly distributed. In addition to this requirement, the difference distribution table of an S-Box should also contain less nonzero entries as possible in its fist column to lessen the probability of the possible iterative characteristics.

In [28] it was shown that for DES-like iterated ciphers, it is feasible to find an upper bound on the probabilities of $r-$round differential by using a non-trivial $1-$round differential with highest probability. If this probability is chosen to be small, the resistance against the differential cryptanalysis can be obtained.

In [16] and [17], the notion of *Markov Cipher*, which gives more information about the probabilities of differentials, was presented and the security of these ciphers against differential cryptanalysis by using Markov chain techniques was discussed. It is known that the block cipher DES, LOKI, FEAL and REDOC are Markov Ciphers [17]. For the immunity of Markov Ciphers against the differential cryptanalysis, for $r-$round Markov the transition probability matrix of the homogeneous Markov chain $\triangle\mathbf{P} = \triangle\mathbf{C}_0, \triangle\mathbf{C}_1, \ldots, \triangle\mathbf{C}_r$ is defined and their irreducibility and the eigenvalues are considered in [17]. In reality, the formulation of these requirements is not practical for a block cipher with large size. Due to this issue, by the help of the results of the differential cryptanalysis of PES [16], the suggested more practical requirement for security is :

The transition probability matrix of a Markov cipher should be non-symmetric [16],[17].

The idea behind this suggestion is that when transition matrix of a Markov cipher is the symmetric, for the one-round differential with high probability among the others, the concatenation of that differential with itself $r-1$ can result in the $r-$round characteristic with high probability that produce an $r-$round differential with high probability; however, this situation can be avoided by making the corresponding transition matrix non-symmetric.

2.1.2 Linear Cryptanalysis

Linear cryptanalysis is one of the most recent method of analysing iterated ciphers. It is essentially a known-plaintext (statistical) attack and was initially used to attack the FEAL cipher by Matsui and Yamagishi [20]. The refinement version of linear cryptanalysis was used to break 16 round DES cipher with 2^{47} known-plaintexts [22]. Matsui's paper [21] which represents the improved version of linear cryptanalysis and its application to first experimental cryptanalysis for breaking the full 16-round DES was appeared in 1994. This experiment was carried out by using twelve HP9735/ PA-RISK 99 MHZ workstations and finally the 56 secret key bits were recovered with 2^{43} known-plaintext/ciphertext pairs in fifty days.

The aim of the linear cryptanalysis is to investigate statistical linear relations between bits of plaintexts, the ciphertexts, the secret keys to get a linear approximate expression for an entire cipher under consideration. Similar to the differential cryptanalysis, the linear cryptanalysis deals with nonlinear parts of the one round of the cipher. To find a statistical linear relation for the nonlinear part (function), two subset A and B

containing some index numbers of inputs and output bits of that part, respectively is constructed and for each input, exclusive-or of inputs bits and corresponding output bits is calculated according to each possible subset A and B. For half of the inputs, if exclusive-or values are equal to zero, then a nonlinear approximation can be obtained by the corresponding subsets A and B. For a smaller or a larger part of the inputs, if they are equal to zero, then a linear approximation can be obtained. In this way, the linear approximations having best probability p (i.e. $|p - 1/2|$ is maximal) are found for the nonlinear parts of one round of the cipher. Then for each linear approximation of these kinds is extended to the round function as a linear equation. Finally linear equations for the round functions are combined to construct a linear expression for the entire cipher. The probability of that expression is calculated from the probabilities of linear equations of the round functions using the following lemma:

Lemma 2.1.3. ([22]) *(Piling-up Lemma) Let* $x_i\,(1 \leq i \leq n)$ *be independent random variables whose values are 0 with probability* p_i *or 1 with probability* $1-p_i$*. Then the probability that* $x_1 \oplus x_2 \oplus \ldots \oplus x_n = 0$ *is*

$$1/2 + 2^{n-1} \prod_{i=1}^{n} (p_i - 1/2).$$

Let us denote $\mathbf{A}$ is n-bit plaintext (ciphertext or key), $\mathbf{A}[i]$ is the the i^{th} bit of $\mathbf{A}$ and $\mathbf{A}[i, j, \ldots, k] := \mathbf{A}[i] \oplus \mathbf{A}[j] \oplus \ldots \oplus \mathbf{A}[k]$.

For a given m-bit cipher, the linear expression is of the form

$$\mathbf{P}[i_1, i_2, \ldots, i_a] \oplus \mathbf{C}[j_1, j_2, \ldots, j_b] = \mathbf{K}[k_1, k_2, \ldots, k_c]$$

where $\mathbf{P}$ is a randomly given plaintext, $\mathbf{C}$ is the corresponding ciphertext, $\mathbf{K}$ is the key used to encrypt $\mathbf{P}$, $i_1, i_2, \ldots, i_a; j_1, j_2, \ldots, j_b$ and $k_1, k_2, \ldots, k_c$ denotes fixed bit locations. This relation holds with the probability p such

that $|p - 1/2|$ is maximal and $p \neq 1/2$. Here the value of $|p - 1/2|$ gives us a measurement for effectiveness of the above expression . One key bit of $K[k_1, k_2, \ldots, k_c]$ is determined using the maximum likelihood method described in [22] if sufficient amount of plaintexts is available. The success rate of this methods depends on the number of plaintexts N and $|p-1/2|$.

Matsui [22] succeeded in finding the linear expression,which is described in above, for the block cipher DES by considering the nonlinear part of its round function, namely S-Boxes.

Some theorical, practical enhancement and extensions of the linear cryptanalysis have appeared since its emergence. Kaliski and Robshaw presented a extension to the linear cryptanalytic attack using multiple linear approximations [13]. It leads to reduction in the amount of data required for a successful linear crytpanalysis of a block cipher. Knudsen and Robshaw [30] suggested an algorithm using non-linear approximations. They replaced the linear approximations used in linear cryptanalysis with non-linear approximations. Shimoyama and Kaneko derived 7 quadratic relations of S-boxes of DES using groebner basis techniques by considering S-Boxes as Boolean polynomials [32]. By using one of these relations, they constructed an improved algorithm for attacking 16 round DES that is a combination of the multiple linear approximation and non-linear approximation methods mentioned above. This algoritm reduces the number of texts used in Matsui's attack [21].

Linear cryptanalysis exploits the low nonlinearity of S-Boxes engaged by a block cipher. To immunize a S-box against linear cryptanalysis, it suffices that all entries of its LAT (Linear Approximation Table) should not to diverge too from 2^{n-1}. Alternatively, its nonlinearity should be high (near to

2^{n-1}) due to the relation between the nonlinearity of a S-box and its LAT.

2.2 IDEA Block Cipher

International Data Encryption Algorithm (IDEA), a slightly modified version of Proposed Encryption Standard (PES), is a block cipher designed by Xuejia Lai and James L. Massey to increase immunity against differential cryptanalysis [15],[17],[16]. IDEA operates on 64-bit plaintext/ciphertext blocks, and 128-bit key and consists of 8 iterated rounds and a final transformation. The rounds and final transformation are arranged to achieve the desired confusion and diffusion by successive usage of three incompatible group operations. The design of IDEA is completely based on the concept of "mixing operations from different algebraic groups such as multiplication modulo $2^{16}+1$ ($\odot$), addition modulo 2^{16} ($\boxplus$) and bitwise XOR ($\bigoplus$, bitwise addition on modulo 2) on 16 bit blocks".

IDEA was developed at ETH Zurich in Switzerland and is the one of the block ciphers (CAST, 3-DES, IDEA) used in message encryption's part of the popular encryption program PGP (Pretty Good Privacy) [10] and patented in the United States and in most European countries. No license fee is required for noncommercial use. The structure of IDEA allows fast implementations both in hardware and software [19].

IDEA encrypts blocks of 64 bits plaintext to blocks of 64 bits ciphertext with 128 bit key. For the encryption, this cipher divides 64-bit plaintext block X into four 16-bit subblocks, $\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3$ and $\mathbf{X}_4$ such that $X = (\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4) = (\mathbf{X}_1^{(0)}, \mathbf{X}_2^{(0)}, \mathbf{X}_3^{(0)}, \mathbf{X}_4^{(0)})$. They are transformed into four 16-bit ciphertext subblocks $\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Y}_3$ and $\mathbf{Y}_4$ by 8 iterated

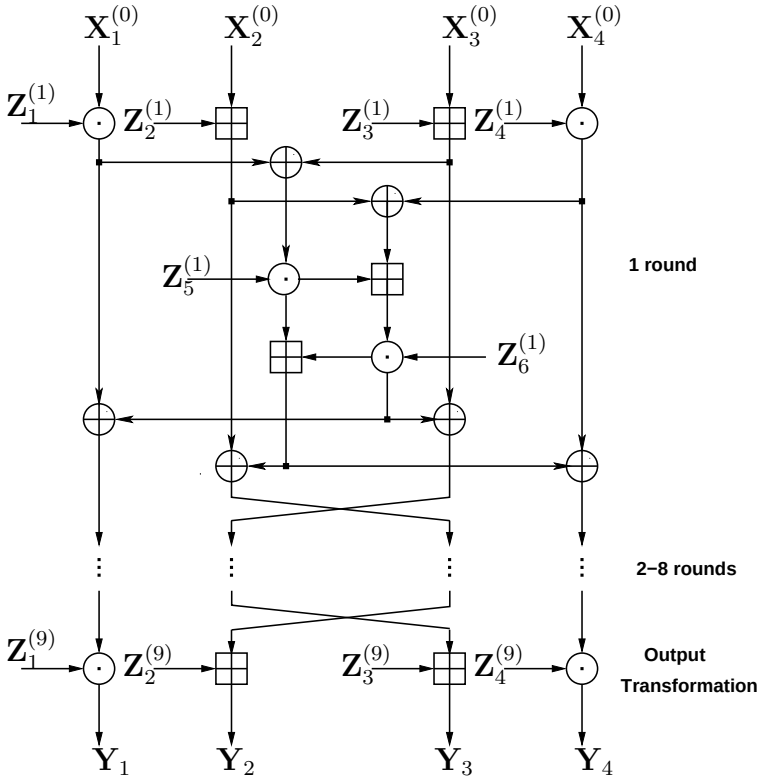

Figure 2.1: Computational graph for the encryption process of the IDEA cipher

rounds and a final output transformation using 52 key subblocks with length 16 derived from a given 128-bit key block. IDEA uses the six key subblocks $\mathbf{Z}_1^{(r)}, \mathbf{Z}_2^{(r)}, .., \mathbf{Z}_6^{(r)}$ for the rounds $r = 1, 2, .., 8$ and the final output transformation uses four 16-bit key subblocks $\mathbf{Z}_1^{(9)}, \mathbf{Z}_2^{(9)}, \mathbf{Z}_3^{(9)}, \mathbf{Z}_4^{(9)}$. The graph of the encryption of IDEA can be seen in Figure 2.1. The key scheduling algorithm and the list of all 16-bit key subblocks (Table A.1) are given in Appendix A.

2.2.1 1-round IDEA and the MA-Structure

Throughout the remaining sections, we denote round key, input and output for 1-round IDEA (see Figure 2.2) as $Z = (\mathbf{Z}_1, \ldots, \mathbf{Z}_6)$, $X = (\mathbf{X}_1, \mathbf{X}_2, \mathbf{X}_3, \mathbf{X}_4)$ and $Y = (\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Y}_3, \mathbf{Y}_4)$, respectively. Then we have

$$\begin{aligned} \mathbf{Y}_1 &= (\mathbf{X}_1 \odot \mathbf{Z}_1) \oplus \mathbf{T}. \\ \mathbf{Y}_2 &= (\mathbf{X}_3 \boxplus \mathbf{Z}_3) \oplus \mathbf{T}. \\ \mathbf{Y}_3 &= (\mathbf{X}_2 \boxplus \mathbf{Z}_2) \oplus \mathbf{U}. \\ \mathbf{Y}_4 &= (\mathbf{X}_4 \odot \mathbf{Z}_4) \oplus \mathbf{U}. \end{aligned} \tag{2.1}$$

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 Figure 2.2):

$$\mathbf{P} = (\mathbf{X}_1 \odot \mathbf{Z}_1) \oplus (\mathbf{X}_3 \boxplus \mathbf{Z}_3) \text{ and } \mathbf{Q} = (\mathbf{X}_2 \boxplus \mathbf{Z}_2) \oplus (\mathbf{X}_4 \odot \mathbf{Z}_4). \tag{2.2}$$

$$\mathbf{U} = (\mathbf{P} \odot \mathbf{Z}_5) \boxplus \mathbf{T} \text{ and } \mathbf{T} = [(\mathbf{P} \odot \mathbf{Z}_5) \boxplus \mathbf{Q}] \odot \mathbf{Z}_6. \tag{2.3}$$

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

Definition 2.2.1. *For any* $\mathbf{A}$ *and* $\mathbf{A}^* \in \mathbb{Z}_2^n$, *we denote* $\boldsymbol{\delta}\mathbf{A} = \mathbf{A} \odot (\mathbf{A}^*)^{-1}$, $\boldsymbol{\partial}\mathbf{A} = \mathbf{A} \boxplus (-\mathbf{A}^*)$ *and* $\triangle\mathbf{A} = \mathbf{A} \oplus \mathbf{A}^*$.

For the differential cryptanalysis, two following useful properties of the MA-structure were provided in [16].

Theorem 2.2.2. *[16] If the function computed by the MA-structure is written as*

$$(\mathbf{U}, \mathbf{T}) = MA(\mathbf{P}, \mathbf{Q}; \mathbf{Z}_5, \mathbf{Z}_6),$$

then for every choice of key $(\mathbf{Z}_5, \mathbf{Z}_6)$, *the inputs* $(\mathbf{P}, \mathbf{Q})$, $(\mathbf{P}^*, \mathbf{Q}^*)$ *and the outputs* $(\mathbf{U}, \mathbf{T})$, $(\mathbf{U}^*, \mathbf{T}^*)$ *of the MA-structure for the same key* $(\mathbf{Z}_5, \mathbf{Z}_6)$ *satisfy*

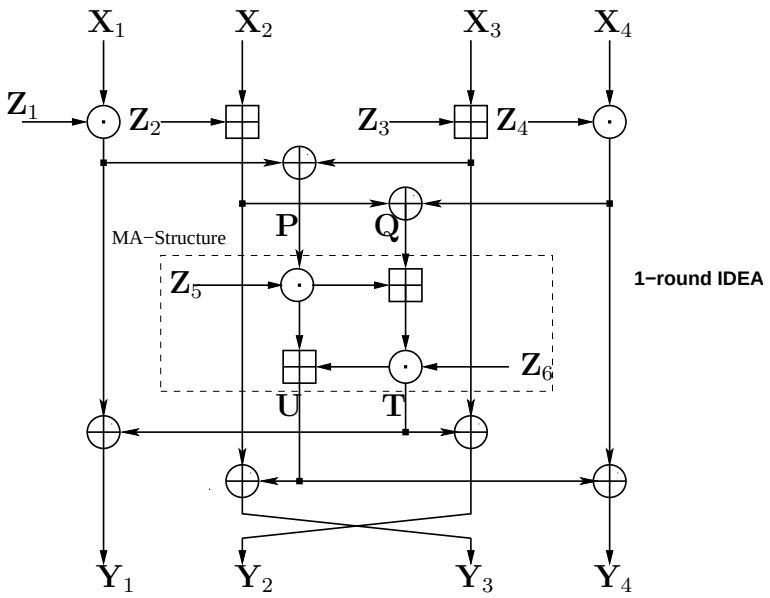

Figure 2.2: Computational graph for the encryption process of 1-round IDEA cipher

the following relations:

$$\boldsymbol{\delta}\mathbf{P} = \mathbf{1} = (1, \ldots, 1), \boldsymbol{\partial}\mathbf{Q} = \mathbf{0} = (0, \ldots, 0) \text{ (i.e. } \triangle\mathbf{Q} = \mathbf{0}) \Longleftrightarrow \boldsymbol{\delta}\mathbf{T} = \mathbf{1}, \boldsymbol{\partial}\mathbf{U} = \mathbf{0}; \tag{2.4}$$

and

$$\boldsymbol{\delta}\mathbf{P} = \mathbf{0}, \mathbf{Q} \boxplus \mathbf{Q}^* = \mathbf{0} \Longleftrightarrow \boldsymbol{\delta}\mathbf{T} = \mathbf{0}, \mathbf{U} \boxplus \mathbf{U}^* = \mathbf{2} = (0, \ldots, 1, 0). \tag{2.5}$$

It is known that $\boldsymbol{\delta}\mathbf{A} = \mathbf{0} \Longleftrightarrow \mathbf{A} \boxplus \mathbf{A}^* = \mathbf{1}$. Note that first property is trivial since the same inputs of the MA-structure produce the same outputs. Second property was discovered by Murphy [17]. We will use these properties to obtain impossible differentials for 1-round IDEA in Section 4.3.

2.2.2 1-round RIDEA and the RMA-Structure

A description of the RIDEA cipher can be found in Section A.3, Appendix A. the RIDEA cipher is the same as IDEA cipher except that one of inputs of the MA-structure, $\mathbf{Q}$ and one subblock of round key, $\mathbf{Z}_6$ are involved in the MA-structure by the multiplication and the addition operations respectively. This slightly changed structure is called the RMA-structure of the RIDEA cipher and round outputs of 1-round RIDEA (Figure 2.3) can be given as follows:

$$\begin{aligned} \mathbf{Y}_1 &= (\mathbf{X}_1 \odot \mathbf{Z}_1) \oplus \widetilde{\mathbf{T}}. \\ \mathbf{Y}_2 &= (\mathbf{X}_3 \boxplus \mathbf{Z}_3) \oplus \widetilde{\mathbf{T}}. \\ \mathbf{Y}_3 &= (\mathbf{X}_2 \boxplus \mathbf{Z}_2) \oplus \widetilde{\mathbf{U}}. \\ \mathbf{Y}_4 &= (\mathbf{X}_4 \odot \mathbf{Z}_4) \oplus \widetilde{\mathbf{U}}. \end{aligned} \tag{2.6}$$

Two input subblocks of the RMA-structure $\mathbf{P}$ and $\mathbf{Q}$ and two output subblocks of the RMA-structure $\widetilde{\mathbf{U}}$ and $\widetilde{\mathbf{T}}$ can be represented as

$$\mathbf{P} = (\mathbf{X}_1 \odot \mathbf{Z}_1) \oplus (\mathbf{X}_3 \boxplus \mathbf{Z}_3) \text{ and } \mathbf{Q} = (\mathbf{X}_2 \boxplus \mathbf{Z}_2) \oplus (\mathbf{X}_4 \odot \mathbf{Z}_4) \tag{2.7}$$

$$\widetilde{\mathbf{U}} = (\mathbf{P} \odot \mathbf{Z}_5) \boxplus \widetilde{\mathbf{T}} \text{ and } \widetilde{\mathbf{T}} = [(\mathbf{P} \odot \mathbf{Z}_5) \boxplus \mathbf{Z}_6] \odot \mathbf{Q} \tag{2.8}$$

Here one can deduce that $\mathbf{Y}_1 \oplus \mathbf{Y}_2 = \mathbf{P}$ and $\mathbf{Y}_3 \oplus \mathbf{Y}_4 = \mathbf{Q}$.

We shall use the following lemma that was given for the implementation issues of IDEA in [16]:

Lemma 2.2.3 (Low-High algorithm for $\odot$)**.** *Let a and b be two non-zero integers in $\mathbb{Z}_{2^n+1}$ and let (ab div 2^n) denotes the quotient when ab is divided by 2^n. Then we have*

$$ab \bmod (2^n{+}1) = \begin{cases} (ab \bmod 2^n) - (ab \text{ div } 2^n) & \text{if } (ab \bmod 2^n) \geq (ab \text{ div } 2^n) \\ (ab \bmod 2^n) - (ab \text{ div } 2^n) + 2^n + 1 & \text{if } (ab \bmod 2^n) < (ab \text{ div } 2^n) \end{cases}$$

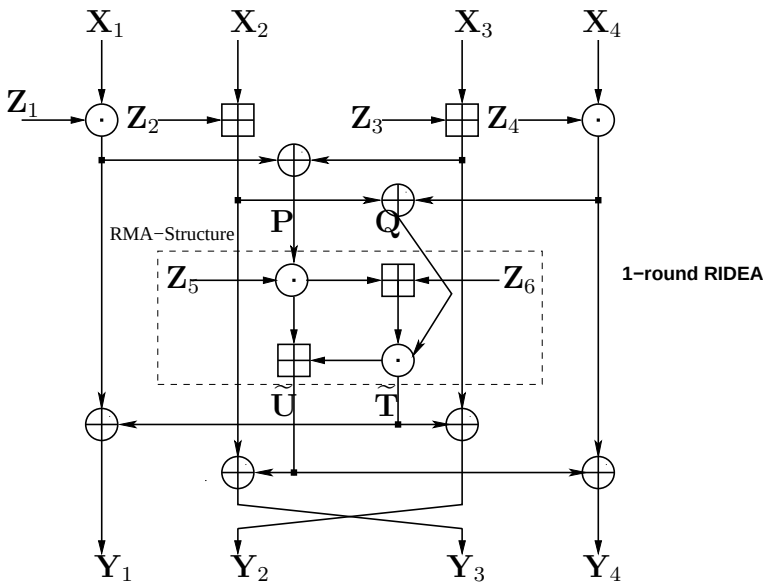

Figure 2.3: Computational graph for the encryption process of 1-round RIDEA cipher

2.3 Security of IDEA

The designer of IDEA claimed that the required confusion for IDEA is achieved by the interaction of the mixing operations from different algebraic groups associated to the operations $\odot, \oplus$ and $\boxplus$ the diffusion in the IDEA cipher is provided by the multiplication-addition (MA) structure (Figure 2.2) [17].

In [17] it was shown that for a suitable chosen difference, IDEA(m) is a Markov cipher for $m = 8, 16, 32, 64$ where $m = 4n$ is the length of the plaintext and n is the length of each subblocks. In addition to this, three classes of highly probable differentials of the IDEA cipher were determined and it was concluded that the IDEA cipher is secure against the differential cryptanalysis attack after 4 rounds [17].

In the literature, Meier [23] showed that the operations $\odot$ and $\boxplus$ satisfy a partial distributive law with a certain probability and presented an attack for 2-rounds of IDEA using that property. Harpes, Kramer and Massey [11] developed a general version of linear cryptanalysis [22] and believed that IDEA is secure against this generalization. In [37] new attacks, based on the principles of related-key differential cryptanalysis, on the key schedules of block ciphers were presented. Because of the simple key schedule of IDEA, a chosen-key differential attack on 3-round IDEA was provided. Besides to that attack, a chosen-key ciphertext only timing attack on full 8-round IDEA was given. Hawkes and O'Connor argued that LSB approximation produce the best probabilities for a linear cryptanalysis of IDEA with independent and uniformly distributed subkeys and mentioned such feasible linear cryptanalysis on IDEA by giving data complexity. Borst, Knudsen and Rijmen [6] presented two attacks on a reduced number of rounds of IDEA. One of them uses differential-linear attack for 3-rounds of IDEA and the other attack uses truncated differentials to analyze 3.5-rounds (3-rounds and an output transformation) of IDEA. Borst [5] described an attack on 3-rounds of IDEA using differential and linear cryptanalysis techniques. New block cipher MMB was proposed in [7] and compared with IDEA to show the desire of the designers of IDEA about providing IDEA to be a successor of DES as a standard block cipher would not be good idea.

In [8], two large classes of weak keys were found for IDEA. This is certainly better than exhaustive search on 128-bit key space and it was claimed that with a slight modification of the key schedule of IDEA, the problem of weak keys can be eliminated. This work was extended to find larger weak key classes for which membership is tested by conforming that a differential-linear approximation holds with probability one and related to

this approximation a weak key class containing 2^{63} 128-bit global keys was found [12]. Besides, a related key differential attack on 4-round IDEA was presented. For this attack, all global keys are weak, and this was applied to find weak key classes for various rounds of IDEA.

In [35], it was proven that the nonlinearity of the vector function corresponds to the multiplication operation $\odot$ is zero for 6 fixed points. Their effects on the linearity of the MA-structure (Multiplication-Addition) structure was investigated. By changing the MA-structure slightly, the RMA-structure was introduced. It was observed that the RMA-structure provides required diffusion for IDEA as the MA-structure does and its nonlinearity is greater than the one provided by the MA-structure.

CHAPTER 3

NONLINEARITY PROPERTIES

3.1 Notation and Preliminaries

We shall use the following notation throughout the rest of the thesis:

- $x \oplus y = x + y \bmod (2)$ 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 $\mathbb{Z}_2$;
- $\boxplus, \odot$ and $\bigoplus$ denote the operations on $\mathbb{Z}_2^n$ which are introduced in Chapter 1;
- When $\mathbf{A} = (a_n, a_{n-1}, \ldots, a_1)$ and $\mathbf{X} = (x_n, x_{n-1}, \ldots, x_1) \in \mathbb{Z}_2^n$,
  a) $\mathbf{A} \bigoplus \mathbf{X} = (a_n \oplus x_n, a_{n-1} \oplus x_{n-1}, \ldots, a_1 \oplus x_1)$.
  b) The dot product $\mathbf{A} \cdot \mathbf{X} = (\sum_{i=1}^{n} a_i x_i) \bmod (2) = a_n x_n \oplus a_{n-1} x_{n-1} \oplus \ldots \oplus a_1 x_1$.
  c) for $\lambda \in \mathbb{Z}_2$, $l_{A,\lambda} \colon \mathbb{Z}_2^n \to \mathbb{Z}_2$ be the function defined by $l_{A,\lambda}(X) = \mathbf{A} \cdot \mathbf{X} \oplus \lambda$ is called an affine function (respectively linear) if $\lambda \neq 0$ (respectively $\lambda = 0$).
- $\mathcal{A} = \{l_{A,\lambda} \mid A \in \mathbb{Z}_2^n, \lambda \in \mathbb{Z}_2\}$ denotes the set of all affine functions on $\mathbb{Z}_2^n$;
- $\lceil x \rceil$ denotes the smallest integer larger than or equal to x.

- $|S|$ denotes the cardinality of the set S.

Let $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ be any function. The non negative integer $H(f) = min_{l_{A,\lambda} \in \mathcal{A}} |\{X \in \mathbb{Z}_2^n \,|\, f(X) \neq l_{A,\lambda}(X)\}|$ which measures the Hamming distance from f from to the set of all affine functions $\mathcal{A}$ 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 $\mathbf{F} : \mathbb{Z}_2^n \to \mathbb{Z}_2^k$ was introduced in [29] as follows:

Let $\mathbf{F} = (f_k, \ldots, f_1)$, $f_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$, where $1 \leq i \leq k$.

Definition 3.1.1.

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

Definition 3.1.2. *Let n be any positive integer and f be a function from $\mathbb{Z}_2^n$ to $\mathbb{Z}_2$. The truth table of a function f is an 2^n-tuple $\{f(\mathbf{0}), f(\mathbf{1}), \ldots, f(\mathbf{2^n - 1})\}$, denoted by T_f.*

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 will now discuss the nonlinearity of this vector valued 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

$$\mathbf{A} \cdot \mathbf{X} \oplus \mathbf{A} \cdot \mathbf{Y} \oplus \mathbf{A} \cdot \mathbf{Z} = 0 \text{ for every } \mathbf{A} \in \mathbb{Z}_2^n \tag{3.1}$$

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

$$\mathbf{1} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} = 0 \tag{3.2}$$

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

$$\mathbf{A} \cdot \mathbf{X} \oplus \mathbf{B} \cdot \mathbf{Y} \oplus \mathbf{C} \cdot \mathbf{Z} \oplus \lambda = 0 \text{ for some } \mathbf{A}, \mathbf{B}, \mathbf{C} \in \mathbb{Z}_2^n \text{ and } \lambda \in \mathbb{Z}_2. \quad (3.3)$$

This relation is called a linear relation for the operation $\bowtie$. Let $v(a) = \mathbf{A}, v(b) = \mathbf{B}, v(c) = \mathbf{C} \in \mathbb{Z}_2^n$ and $\lambda \in \mathbb{Z}_2$, now we consider those $\mathbf{X} \in \mathbb{Z}_2^n$ satisfying (3.3), where $\mathbf{X} \bowtie \mathbf{Z} = \mathbf{Y}$. Let $L_{\bowtie,Z}(a, b, c, \lambda)$ be the number of those $\mathbf{X} \in \mathbb{Z}_2^n$ such that (3.3) holds with $\mathbf{X} \bowtie \mathbf{Z} = \mathbf{Y}$. It is clear from the Definition 3.1.1 that $L_{\bowtie,Z}(a, b, c, \lambda) = 2^n$ if and only if the nonlinearity of the vector valued function $\mathbf{X} \to \mathbf{X} \bowtie \mathbf{Z}$ is zero.

3.2 Nonlinearity of Operations

For a fixed $z \in \mathbb{Z}_{2^n}$ and the operation $\bowtie \in \{\boxplus, \odot, \oplus\}$, the mapping $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$ given by $\mathbf{X} \to \mathbf{X} \bowtie \mathbf{Z} = \mathbf{Y}$ will be denoted in this section by $\mathbf{t}_z(\mathbf{X}) = \mathbf{t}(\mathbf{Z}, \mathbf{X})$, where $\mathbf{t} \in \{\mathbf{f}, \mathbf{g}, \mathbf{h}\}$. The following lemma follows easily from the identity (3.1) and (3.2).

Lemma 3.2.1. *For $n \geq 1$, the nonlinearity $N(\mathbf{f}_Z)$ and $N(\mathbf{h}_z)$ of $\mathbf{f}_z$ and $\mathbf{h}_z$ equal to 0 for every $z \in \mathbb{Z}_{2^n}$.*

For the sake of the completeness of the thesis, we will give the proof of one case of the following Theorem given in [35]:

Theorem 3.2.2. *For $n \geq 2$, the nonlinearity $N(\mathbf{g}_z)$ of the vector function $\mathbf{g}_z(\mathbf{X}) = \mathbf{g}(\mathbf{Z}, \mathbf{X})$ is zero for $z = 0$, 1, 2, 2^{n-1}, $2^{n-1} + 1$, $2^n - 1$.*

Proof For $z = 2^{n-1}$, let $d^{-1}(x) = \tilde{x} = \sum_{i=1}^{n+1} \tilde{x}_i 2^{i-1}$ and $X = \sum_{i=1}^{n} x_i 2^{i-1}$. Then we have $\mathbf{g}_{2^{n-1}}(\mathbf{X}) = v(d(2^{n-1}\tilde{x} \bmod (2^n + 1)))$ for any $x \in \mathbb{Z}_{2^n}$. $2^{n-1}\tilde{x} \bmod (2^n) = \sum_{i=1}^{n+1} \tilde{x}_i 2^{n+i-2} \bmod (2^n) = \tilde{x}_1 2^{n-1}$ and $2^{n-1}\tilde{x}$ div $(2^n) = \sum_{i=1}^{n+1} \tilde{x}_i 2^{n+i-2}$ div $(2^n) = \sum_{i=2}^{n+1} \tilde{x}_i 2^{i-2}$. To compute the component functions $r_i : \mathbb{Z}_2^n \to \mathbb{Z}_2$ of $\mathbf{g}_{2^{n-1}} = (r_n, \ldots, r_1)$, we need to look at several

cases:

Case 1: For $x \neq 0$ (i.e. $\tilde{x} = x$) and $x_1 \neq 0$,
$2^{n-1} = x_1 2^{n-1} = 2^{n-1}x \bmod (2^n) \geq 2^{n-1}x \text{ div } (2^n) = \sum_{i=2}^{n} x_i 2^{i-2}$. Then by using Lemma 2.2.3, $2^{n-1}x \bmod (2^n + 1) = \sum_{i=0}^{n-2} 2^i + 1 - \sum_{i=2}^{n} x_i 2^{i-2} = 1 + \sum_{i=2}^{n}(1 - x_i)2^{i-2}$ and from that equation the right-end component of the $\mathbf{g}_{2^{n-1}}(\mathbf{X})$, $r_1(\mathbf{X}) = (2 - x_2) \bmod (2) = x_2$.

Case 2: For $x \neq 0$ and $x_1 = 0$, $\sum_{i=2}^{n} x_i 2^{i-2} = 2^{n-1}x \text{ div } (2^n) > 2^{n-1}x \bmod (2^n) = 2^{n-1}x_1 = 0$. From Lemma 2.2.3, $2^{n-1}X \bmod (2^n + 1) = 2^n + 1 - (\sum_{i=2}^{n} x_i 2^{i-2})$. Hence $r_1(\mathbf{X}) = 1 - x_2 \bmod (2) = 1 \oplus x_2$.

Case 3: For $x = 0$, (i.e. $\tilde{x} = 2^n$), From Lemma 2.2.3, $2^{n-1}\tilde{x} \bmod (2^n+1) = 2^n + 1 - 2^{n-1} = 2^{n-1} + 1$ since $2^{n-1}\tilde{x} \bmod (2^n) = 0$ and $2^{n-1}\tilde{x} \text{ div } (2^n) = 2^{n-1}$ and we have $\mathbf{g}_{2^{n-1}}(\mathbf{0}) = (1, 0, \ldots, 0, 1)$. With this we computed explicitly all the values $\mathbf{g}_{2^{n-1}}(\mathbf{X})$ and leave the reader to check that $\mathbf{1} \cdot \mathbf{g}_{2^{n-1}}(\mathbf{X}) = r_1(\mathbf{X}) = x_1 \oplus x_2 \oplus 1 = \mathbf{3} \cdot \mathbf{X} \oplus 1$. This gives immediately $N(\mathbf{g}_{2^{n-1}}) = 0$. □

Lemma 3.2.3. *For $n \in \mathbb{Z}_+$ such that $gcd(a, 2^n + 1) = 1$, we have $N(\mathbf{g}_a) = N(\mathbf{g}_b)$ when $ab \equiv 1$ mod $(2^n + 1)$.*

Proof We have $\mathbf{g}_b(\mathbf{X}) = \mathbf{g}_{a^{-1}}(\mathbf{X})$ since $ab \equiv 1 \bmod (2^n+1)$. By Theorem 1 in [29], $N(\mathbf{g}_a) = N((\mathbf{g}_a)^{-1}) = N(\mathbf{g}_b)$. □

Lemma 3.2.4. *$N(\mathbf{g}_a) = N(\mathbf{g}_b)$ when $a + b \equiv 0$ mod $(2^n + 1)$.*

Proof The case $a = b = 0$ is trivial. For other (a, b) pairs, one can use the obvious relation $v^{-1}(\mathbf{g}_a(\mathbf{X})) + v^{-1}(\mathbf{g}_b(\mathbf{X})) \equiv 0 \bmod (2^n + 1)$ to complete the proof. □

Lemma 3.2.5. *$N(\mathbf{g}_{2^k}) = N(\mathbf{g}_{2^s})$ when $k+s=n$ for $k,s \geq 0$.*

Proof For $k+s=n$, we obtain that $2^s(2^k+2(2^s)^{-1}) \equiv 2^n+2 \equiv 1 \bmod (2^n+1)$. Here $(2^s)^{-1} \equiv 2^k+2(2^s)^{-1} \bmod (2^n+1)$ and we have $(2^s)^{-1}+2^k \equiv 0 \bmod (2^n+1)$. By using Lemma 3.2.4, we get $N(\mathbf{g}_{(2^s)^{-1}}) = N(\mathbf{g}_{2^k})$. From Theorem 1 in [29], we known that $N(\mathbf{g}_{(2^s)^{-1}}) = N(\mathbf{g}_{2^s})$. This completes the proof. □

Theorem 3.2.6. *For $n \geq 3$ and $2 \leq k \leq \lceil (n-1)/2 \rceil$, we have $N(\mathbf{g}_b) \leq 2^{k-1}$ when*

(i) $b = 2^k$ and $b = 2^{n-k}$.

(ii) $b + 2^k \equiv 0$ mod (2^n+1).

(iii) $b2^k \equiv 1$ mod (2^n+1).

Proof Assume that $n \geq 3$ and $2 \leq k \leq \lceil (n-1)/2 \rceil$. For every $\mathbf{X} \in \mathbb{Z}_2^n$, let $\mathbf{g}_{2^k}(\mathbf{X}) = (\mathbf{g}_{2^k}{}^{(n)}(\mathbf{X}), \ldots, \mathbf{g}_{2^k}{}^{(2)}(\mathbf{X}), \mathbf{g}_{2^k}{}^{(1)}(\mathbf{X}))$, and $\mathbf{g}_{2^k}{}^{(i)}(\mathbf{X})$ be i^{th} coordinate function of $\mathbf{g}_{2^k}(\mathbf{X})$.
Since $\mathbf{g}_2(0) = 2^n-1$, $\mathbf{g}_2(2^{n-1}) = 0$ and $\mathbf{g}_2(2j)$ is even and $\mathbf{g}_2(2j+1)$ is odd for all $j \in \{1, \ldots, 2^{n-1}-1\}$, the truth table of $\mathbf{g}_2{}^{(1)}$, $T_{\mathbf{g}_2{}^{(1)}} = S^{2^n}$, 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 $T_{\mathbf{g}_{2^k}{}^{(1)}}$ becomes $\{\underbrace{S^{2^{n-k+1}}, \ldots, S^{2^{n-k+1}}}_{(2^{k-1})-times}\}$. Therefore,
$\mathbf{g}_2^{(1)}(\mathbf{X}) = \overline{x_1}\,\overline{x_2} \ldots \overline{x_{n-1}} \oplus x_n$ and $\mathbf{g}_{2^k}^{(1)}(\mathbf{X}) = \overline{x_1}\,\overline{x_2} \ldots \overline{x_{n-k}} \oplus x_{n-k+1}$ according to their truth tables, where $\overline{x_i} = x_i \oplus 1$. We know that $\mathbf{g}_{2^k}^{(1)}(\mathbf{X}) \oplus \mathbf{g}_{2^k}^{(2)}(\mathbf{X}) = \mathbf{g}_{2^{k-1}}^{(1)}(\mathbf{X})$ since by the proof of Theorem 1 in [35], $y_2 \oplus y_1 = x_1$ for $\mathbf{g}_2(\mathbf{X}) = \mathbf{Y}$. The hamming distance between $\mathbf{g}_{2^k}^{(1)}(\mathbf{X})$ and x_{n-k+1} is 2^k.
This implies that $N(\mathbf{g}_{2^k}^{(1)}(\mathbf{X})) \leq 2^k$. By Theorem 12 in [38], $2^k \leq N(\mathbf{g}_{2^k}^{(1)}(\mathbf{X}))$

since the term $x_1 \dots x_{n-k}$ is not properly covered (see Definition 9 in [38]) by any other terms in $\mathbf{g}_{2^k}^{(1)}(\mathbf{X})$. Then, $N(\mathbf{g}_{2^k}{}^{(1)}(\mathbf{X})) = 2^k$ and we get $N(\mathbf{g}_{2^k}{}^{(1)}(\mathbf{X}) \oplus \mathbf{g}_{2^k}{}^{(2)}(\mathbf{X})) = N(\mathbf{g}_{2^{k-1}}{}^{(1)}(\mathbf{X})) = 2^{k-1}$. Hence, $N(\mathbf{g}_{2^k}(\mathbf{X})) \leq 2^{k-1}$ by using Definition 3.1.1. The remaining parts of this theorem can be easily proven by using Lemma 3.2.3, 3.2.4 and 3.2.5. □

Remark 1 We have checked that the inequalities in this theorem are equalities for $n \leq 16$, and we conjecture that this is also true for $n > 16$.

3.3 Linear Relations for Operations

As it can be seen from the proof of Theorem 3.2.2, we get the following linear relations for every $\mathbf{X} = v(x) \in \mathbb{Z}_2^n$ such that $\mathbf{X} \bigodot \mathbf{Z} = \mathbf{Y}$:

$$\mathbf{1} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} \oplus 1 = 0 \text{ for } z \in \{0, 1\} \tag{3.4}$$

$$\mathbf{3} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} \oplus 1 = 0 \text{ for } z \in \{2^{n-1}, 2^{n-1} + 1\} \tag{3.5}$$

$$\mathbf{1} \cdot \mathbf{X} \oplus \mathbf{3} \cdot \mathbf{Y} \oplus \mathbf{1} \cdot \mathbf{Z} = 0 \text{ for } z \in \{2, 2^n - 1\}, \tag{3.6}$$

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

We now give some properties of $L_{\bowtie,z}(a, b, c, \lambda)$ and in particular compute them for various z.

Proposition 3.3.1. *For $n \geq 2$ and $z \in \mathbb{Z}_{2^n}$, we have the following equalities:*

1) For all z and $a \in \{0, \dots, 2^n - 1\}$, $L_{\bigoplus,z}(a, a, a, 0) = 2^n$.

2) For all z, $L_{\boxplus,z}(1, 1, 1, 0) = 2^n$.

3) For $z \in \{2^{n-1}, 2^{n-1}+1\}$, $L_{\bigodot,z}(3,1,1,1) = 2^n$.

4) For $z \in \{2, 2^n - 1\}$, $L_{\bigodot,z}(1,3,1,0) = 2^n$.

5) For those $z \in \mathbb{Z}_{2^n}$ *such that* $gcd(d^{-1}(z), 2^n+1) = 1$, *let* z^{-1} *be the inverse of* $d^{-1}(z)$ *in* $\mathbb{Z}^*_{2^n+1}$. *Then* $L_{\bigodot,z}(a,b,0,\lambda) = L_{\bigodot,z^{-1}}(b,a,0,\lambda)$.

6) $L_{\bigboxplus,z}(a,b,0,\lambda) = L_{\bigboxplus,-z}(b,a,0,\lambda)$.

7) For $z + z' \equiv 0 \ mod\ (2^n+1)$, $L_{\bigodot,z}(a,b,0,\lambda) = L_{\bigodot,z'}(a,b,0,\lambda')$.

8) $L_{\bigodot,0}(2,2,0,0) = 2^n$; $L_{\bigodot,0}(3,3,0,1) = 2^n$; $L_{\bigodot,0}(6,4,0,0) = 2^n$; $L_{\bigodot,0}(7,5,0,1) = 2^n$; $L_{\bigodot,0}(4,6,0,0) = 2^n$; $L_{\bigodot,0}(5,7,0,1) = 2^n$.

9) For $m \in \{0, 1, \ldots, n-3\}$,
$L_{\bigodot,0}(2^{n-1-m}, 2^{n-1-m}, 0, 1) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+1, 2^{n-1-m}+1, 0, 0) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2, 2^{n-1-m}+2, 0, 1) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+3, 2^{n-1-m}+3, 0, 0) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+4, 2^{n-1-m}+6, 0, 1) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+5, 2^{n-1-m}+7, 0, 0) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+6, 2^{n-1-m}+4, 0, 1) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+7, 2^{n-1-m}+5, 0, 0) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}, 2^{n-1-m}+2^{n-2-m}, 0, 0) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}+1, 2^{n-1-m}+2^{n-2-m}+1, 0, 1) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}+2, 2^{n-1-m}+2^{n-2-m}+2, 0, 0) = 2^n - 2^{m+2}$.

$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}+3, 2^{n-1-m}+2^{n-2-m}+3, 0, 1) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}+4, 2^{n-1-m}+2^{n-2-m}+6, 0, 0) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}+5, 2^{n-1-m}+2^{n-2-m}+7, 0, 1) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}+6, 2^{n-1-m}+2^{n-2-m}+4, 0, 0) = 2^n - 2^{m+2}$.
$L_{\bigodot,0}(2^{n-1-m}+2^{n-2-m}+7, 2^{n-1-m}+2^{n-2-m}+5, 0, 1) = 2^n - 2^{m+2}$.

10) *For* $2 \le k \le n-1$,

i) $L_{\bigodot,2^k}(2^{n-k}, 1, 0, 0) = 2^n - 2^k$.

ii) $L_{\bigodot,2^k}(2^{n-k+1}, 3, 0, 0) = 2^n - 2^{k-1}$.

iii) $L_{\bigodot,2^k}(2^{n-k+1}+2^{n-k}, 2, 0, 0) = 2^n - 2^{k-1}$.

11) *For* $2 \le k \le n-1$,

i) $L_{\bigodot,2^k}(1, 2^k, 0, 1) = 2^n - 2^k$.

For $2 \le k \le n-2$,

ii) $L_{\bigodot,2^k}(2, 2^{k+1}+2^k, 0, 0) = 2^n - 2^{k-1}$.

iii) $L_{\bigodot,2^k}(3, 2^{k+1}, 0, 1) = 2^n - 2^{k-1}$.

12) *For all* z, $L_{\boxplus,z}(2,2,2,0) = 0.75 \cdot 2^n$.

13) *For* $z \in \{\, 4m+1 \mid m = 0, 1, \ldots, 2^{n-2}-1 \,\}$,
$L_{\boxplus,z}(1,1,0,1) = L_{\boxplus,z}(3,2,0,0) = 2^n$.

14) *For* $z \in \{\, 4m+3 \mid m = 0, 1, \ldots, 2^{n-2}-1 \,\}$,
$L_{\boxplus,z}(1,1,0,1) = L_{\boxplus,z}(3,2,0,1) = 2^n$.

For the remaining cases, $k = 1, 2, \ldots, n-2$ *:*

15) *For* $z \in \{\, 2^k + j2^{k+2} \mid j = 0, 1, \ldots, 2^{n-k-2} - 1\}$ *and* $a \in \{1, 2^2, 2^3, \ldots, 2^{k-1}\}$,
$L_{\boxplus,z}(a, a, 0, 0) = L_{\boxplus,z}(2^k, 2^k, 0, 1) = L_{\boxplus,z}(2^{k+1} + 2^k, 2^{k+1}, 0, 0) = 2^n$.

16) *For* $z \in \{\, 2^k + 2^{k+1} + j2^{k+2} \mid j = 0, 1, \ldots, 2^{n-k-2} - 1\,\}$ *and* $a \in \{1, 2^2, 2^3, \ldots, 2^{k-1}\}$,
$L_{\boxplus,z}(a, a, 0, 0) = L_{\boxplus,z}(2^k, 2^k, 0, 1) = L_{\boxplus,z}(2^{k+1} + 2^k, 2^{k+1}, 0, 1) = 2^n$.

17) *For* $z = 2^{n-1}$ *and* $a \in \{1, 2^2, 2^3, \ldots, 2^{n-2}\}$,
$L_{\boxplus,z}(a, a, 0, 0) = L_{\boxplus,z}(2^{n-1}, 2^{n-1}, 0, 1) = 2^n$.

Proof Parts *1,2,3,4* and both *5* and *6* follow easily from equations (3.1),(3.2),(3.5),(3.6) and the definition of $L_{\bowtie,z}$, respectively.

Part *7* follows easily from the fact that $v^{-1}(\mathbf{g}_z(\mathbf{X})) + v^{-1}(\mathbf{g}_{Z'}(\mathbf{X})) \equiv 0 \bmod (2^n + 1)$.

For part *8*, $\mathbf{2} \cdot \mathbf{X} = \mathbf{2} \cdot \mathbf{Y}$ since $\mathbf{X} \odot \mathbf{0} = v(2^n + 1 - x)$ for every $v(x) = \mathbf{X} \in \mathbb{Z}_2^n$. Using this equality and equation (4), we get $\mathbf{3} \cdot \mathbf{X} \oplus 1 = \mathbf{3} \cdot \mathbf{Y}$. If $\mathbf{2} \cdot \mathbf{X} = 0$, then $\mathbf{4} \cdot \mathbf{X} = \mathbf{4} \cdot \mathbf{Y}$. Otherwise, $\mathbf{4} \cdot \mathbf{X} \oplus 1 = \mathbf{4} \cdot \mathbf{Y}$. This means that $\mathbf{4} \cdot \mathbf{X} = \mathbf{6} \cdot \mathbf{Y}$.

For part *9*, for the first $\mathbf{K} = v(k)$ such that $\mathbf{K} \cdot \mathbf{X} = 1$, we have $\mathbf{J} \cdot \mathbf{X}' = \mathbf{J} \cdot \mathbf{X}$ and $\mathbf{T} \cdot \mathbf{X}' = \mathbf{T} \cdot \mathbf{X} \oplus 1$, where $\mathbf{J} = v(j), \mathbf{T} = v(t), 1 \leq k \leq n-1, 1 \leq j \leq k-1$ and $k - 1 < t \leq n - 1$ since $\mathbf{X} \odot \mathbf{0} = v(2^n + 1 - x)$ for every $\mathbf{X} \in \mathbb{Z}_2^n$. The

proof of this part follows from this observation and part *8*.

Parts *10(i)* and *10(ii)* can be directly proven by using the following facts :

- The hamming distance between $\mathbf{1} \cdot \mathbf{g}_{2^k}(\mathbf{X})$ and $\mathbf{S} \cdot \mathbf{X}$ is 2^k, where $\mathbf{S} = v(n-k)$.

- $\mathbf{1} \cdot \mathbf{g}_{2^k}(\mathbf{X}) \oplus \mathbf{2} \cdot \mathbf{g}_{2^k}(\mathbf{X}) = \mathbf{1} \cdot \mathbf{g}_{2^{k-1}}(\mathbf{X})$.

To prove part *10(iii)*, it is enough to combine equalities in parts *10(i)* and *10(ii)*.

All cases of part *11* can be shown by using parts *5*, *7* and *10*.

In order to prove part *12*, we use the following fact:

$$\mathbf{2} \cdot \mathbf{Y} = \mathbf{2} \cdot \mathbf{X} \oplus (\mathbf{1} \cdot \mathbf{X})(\mathbf{1} \cdot \mathbf{Z}) \text{ for all } \mathbf{X} \text{ and } \mathbf{Z} \in \mathbb{Z}_2^n. \tag{3.7}$$

To prove parts *13* and *14*, it suffices to consider equations (3.3) and (3.7). Note that for both parts, $\mathbf{1} \cdot \mathbf{Z} = 1$.

Parts *15* and *16* hold since it is easy to observe that $\mathbf{2^l} \cdot \mathbf{Z} = 0$, where $l \in \{0, \ldots, k-1\}$ and $\mathbf{2^k} \cdot \mathbf{Z} = 1$. Moreover, $\mathbf{2^{k+1}} \cdot \mathbf{Z} = 0$ and $\mathbf{2^{k+1}} \cdot \mathbf{Z} = 1$ for parts *15* and *16*, respectively.

Part *17* is also satisfied because of the equation $\mathbf{2^l} \cdot \mathbf{Z} = 0$, where $l \in \{0, \ldots, n-2\}$. □

Remark 2

1) A weak key class having 2^{23} keys of IDEA cipher was constructed in

[8] using three linear relations (with probability one) for IDEA cipher's operations given in equations (3.1),(3.2) and (3.4). By the help of these relations and linear relation in equation (3.5), the number of elements of this weak key class is increased to 2^{24} in Section 3.6.

2) We note that part *8* was observed by Nakahara independently [27].

3) Parts *10* and *11* hold for $z = (2^k)^{-1}$ and $z = 2^n + 1 - 2^k$ due to parts *5* and *7*.

3.4 Linear Relations for 1-round IDEA

3.4.1 Known Linear Relations

For 1-round IDEA, Daemen et al. [8] found 15 linear relations hold with probability one due to the linearity of operations of IDEA (see equations in 3.1, 3.2, 3.4). These relations marked by (*) are given in Table 3.1. 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 3.1). 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 [33],[35]. Similar to the work of Daemen et al. [8], 0, 1 and these key values were used as round multiplicative keys to derive extra 39 linear relations in [34]. All these 54 linear relations (holding with probability one) with the related key subbblocks restrictions are listed in Table 3.1. 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, we can express

Table 3.1: List of linear relations for 1-round IDEA given in [8] (indicated by *) and [34]. 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
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
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
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
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
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
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	-
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	-
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
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	-	-
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	-	-
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	-	-	-	$\mp 2^{15}$	-	-
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	-
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
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
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
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
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
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	-
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	-
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	-
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	-
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	$\mp 2^{15}$	-
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	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	-
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	-	-	-	-	-
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	-	$2k$	-	-	-
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	$\mp 2^{15}$	-	-	-	-	-

Table 3.1 (cont'd)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6
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
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
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
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
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
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
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	-
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	-
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	-	$2k$	-	$\mp 2^{15}$	-
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
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
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
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
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
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
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
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
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
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
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	-	-
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	-	-	$\mp 2^{15}$	-	-
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	-	-
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	$\mp 2^{15}$	-	-	$\mp 2^{15}$	-	-
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	-	-
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	-	$2k$	$\mp 2^{15}$	-	-
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	-	-
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	-	-
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	-	-

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 24^{th} linear relation in Table 3.1, one of 15 linear relations found in [8]:

Example 1: Adding first two output of 1-round IDEA, namely $\mathbf{Y}_1$ and $\mathbf{Y}_2$, 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 $\mathbf{Y}_1 = \mathbf{X}_1 \bigodot \mathbf{Z}_1$ is $\mathbf{1} \cdot \mathbf{Y}_1 = \mathbf{1} \cdot \mathbf{X}_1 \oplus \mathbf{1} \cdot \mathbf{Z}_1 \oplus 1$ from the equation 3.4 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 equation 3.2. The addition of $\mathbf{1} \cdot \mathbf{Y}_1$ and $\mathbf{1} \cdot \mathbf{Y}_2$ becomes

$$\mathbf{1} \cdot \mathbf{Y}_1 \oplus \mathbf{1} \cdot \mathbf{Y}_2 = \mathbf{1} \cdot \mathbf{X}_1 \oplus \mathbf{1} \cdot \mathbf{Z}_1 \oplus \mathbf{1} \cdot \mathbf{X}_3 \oplus \mathbf{1} \cdot \mathbf{Z}_3 \oplus 1 \tag{3.8}$$

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

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

Example 2: From the Table 3.1, 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 39 linear relations derived in [34], is the 42^{th} linear relation in Table 3.1.

3.4.2 New Linear Relations

Let us consider the 35^{th} and the 45^{th} linear relations for 1-round IDEA in Table 3.1 to obtain a new relation which is not listed in Table 3.1.

For the 35^{th} 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 45^{th} 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 equations (3.9) and (3.10) respectively

$$\mathbf{1}\cdot\mathbf{Z}_1 \oplus \mathbf{1}\cdot\mathbf{Z}_2 \oplus \mathbf{2}\cdot\mathbf{Z}_3 \oplus \mathbf{1}\cdot\mathbf{Z}_5 \oplus \mathbf{1}\cdot\mathbf{X}_1 \oplus \mathbf{1}\cdot\mathbf{X}_2 \oplus \mathbf{2}\cdot\mathbf{X}_3 \oplus \mathbf{1}\cdot\mathbf{Y}_2 \oplus \mathbf{1}\cdot\mathbf{Y}_3 \oplus \mathbf{1} = 0 \tag{3.9}$$

$$\mathbf{1}\cdot\mathbf{Z}_1 \oplus \mathbf{1}\cdot\mathbf{Z}_2 \oplus \mathbf{2}\cdot\mathbf{Z}_3 \oplus \mathbf{1}\cdot\mathbf{Z}_6 \oplus \mathbf{1}\cdot\mathbf{X}_1 \oplus \mathbf{1}\cdot\mathbf{X}_2 \oplus \mathbf{3}\cdot\mathbf{X}_3 \oplus \mathbf{3}\cdot\mathbf{Y}_1 \oplus \mathbf{3}\cdot\mathbf{Y}_2 \oplus \mathbf{1}\cdot\mathbf{Y}_4 \oplus \mathbf{1} = 0 \tag{3.10}$$

Equations (3.9) and (3.10) 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:

$$\mathbf{1} \cdot \mathbf{Z}_5 \oplus \mathbf{1} \cdot \mathbf{Z}_6 \oplus \mathbf{1} \cdot \mathbf{X}_3 \oplus \mathbf{3} \cdot \mathbf{Y}_1 \oplus \mathbf{2} \cdot \mathbf{Y}_2 \oplus \mathbf{1} \cdot \mathbf{Y}_3 \oplus \mathbf{1} \cdot \mathbf{Y}_4 \oplus \mathbf{1} = 0 \tag{3.11}$$

We have used many inputs for 1-round IDEA to check that linear relation in (3.11) 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 3.1. Considering these known linear relations, we found additional 242 new linear relations for 1-round IDEA (see Table B.1, 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 unneccessary restrictions using 50000 test vectors.

We note that this algorithm with first 5 steps was presented in [36]. The last step has been added as a result of comments provided by Nakahara [27]. All 54 linear relations in Table 3.1 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.

3.5 Linear Relations for 1-round RIDEA

In order to derive 15 linear relations for 1-round IDEA discovered in [8], all 15 combinations of round output subblocks $\mathbf{Y}_i$ in Section 2.2.1 should be examined. For each of these combinations, there is only one related linear relation if multiplicative key subblocks are restricted to 0 or 1 when it is necessary. Using the same approach to derive these relations, other set of 39 linear relations were discovered in [34]. And based on these linear relations, new set of linear relations has been produced by Algorithm 1 in Section 3.4.2. Starting point for finding linear relations 1-round RIDEA is to study all 15 combinations of round output subblocks $\mathbf{Y}_i$ in Section 2.2.2. For only combinations $\mathbf{Y}_1 \bigoplus \mathbf{Y}_2$, $\mathbf{Y}_3 \bigoplus \mathbf{Y}_4$, $\mathbf{Y}_1 \bigoplus \mathbf{Y}_2 \bigoplus \mathbf{Y}_3 \bigoplus \mathbf{Y}_4$, $\mathbf{Y}_2 \bigoplus \mathbf{Y}_3$, $\mathbf{Y}_1 \bigoplus \mathbf{Y}_4$, $\mathbf{Y}_1 \bigoplus \mathbf{Y}_3$ and $\mathbf{Y}_2 \bigoplus \mathbf{Y}_4$, there are 7 linear relations for 1-round RIDEA like those discovered in [8]. Because $\widetilde{\mathbf{T}}$ in Section 2.2.2 can not be expressed by a linear relation since $\mathbf{Q}$ involves in the RMA-structure by $\bigodot$ operation, $\mathbf{Q}$ frequently changes and it can not be restricted as round multiplicative key subblocks. This is also case for $\widetilde{\mathbf{U}}$ because $\widetilde{\mathbf{U}} = (\mathbf{P} \bigodot \mathbf{Z}_5) \boxplus \widetilde{\mathbf{T}}$. Hence the number of linear relations for 1-round RIDEA is 7 if restriction for only key points 0 or 1 is done. This means that the number of linear relations for 1-round RIDEA is quite less than for 1-round IDEA considering other approaches introduced for 1-round IDEA to obtain more linear relations based on known ones.

3.6 Linear Weak Key Classes for IDEA

As indicated in Table 3.2, three linear relations, namely the 24^{th}, the 33^{th} and the 12^{th} relations in Table 3.1 were successively used to find a linear relation for 8,5-round IDEA holding with probability one [8]. 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

Table 3.2: 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	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	-	-

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 3.3). 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 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 (Figure 3.3) and there are 2^{24} such keys.

If we choose four 16-bit input subblocks for 8,5-round IDEA as $\mathbf{X}_1^{(1)} \in$

Table 3.3: 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	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	-	-

$\{\mathbf{0},\mathbf{1}\}$ and for any $\mathbf{X}_2^{(1)}, \mathbf{X}_3^{(1)}$ and $\mathbf{X}_4^{(1)} \in \{\mathbf{0},\ldots,\mathbf{2^{16}-1}\}$ and we remove restriction on $\mathbf{Z}_1^{(1)}$ subkey of the first round relation in Table 3.2, we can construct a class of weak keys with cardinality 2^{27}. Because in this case zero key bits' indices of the master key are between 4-25, 29-71, and 75-110. Hence we have the same linear relation $(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0}) \rightarrow (\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$ for 8,5-round IDEA in Table 3.2 under the chosen plaintext assumption given above.

We haven't discovered other linear relations in Table 3.1 and Table B.1 similar to the best linear relation giving a large class of weak keys because of the following reasons:

- If we compare Table 3.1 with Table B.1 in Appendix, then it can be seen that for most cases, linear relations in Table 3.1 derived in [8] have less key restrictions than others.

- In Table 3.1, 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 restric-

tions. There aren't any linear relations with one key subblock restriction in Table B.1, but there are linear relations numbered with $44, 226, 105, 141, 181$ having two key subblocks restrictions in Table B.1. 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 [8] in both Table 3.1 and Table B.1. 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 138^{th} linear relation in Table B.1, 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 Table 3.1 and Table B.1.

Now we discuss cases for which the nonlinearity of a function of the form $x_i y_j \oplus y_k$ is zero, where $\mathbf{X} = (x_n, x_{n-1}, \ldots, x_1), \mathbf{g}_Z(\mathbf{X}) = \mathbf{Y} = \mathbf{Z} \odot \mathbf{X}$, $x_i = \mathbf{2}^{i-1} \cdot \mathbf{X}, y_k = \mathbf{2}^{k-1} \cdot \mathbf{Y}$.

Proposition 3.6.1. *For all $n \geq 2$, we have*

1) $H((\mathbf{1} \cdot \mathbf{X})(\mathbf{1} \cdot \mathbf{g}_0(\mathbf{X})) \oplus \mathbf{1} \cdot \mathbf{g}_0(X)) = H((\mathbf{2} \cdot \mathbf{X})(\mathbf{2} \cdot \mathbf{g}_0(\mathbf{X})) \oplus \mathbf{1} \cdot \mathbf{g}_0(\mathbf{X})) = 0.$
$H((\mathbf{1} \cdot \mathbf{X})(\mathbf{1} \cdot \mathbf{g}_0(\mathbf{X})) \oplus \mathbf{2} \cdot \mathbf{g}_0(\mathbf{X})) = H((\mathbf{2^2} \cdot \mathbf{X})(\mathbf{2} \cdot \mathbf{g}_0(\mathbf{X})) \oplus \mathbf{2^3} \cdot \mathbf{g}_0(\mathbf{X})) = 0.$

$H((\mathbf{1}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_0(\mathbf{X}))\oplus\mathbf{2^2}\cdot\mathbf{g}_0(\mathbf{X}))=H((\mathbf{2}\cdot\mathbf{X})(\mathbf{2}\cdot\mathbf{g}_0(\mathbf{X}))\oplus\mathbf{2^2}\cdot\mathbf{g}_0(\mathbf{X}))=0$. $H((\mathbf{2}\cdot\mathbf{X})(\mathbf{2^2}\cdot\mathbf{g}_0(\mathbf{X}))\oplus\mathbf{2^3}\cdot\mathbf{g}_0(\mathbf{X}))=H((\mathbf{2^2}\cdot\mathbf{X})(\mathbf{2^2}\cdot\mathbf{g}_0(\mathbf{X}))\oplus\mathbf{2^3}\cdot\mathbf{g}_0(\mathbf{X}))=0$.

2) *For* $k\in\{2,\ldots,n-1\}$, $H((\mathbf{2^{n-k}}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_{2^k}(\mathbf{X}))\oplus\mathbf{2}\cdot\mathbf{g}_{2^k}(\mathbf{X}))=0$.

3) $H((\mathbf{1}\cdot\mathbf{X})(\mathbf{2}^{n-1}\cdot\mathbf{g}_{2^{n-2}}(\mathbf{X}))\oplus\mathbf{1}\cdot\mathbf{g}_{2^{n-2}}(\mathbf{X}))=H((\mathbf{2^2}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_{2^{n-2}}(\mathbf{X}))\oplus\mathbf{2}\cdot\mathbf{g}_{2^{n-2}}(\mathbf{X}))=0$.

4) $H((\mathbf{1}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_{2^{n-1}}(\mathbf{X}))\oplus\mathbf{2}\cdot\mathbf{g}_{2^{n-1}}(\mathbf{X}))=H((\mathbf{2}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_{2^{n-1}}(\mathbf{X}))\oplus\mathbf{2}\cdot\mathbf{g}_{2^{n-1}}(\mathbf{X}))=0$.

5) *For* $z\in\{2^{n-1},2^{n-1}+1\}$ $H((\mathbf{1}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_z(\mathbf{X}))\oplus\mathbf{2}\cdot\mathbf{g}_z(\mathbf{X}))=H((\mathbf{2}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_z(\mathbf{X}))\oplus\mathbf{2}\cdot\mathbf{g}_z(\mathbf{X}))=0$

6) *For* $i\in\{2,\ldots,n-1\}$, $H((\mathbf{2^{i-1}}\cdot\mathbf{X})(\mathbf{2^{i-2}}\cdot\mathbf{g}_{2^{n-1}+1}(\mathbf{X}))\oplus\mathbf{2^{i-1}}\cdot\mathbf{g}_{2^{n-1}+1}(\mathbf{X}))=0$.

Proof Proposition 3.3.1 can be directly used to prove part *1*.
To prove part *2*, we consider the following facts used in the proof of Theorem 3.2.6:

- $\mathbf{1}\cdot\mathbf{g}_{2^k}(\mathbf{X})\oplus\mathbf{2}\cdot\mathbf{g}_{2^k}(\mathbf{X})=\mathbf{1}\cdot\mathbf{g}_{2^{k-1}}(\mathbf{X})$
- $\mathbf{1}\cdot\mathbf{g}_{2^k}(\mathbf{X})=\mathbf{1}\cdot\mathbf{g}_{2^k}(\mathbf{X})=\overline{x_1}\,\overline{x_2}\ldots\overline{x_{n-k}}\oplus x_{n-k+1}$

From these two facts, we have $\mathbf{2}\cdot\mathbf{g}_{2^k}(\mathbf{X})=\mathbf{2}\cdot\mathbf{g}_{2^k}(\mathbf{X})=\mathbf{1}\cdot\mathbf{g}_{2^k}(\mathbf{X})\oplus\mathbf{1}\cdot\mathbf{g}_{2^{k-1}}(\mathbf{X})$ and therefore, we get $(\mathbf{2}^{n-k}\cdot\mathbf{X})(\mathbf{1}\cdot\mathbf{g}_{2^k}(\mathbf{X}))\oplus\mathbf{2}\cdot\mathbf{g}_{2^k}(\mathbf{X})=\mathbf{1}\oplus 2^{n-k+1}\cdot\mathbf{X}$. This finishes the proof of this part. In a similar fashion, other parts can be easily proven. □

CHAPTER 4

DIFFERENCE PROPERTIES

4.1 Difference Properties of Operations

Differential cryptanalysis is a powerful technique to analyze symmetric ciphers and cryptographic hash functions (Section 2.1.1). This is done by considering how input differences affect the output differences. This fact leads us to do the similar thing for the function $\mathbf{X} \to \mathbf{X} \bowtie \mathbf{Z} = \mathbf{Y}$ corresponding to the operation $\bowtie \in \{\boxplus, \odot, \bigoplus\}$. We introduce the set $\mathbf{D}_{\bowtie,z}(a,b)$ for fixed a, b and $z \in \mathbb{Z}_{2^n}$ associated to $\bowtie$ and obtain several interesting properties of it. We hope that these properties could be exploited to cryptanalyze ciphers which operation $\bowtie$ is used.

Definition 4.1.1. *For fixed* $a = v^{-1}(\mathbf{A}), b = v^{-1}(\mathbf{B}), z = v^{-1}(\mathbf{Z}) \in \mathbb{Z}_{2^n}$ *and* $\bowtie \in \{\boxplus, \odot, \bigoplus\}$, *let*
$\mathbf{D}_{\bowtie,z}(a,b) = \{(\mathbf{X}, \mathbf{X}_a) \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n \,|\, (\mathbf{X} \bowtie \mathbf{Z}) \bigoplus (\mathbf{X}_a \bowtie \mathbf{Z}) = \mathbf{B}\,, \mathbf{X}_a = \mathbf{X} \bigoplus \mathbf{A}\}$.

Proposition 4.1.2. *We have the following:*

1) $|\mathbf{D}_{\boxplus,z}(a,b)| = |\mathbf{D}_{\boxplus,-z}(b,a)|$, *where* $-z$ *is the additive inverse of* z *in* $\mathbb{Z}_{2^n}$.

2) $|\mathbf{D}_{\boxplus,z}(a,b)| = |\mathbf{D}_{\boxplus,-z}(a,b)|$.

3) $|\mathbf{D}_{\boxplus,z}(a,b)| = |\mathbf{D}_{\boxplus,z}(b,a)|$.

4) $|\mathbf{D}_{\odot,z}(a,b)| = |\mathbf{D}_{\odot,z^{-1}}(b,a)|$, *where* $z^{-1} = d((d^{-1}(z))^{-1})$ *provided that* $d^{-1}(z)$ *has the inverse* $(d^{-1}(z))^{-1}$ *in* $\mathbb{Z}^*_{2^n+1}$.

Proof For part *1*, it is easy to see that the map

$\varphi : \mathbf{D}_{\boxplus,z}(a,b) \longrightarrow \mathbf{D}_{\boxplus,-z}(b,a)$ given by $(\mathbf{X}, \mathbf{X}_a) \longmapsto (\mathbf{X}\boxplus\mathbf{Z}, \mathbf{X}_a\boxplus\mathbf{Z})$.

is one-to-one and onto, and therefore $|\mathbf{D}_{\boxplus,z}(a,b)| = |\mathbf{D}_{\boxplus,-z}(b,a)|$.

Part *2* follows from the bijectivity property of the map

$\phi : \mathbf{D}_{\boxplus,z}(a,b) \longrightarrow \mathbf{D}_{\boxplus,-z}(a,b)$, $\phi(\mathbf{X}, \mathbf{X}_a) = ((\mathbf{2^n - 1})\boxplus(-\mathbf{X}), (\mathbf{2^n - 1})\boxplus(-\mathbf{X}_a))$ and the following two facts:

- $((\mathbf{2^n - 1})\boxplus(-\mathbf{X}))\bigoplus((\mathbf{2^n - 1})\boxplus(-\mathbf{X}_a)) = \mathbf{A}$ for every $(\mathbf{X}, \mathbf{X}_a)$.
- $(((\mathbf{2^n - 1})\boxplus(-\mathbf{X}))\boxplus(-\mathbf{Z}))\bigoplus(((\mathbf{2^n - 1})\boxplus(-\mathbf{X}_a))\boxplus(-\mathbf{Z})) = ((\mathbf{2^n - 1})\boxplus(-(\mathbf{X}\boxplus\mathbf{Z})))\bigoplus((\mathbf{2^n - 1})\boxplus(-(\mathbf{X}_a\boxplus\mathbf{Z}))) = \mathbf{B}$ for every $(\mathbf{X}, \mathbf{X}_a) \in \mathbf{D}_{\boxplus,z}(a,b)$.

Part *3* follows from parts *1* and *2*.
For part *4*, the following ψ map is bijective:

$\psi : \mathbf{D}_{\bigodot,z}(a,b) \longrightarrow \mathbf{D}_{\bigodot,z^{-1}}(b,a)$ given by $(\mathbf{X}, \mathbf{X}_a) \longmapsto (\mathbf{X}\bigodot\mathbf{Z}, \mathbf{X}_a\bigodot\mathbf{Z})$.

Hence these two sets have the same cardinality. □

Proposition 4.1.3. *Let a, b and $z \in \mathbb{Z}_{2^n}$. Then*

1) For all a, b and z, $0 \leq |\mathbf{D}_{\bowtie,z}(a,b)| \leq 2^{n-1}$.

2) For all a and z, $|\mathbf{D}_{\bigoplus,z}(a,a)| = 2^{n-1}$.

3) For all a, $|\mathbf{D}_{\boxplus,0}(a,a)| = |\mathbf{D}_{\boxplus,2^{n-1}}(a,a)| = |\mathbf{D}_{\bigodot,1}(a,a)| = 2^{n-1}$.

4) For all z, $|\mathbf{D}_{\boxplus,z}(2^{n-1},2^{n-1})| = 2^{n-1}$.

5) For $z \in \{0,1\}$, $|\mathbf{D}_{\bigodot,z}(2^{n-1},2^{n-1})| = 2^{n-1}$.

6) For $z \in \{0,1\}$, $|\mathbf{D}_{\bigodot,z}(1,1)| = 2^{n-1}$.

7) For all even z, $|\mathbf{D}_{\boxplus,z}(1,1)| = 2^{n-1}$.

8) For $2 \leq k \leq n-2$, $z \in \{2^k, 2^n - 2^k\}$, and $(a,b) \in \{(m,m), (2^{n-1}+m, 2^{n-1}+m) \,|\, m = 1,\ldots,2^k-1\}$, $|\mathbf{D}_{\boxplus,z}(a,b)| = 2^{n-1}$.

9) For $z \in \{2^{n-2}, 2^n - 2^{n-2}\}$ and $(a,b) \in \{(j,j), (2^{n-2}+j, 2^{n-2}+2^{n-1}+j), (2^{n-2}+2^{n-1}+j, 2^{n-2}+j) \,|\, j = 1,\ldots,2^{n-2}-1\}$, $|\mathbf{D}_{\boxplus,z}(a,b)| = 2^{n-1}$.

10) For $z \in \{\ 2^l k, 2^n - 2^l k \ \mid\ 2 \leq l \leq n-2\,,\ k = 2m-1\,,\ m \in \mathbb{Z}^+$ and $2^l k < 2^n\ \}$ and $a \in \{1,\ldots,2^l-1\}$, $|\mathbf{D}_{\boxplus,z}(a,a)| = 2^{n-1}$.

Proof It is easy to check the parts *1* through *5* and therefore we shall give the proof for the rest. Assume that $\mathbf{Y} = \mathbf{X} \boxplus \mathbf{Z}$ and $\mathbf{Y}_a = \mathbf{X}_a \boxplus \mathbf{Z}$ for $\mathbf{A} = v(a) \in \mathbb{Z}_2^n$ and $\mathbf{X}_a = \mathbf{X} \bigoplus \mathbf{A}$.

For part *6*, it is known that $\mathbf{Y} = \mathbf{X} \bigodot \mathbf{0} = v(2^n + 1 - x)$ and $\mathbf{Y}_1 = \mathbf{X}_1 \bigodot \mathbf{0} = v(2^n + 1 - x_1)$. Hence we have $\mathbf{Y} \bigoplus \mathbf{Y}_1 = \mathbf{1}$ when $z = 0$.

For part *7*, for even values of z, we have $(\mathbf{1}\cdot(\mathbf{X}\boxplus\mathbf{Z}))\bigoplus(\mathbf{1}\cdot(\mathbf{X}_1\boxplus\mathbf{Z})) = (\mathbf{1}\cdot\mathbf{X})\bigoplus(\mathbf{1}\cdot\mathbf{X}_1) = 1$ and $\mathbf{2^l}\cdot\mathbf{Y}_1 = \mathbf{2^l}\cdot\mathbf{Y}$ for $1 \leq l \leq n-1$.

To prove part *8*, for $z = 2^k$, $a \in \{1, \ldots, 2^k - 1\}$ and every $(\mathbf{X}, \mathbf{X}_a)$ pair, $\mathbf{Y}\bigoplus\mathbf{Y}_a = \mathbf{A}$ since $\mathbf{2^l}\cdot\mathbf{Y}_a = \mathbf{2^l}\cdot\mathbf{X} \oplus \mathbf{2^l}\cdot\mathbf{A}$ and $\mathbf{2^l}\cdot\mathbf{Y} = \mathbf{2^l}\cdot\mathbf{X}$, where $l \in \{0, \ldots, k-1\}$, $\mathbf{2^k}\cdot\mathbf{Y}_a = \mathbf{2^k}\cdot\mathbf{Y} = \mathbf{2^k}\cdot\mathbf{X} \oplus 1$ and $\mathbf{2^l}\cdot\mathbf{Y}_a = \mathbf{2^l}\cdot\mathbf{X}_a = \mathbf{2^l}\cdot\mathbf{X} = \mathbf{2^l}\cdot\mathbf{Y}$ for $k < l \leq n-1$ because $\mathbf{2^t}\cdot\mathbf{A} = 0$ for $t \geq k$.

For $z = 2^k$ and $a = 2^{n-1} + m$, where $m \in \{1, \ldots, 2^k - 1\}$, $\mathbf{Y}\bigoplus\mathbf{Y}_a = \mathbf{A}$. Because only difference comparing to first case is as follows:

$\mathbf{2^{n-1}}\cdot\mathbf{Y}_a = \mathbf{2^{n-1}}\cdot\mathbf{X} \oplus 1 = \mathbf{2^{n-1}}\cdot\mathbf{Y}$

By Proposition 4.1.2, part *8* also hold for $-z = 2^n - 2^k$ which is an additive inverse of $z = 2^k$.

Similar to part *8*, part *9* (respectively part *10*) can be proven by using the former (respectively the latter) fact:

- $\mathbf{2^{n-1}}\cdot\mathbf{Y}_a = \mathbf{2^{n-1}}\cdot\mathbf{Y} \oplus 1 = \mathbf{2^{n-1}}\cdot\mathbf{X} \oplus \mathbf{2^{n-2}}\cdot\mathbf{X} \oplus 1$, where $\mathbf{2^{n-1}}\cdot\mathbf{X}_a = \mathbf{2^{n-1}}\cdot\mathbf{X}$.
- $\mathbf{2^s}\cdot(\mathbf{2^l}\cdot\mathbf{k}) = 0$ for $0 \leq s \leq l-1$. □

Remark 3 In [8], a weak class of keys with cardinality 2^{35} and extended version of this class having 2^{51} keys were found based on parts *2, 4* and *5*.

4.2 Impossible Differences for Operations

Lemma 4.2.1. *For all integer* $n \geq 4$,

1) $|\mathbf{D}_{\boxplus,z}(a,b)| = 0$ *for all* $z \in \mathbb{Z}_{2^n}$, *when*

(i) a *is odd and* b *is even or*

(ii) a *is even and* b *is odd.*

2) $|\mathbf{D}_{\boxplus,z}(a, 2^k-1)| = |\mathbf{D}_{\boxplus,z}(2^k-1, a)| = 0$ *for all* $z \in \mathbb{Z}_{2^n}$, *when* $k \in \{2, \ldots, n-2\}$ *and odd* $a \in \{2^s+1, \ldots, (\sum_{i=k}^{s} 2^i)-1 \mid k+1 \leq s \leq n-1\}$.

3) $|\mathbf{D}_{\boxplus,2^k}(2^k, 2^k)| = 0$ *for* $k \in \{1, \ldots, n-2\}$.

4) $|\mathbf{D}_{\boxplus,z}(a,b)| = |\mathbf{D}_{\boxplus,z}(b,a)| = 0$ *for all* $z \in \mathbb{Z}_{2^n}$ *for even* a *and* b *such that* $\mathbf{2}^i \cdot \mathbf{A} = 0$, $\mathbf{2}^l \cdot \mathbf{A} = 1$, $\mathbf{2}^j \cdot \mathbf{B} = 0$, $\mathbf{2}^k \cdot \mathbf{B} = 1$, *where* $l < k$, $i \in \{0, \ldots, l-1\}$ *and* $j \in \{0, \ldots, k-1\}$.

5) $|\mathbf{D}_{\boxplus,z}(a,b)| = 0$ *for all* $z \in \mathbb{Z}_{2^n} \setminus \{0\}$ *and all* $a, b \in \mathbb{Z}_{2^n}$ *such that* $b \equiv a + z \mod 2^n$.

Proof

For part *1*, let us consider the least significant bits of both sides of the equality $(\mathbf{X} \boxplus \mathbf{Z}) \bigoplus (\mathbf{X}_a \boxplus \mathbf{Z}) = \mathbf{B}$. If $|\mathbf{D}_{\boxplus,z}(a,b)| > 0$, then they should be equal to each other due to the equations 3.1 and 3.2. That is, $\mathbf{1} \cdot \mathbf{X} \oplus \mathbf{1} \cdot \mathbf{Z} \oplus \mathbf{1} \cdot \mathbf{X}_a \oplus \mathbf{1} \cdot \mathbf{Z} = \mathbf{1} \cdot \mathbf{A} = \mathbf{1} \cdot \mathbf{B}$. This completes the proof of this part.

For part *5*, $|\mathbf{D}_{\boxplus,z}(a,b)| = 0$ for every odd z since if $|\mathbf{D}_{\boxplus,z}(a,b)| > 0$, then $\mathbf{1}\cdot((\mathbf{X}\boxplus\mathbf{Z})\bigoplus(\mathbf{X}_a\boxplus\mathbf{Z})) = \mathbf{1}\cdot\mathbf{A} = \mathbf{1}\cdot\mathbf{B} = \mathbf{1}\cdot\mathbf{A}\oplus\mathbf{1}\cdot\mathbf{Z}$. With comparing other bits of $(\mathbf{X}\boxplus\mathbf{Z})\bigoplus(\mathbf{X}_a\boxplus\mathbf{Z})$ and $\mathbf{B}$, it can be easily concluded that $|\mathbf{D}_{\boxplus,z}(a,b)| > 0$ only if $z = 0$. We leave the proof of other parts to the reader.

Conjecture 4.2.2. *For all $z \in \mathbb{Z}_{2^n}$, there exists one and only one (a,b) such that $|\mathbf{D}_{\odot,z}(a,b)| = 0$. In fact, this (a,b) is equal to $(1,2^{n-1})$.*

4.3 Impossible Differentials for 1-round IDEA

In [4], a general technique called *miss in the middle* was used to construct impossible differential by finding two events with probability one whose conditions cannot be satisfied together. $(\mathbf{A};\mathbf{0};\mathbf{A};\mathbf{0}) \longrightarrow (\mathbf{B};\mathbf{B};\mathbf{0};\mathbf{0})$ (respectively $(\mathbf{0};\mathbf{A};\mathbf{0};\mathbf{A}) \longrightarrow (\mathbf{0};\mathbf{0};\mathbf{B};\mathbf{B})$), a 2,5-round IDEA impossible differential (where $\mathbf{A} = v(a), \mathbf{B} = v(b)$ and $a \neq 0 \neq b$) was discovered in [4]. In this section we find impossible differentials for 1-round IDEA directly.

Definition 4.3.1. *For a fixed round key Z, a differential for 1-round IDEA under the XOR operation is of the form:*
$(\triangle\mathbf{X}_1, \triangle\mathbf{X}_2, \triangle\mathbf{X}_3, \triangle\mathbf{X}_4) \longrightarrow (\triangle\mathbf{Y}_1, \triangle\mathbf{Y}_2, \triangle\mathbf{Y}_3, \triangle\mathbf{Y}_4)$, *where* $\triangle\mathbf{X}_i = \mathbf{X}_i\bigoplus\mathbf{X}_i^*$ *for* $i \in \{1,2,3,4\}$ *and*

$$\triangle\mathbf{Y}_1 = \{(\mathbf{X}_1\odot\mathbf{Z}_1)\bigoplus\mathbf{T}\}\bigoplus\{(\mathbf{X}_1^*\odot\mathbf{Z}_1)\bigoplus\mathbf{T}^*\} = (\mathbf{X}_1\odot\mathbf{Z}_1)\bigoplus(\mathbf{X}_1^*\odot\mathbf{Z}_1)\bigoplus\triangle\mathbf{T}$$
$$\triangle\mathbf{Y}_2 = \{(\mathbf{X}_3\boxplus\mathbf{Z}_3)\bigoplus\mathbf{T}\}\bigoplus\{(\mathbf{X}_3^*\boxplus\mathbf{Z}_3)\bigoplus\mathbf{T}^*\} = (\mathbf{X}_3\boxplus\mathbf{Z}_3)\bigoplus(\mathbf{X}_3^*\boxplus\mathbf{Z}_3)\bigoplus\triangle\mathbf{T}$$
$$\triangle\mathbf{Y}_3 = \{(\mathbf{X}_2\boxplus\mathbf{Z}_2)\bigoplus\mathbf{U}\}\bigoplus\{(\mathbf{X}_2^*\boxplus\mathbf{Z}_2)\bigoplus\mathbf{U}^*\} = (\mathbf{X}_2\boxplus\mathbf{Z}_2)\bigoplus(\mathbf{X}_2^*\boxplus\mathbf{Z}_2)\bigoplus\triangle\mathbf{U}$$
$$\triangle\mathbf{Y}_4 = \{(\mathbf{X}_4\odot\mathbf{Z}_4)\bigoplus\mathbf{U}\}\bigoplus\{(\mathbf{X}_4^*\odot\mathbf{Z}_4)\bigoplus\mathbf{U}^*\} = (\mathbf{X}_4\odot\mathbf{Z}_4)\bigoplus(\mathbf{X}_4^*\odot\mathbf{Z}_4)\bigoplus\triangle\mathbf{U}$$

Definition 4.3.2. *A differential for 1-round IDEA is impossible if it is not satisfied by any round key Z.*

From the identity (2.4) in Section 2.2.1, we know that if $\triangle\mathbf{P} = \mathbf{P}\bigoplus\mathbf{P}^* = \mathbf{0}$ and $\triangle\mathbf{Q} = \mathbf{Q}\bigoplus\mathbf{Q}^* = \mathbf{0}$, then we have $\triangle\mathbf{U} = \mathbf{U}\bigoplus\mathbf{U}^* = \mathbf{0}$ and $\triangle\mathbf{T} = \mathbf{T}\bigoplus\mathbf{T}^* = \mathbf{0}$ for two MA-structure outputs $(\mathbf{U}, \mathbf{T})$ and $(\mathbf{U}^*, \mathbf{T}^*)$. Assuming that $\triangle\mathbf{P} = \mathbf{0}$ and $\triangle\mathbf{Q} = \mathbf{0}$, we have the following type of differentials for 1-round IDEA for every $\triangle\mathbf{X}_i$ differences

$$(\triangle\mathbf{X}_1, \triangle\mathbf{X}_2, \triangle\mathbf{X}_3, \triangle\mathbf{X}_4) \longrightarrow (\triangle\mathbf{Y}_1, \triangle\mathbf{Y}_2, \triangle\mathbf{Y}_3, \triangle\mathbf{Y}_4) \tag{4.1}$$

where $\triangle\mathbf{Y}_1 = (\mathbf{X}_1\bigodot\mathbf{Z}_1)\bigoplus(\mathbf{X}_1^*\bigodot\mathbf{Z}_1)$, $\triangle\mathbf{Y}_2 = (\mathbf{X}_3\boxplus\mathbf{Z}_3)\bigoplus(\mathbf{X}_3^*\boxplus\mathbf{Z}_3)$, $\triangle\mathbf{Y}_3 = (\mathbf{X}_2\boxplus\mathbf{Z}_2)\bigoplus(\mathbf{X}_2^*\boxplus\mathbf{Z}_2)$, $\triangle\mathbf{Y}_4 = (\mathbf{X}_4\bigodot\mathbf{Z}_4)\bigoplus(\mathbf{X}_4^*\bigodot\mathbf{Z}_4)$.

Note that if $\triangle\mathbf{Y}_1 = \triangle\mathbf{Y}_2$ and $\triangle\mathbf{Y}_3 = \triangle\mathbf{Y}_4$, then many types of impossible differentials for 1-round IDEA can be derived by using parts of Lemma 4.2.1. For example,

- let us consider the part *5* of Lemma 4.2.1. For all $a, b, z \in \mathbb{Z}_{2^n}$ such that $z \neq 0$, $b \equiv a + z \mod 2^n$ and $\mathbf{B} = v(b)$, if we choose $\triangle\mathbf{X}_2$ as $\mathbf{A} = v(a)$, then we have the following type of impossible differentials for 1-round IDEA based on (4.1) type of differential for 1-round IDEA:

  $$(\triangle\mathbf{X}_1, \mathbf{A}, \triangle\mathbf{X}_3, \triangle\mathbf{X}_4) \longrightarrow (\triangle\mathbf{Y}_1, \triangle\mathbf{Y}_2, \mathbf{B}, \mathbf{B})$$

- The following type of impossible differentials for 1-round IDEA can be derived due to the part *3* of Lemma 4.2.1 by choosing $\triangle\mathbf{X}_2$ as odd $a \in \{2^s + 1, \ldots, (\sum_{i=k}^{s} 2^i) - 1 \mid k + 1 \leq s \leq 15, k = 1, \ldots, 14\}$:

  $$(\triangle\mathbf{X}_1, \mathbf{A}, \triangle\mathbf{X}_3, \triangle\mathbf{X}_4) \longrightarrow (\triangle\mathbf{Y}_1, \triangle\mathbf{Y}_2, \mathbf{C}_k, \mathbf{C}_k),$$

  where $\mathbf{C}_k = v(2^k - 1)$.

Let us discuss another type of differentials for 1-round IDEA to find impossible differentials using the identity (2.5) in Section 2.2.1 and the part

2 of Lemma 4.2.1. Assuming that $\mathbf{P}\boxplus\mathbf{P}^* = \mathbf{1}$ and $\mathbf{Q}\boxplus\mathbf{Q}^* = \mathbf{0}$, we have $\mathbf{U}\boxplus\mathbf{U}^* = \mathbf{2}$ (i.e. $\triangle\mathbf{U} = \mathbf{U}\bigoplus\mathbf{U}^*$ is even) and $\mathbf{T}\boxplus\mathbf{T}^* = \mathbf{1}$ (i.e. $\triangle\mathbf{T} = \mathbf{T}\bigoplus\mathbf{T}^*$ is odd). Then considering $\triangle\mathbf{Y}_2$ or $\triangle\mathbf{Y}_3$ listed in Definition 4.3.1, the following differentials for 1-round IDEA are impossible:

- $(\triangle\mathbf{X}_1, \triangle\mathbf{X}_2, \mathbf{A}, \triangle\mathbf{X}_4) \longrightarrow (\triangle\mathbf{Y}_1, \mathbf{B}, \triangle\mathbf{Y}_3, \triangle\mathbf{Y}_4)$ if both a and b are even (respectively odd).
- $(\triangle\mathbf{X}_1, \mathbf{A}, \triangle\mathbf{X}_3, \triangle\mathbf{X}_4) \longrightarrow (\triangle\mathbf{Y}_1, \triangle\mathbf{Y}_2, \mathbf{B}, \triangle\mathbf{Y}_4)$ if a is even (respectively odd) b is odd (respectively even).

4.4 Impossible Differentials for Pseudo-Hadamard Transform

The Pseudo-Hadamard transform (PHT), used in block ciphers such as SAFER and Twofish, is a reversible transformation of two n-bit blocks that provides cryptographic diffusion. The PHT can be defined as

$$\mathrm{PHT}(\mathbf{X}_1,\, \mathbf{X}_2) = (\mathbf{Y}_1,\, \mathbf{Y}_2) = (\mathbf{2X}_1\boxplus\mathbf{X}_2, \mathbf{X}_1\boxplus\mathbf{X}_2).$$

For $\triangle\mathbf{X}_i = \mathbf{X}_i\bigoplus\mathbf{X}_i^*$ and $\triangle\mathbf{Y}_i = \mathbf{Y}_i\bigoplus\mathbf{Y}_i^*$, $i \in \{1, 2\}$, let
$(\triangle\mathbf{X}_1,\, \triangle\mathbf{X}_2) \longrightarrow (\triangle\mathbf{Y}_1,\, \triangle\mathbf{Y}_2)$ be a differential for PHT, where
$\triangle\mathbf{Y}_1 = (\mathbf{2X}_1\boxplus\mathbf{X}_2)\bigoplus(\mathbf{2X}_1^*\boxplus\mathbf{X}_2^*)$ and $\triangle\mathbf{Y}_2 = (\mathbf{X}_1\boxplus\mathbf{X}_2)\bigoplus(\mathbf{X}_1^*\boxplus\mathbf{X}_2^*)$.

If $\triangle\mathbf{X}_1 = \mathbf{0}$ for such differentials, then we have $\mathbf{2X}_1 = \mathbf{2X}_1^*$ and $\mathbf{X}_1 = \mathbf{X}_1^*$. Here both $v^{-1}(\mathbf{2X}_1)$ and $v^{-1}(\mathbf{X}_1)$ can be considered as z in all parts of Lemma 4.2.1 and then for varying $\triangle\mathbf{X}_2$, all impossible differences $\triangle\mathbf{Y}_1$ and $\triangle\mathbf{Y}_2$ can be found by using all parts of this Lemma to list many impossible differentials for PHT. In the same manner, if $\triangle\mathbf{X}_2$ is chosen as $\mathbf{0}$, then many impossible differentials for PHT can be found.

CHAPTER 5

CONCLUSION

We considered three mixing operations, the addition ($\boxplus$), the multiplication ($\odot$) and the XOR ($\oplus$) as vector functions from $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ to $\mathbb{Z}_2^n$. By fixing one of the variables, namely $\mathbf{Z} = v(z) \in \mathbb{Z}_2^n$ in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$, we obtained vector valued functions $\mathbf{f}_z$, $\mathbf{g}_z$ and $\mathbf{h}_z$: $\mathbb{Z}_2^n \to \mathbb{Z}_2^n$. In this thesis,

- We gave some transformations $\tau : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}$ such that the nonlinearity of $\mathbf{g}_z$ and the nonlinearity of $\mathbf{g}_{\tau(z)}$ are the same.
- We presented an upper bound for the nonlinearity of $\mathbf{g}_{2^k}$ and we checked that this upper bound is sharp for $n \leq 16$ and conjectured that it is so for any positive integer n.
- We provided the list of those z such that the nonlinearity of $\mathbf{f}_z$ and the nonlinearity of $\mathbf{g}_z$ are zero and we obtained all associated linear relations for those $\mathbf{f}_z$ and $\mathbf{g}_z$. In addition to this, for some $z \in \mathbb{Z}_{2^n}$ we obtained relations from the function $\mathbf{g}_z$ which are almost linear, namely linear relations with a high probability.
- We derived an algorithm to find 242 new linear relations for 1-round IDEA.
- We found two classes of weak keys with cardinality 2^{24} and 2^{27}. This fact extends the related work done by Daemen et al.
- We observed that 1-round RIDEA has quite less linear relations than 1-round IDEA.

- We obtained several algebraic properties of the operations $\boxplus$, $\odot$, $\oplus$ and cryptographic properties of the set of input and output differences defined by them.
- We found impossible differentials for 1-round IDEA and Pseudo-Hadamard Transform.

The design of the MESH block ciphers are based on operations of IDEA. In fact, both operations $\boxplus$ and $\oplus$ have been widely used as building blocks in many cryptosystems such as RC6, Twofish, MARS, FEAL, SAFER family and Helix ciphers. In the literature some of the properties of the operations were used to attack the block cipher IDEA. We hope that the several other properties of the mixing operations presented in this thesis can be used to cryptanalyze the ciphers mentioned above.

REFERENCES

[1] E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems. Journal of Cryptography, 4(1):3-72, 1991.

[2] E. Biham and A. Shamir, Differential Cryptanalysis of the Full 16-round DES, Advances in Cryptology – CRYPTO '92, Springer Verlag, pp.487-496, 1992

[3] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[4] E. Biham, A. Biryukov and A. Shamir, Miss in the Middle Attacks on IDEA and Khufu, Fast Software Encryption Workshop, LNCS 1636, pp 124-138, Springer-Verlag, 1999.

[5] J. Borst, Differential-Linear Cryptanalysis of IDEA, Department of Electrical Engineering, ESAT-COSIC Technical Report 96/2, 14 pages.

[6] J. Borst, L.R. Knudsen and V. Rijmen, Two Attacks on Reduced IDEA (Extended Abstract), Advances in Cryptology - EUROCRYPTO'97, Proceedings, Springer-Verlag, pp.1–13, 1998.

[7] J. Daemen, R. Govaerts, J. Vandewalle, Block ciphers based on modular arithmetic, Proceedings of the 3rd symposium on State and Progress of Research in Cryptography, W. Wolfowicz, Ed., Fondazione Ugo Bordoni, 1993, pp. 80-89.

[8] J. Daemen, R. Govaerts and J. Vandewalle, Weak Keys for IDEA. Advances in Cryptology, Proc. EUROCRYPTO'93, LNCS 773, Springer-Verlag, pp. 224-231, 1994.

[9] J. Daemen and V. Rijmen, The Design of Rijndael, ISBN 3540425802, Springer Verlag, 2002.

[10] S. Garfinkel, PGP: Pretty Good Privacy, ISBN 1565920988, O'Reilly Media, 1994.

[11] C. Harpes, G. G. Kramer, and J.L. Massey, Generilisation of linear cryptanalysis and the applicability of Matsui's piling-up lemma, Advances in Cryptology, EUROCRYPT0'95, LNCS, vol 921, pp 24-38, 1995.

[12] P. Hawkes, Differential-Linear Weak Key Classes of IDEA, Advances in Cryptology, EUROCRYPT0'98, pp. 112-126, 1998.

[13] B. Kaliski, M. Robshaw , Linear Cryptanalysis Using Multiple Approximations, CRYPTO'94, LNCS 839, page 26-38, (1994)

[14] L.R. Knudsen, Truncated and higher order differentials, In B. Preneel, editor, Fast Software Encryption - Second International Workshop, Leuven, Belgium, LNCS 1008, pages 196-211. Springer Verlag, 1995.

[15] X. Lai and J. L. Massey, A Proposal for a New Block Encryption Standard. Advances in Cryptology - EUROCRYPTO'90, Proceedings, LNCS 473, pp. 389-404, Springer-Verlag, Berlin, 1990.

[16] X. Lai, On the design and security of block cipher. ETH Series in Information Processing, V.1, Konstanz: Hartung-Gorre Verlag, 1992

[17] X. Lai, J. L. Massey and S. Murphy, Markov Ciphers and Differential Cryptanalysis. Advances in Cryptology EUROCRYPT91, Proceedings, Springer-Verlag, LNCS 547, pp. 1738, Springer-Verlag, 1991.

[18] X. Lai, Higher order derivatives and differential cryptanalysis, In Proc. "Symposium on Communication, Coding and Cryptography", in honor

of James L. Massey on the occasion of his 60'th birthday, Feb. 10-13, 1994, Monte-Verita, Ascona, Switzerland, 1994.

[19] H. Lipmaa, IDEA: A Cipher for Multimedia Architectures?, Selected Areas in Cryptography 1998, LNCS volume 1556 , pp 253–268, Kingston, Canada, August 17–18, 1998. Springer-Verlag.

[20] M. Matsui and A.Yamagishi, A New Method for Known Plaintext Attack of FEAL Cipher, Lectures Notes in Computer Science, Advances in Cryptology, proceedings of EUROCRYPT'92, pp. 81-91, 1992.

[21] M. Matsui, The First Experimental Cryptanalysis of the Data Encryption Standard, Advances in Cryptology — CRYPTO'94. 1-11

[22] M. Matsui, Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology EUROCRYPT 93 Proceedings, Springer-Verlag, LNCS 765, 1994, pp. 386397.

[23] W. Meier, On the Security of the IDEA Block Cipher. Advances in Cryptology EUROCRYPT 93 Proceedings, Springer-Verlag, LNCS 765, 1994, pp. 371385.

[24] S. Murphy, The Cryptanalysis of FEAL-4 with 20 Chosen Plaintexts, Journal of Cryptography, No.3, 1990

[25] J. Nakahara Jr., Cryptanalysis and Design of Block Ciphers, SCD/COSIC Group, Dept. Elektrotechniek, Katholieke Universiteit Leuven, Belgium, Jun. 2, 2003.

[26] J. Nakahara, Jr., V. Rijmen, B. Preneel, J. Vandewalle, The MESH Block Ciphers. The 4th International Workshop on Info. Security Applications, WISA 2003, Springer-Verlag, LNCS 2908, 2003, pp. 458-473.

[27] J. Nakahara Jr., personal communication, November 2004.

[28] K. Nyberg and L.R. Knudsen, Provable security against differential cryptanalysis, Advances in Cryptology – CRYPTO '92 pp. 566-574, 1992.

[29] K. Nyberg, On the construction of highly nonlinear permutations. In Extended Abstracts – EUROCRYPTO'92, pages 89-94, May 1992.

[30] M. Robshaw and L.R. Knudsen, Non-Linear Approximations in Linear Cryptanalysis, EUROCRYPTO'96, LNCS 1070, pp. 224-236, 1996.

[31] C. Shannon, Communication Theory of Secrecy Systems, Bell Systems Technical Journal, v28, Oct 1949, pp. 659-715.

[32] T. Shimoyama and T. Kaneko, Quadratic Reation of S-box and Its Application to the Linear Attack of Full Round DES, Advances in Cryptology, CRYPTO'98, LNCS 1462, pp. 200-211

[33] H. M. Yıldırım, Nonlinearity Properties of the Mixing Operations of the Block Cipher IDEA, Master Thesis, Middle East Technical University, Sep 2000.

[34] H. M. Yıldırım, Some Linear Relations for Block Cipher IDEA, Master Thesis (Term Project), Middle East Technical University, Jan 2002.

[35] H. M. Yıldırım, Nonlinearity Properties of the Mixing Operations of the Block Cipher IDEA, Progress in Cryptology - INDOCRYPT 2003, LNCS 2904, pp. 68-81, Springer-Verlag Heidelberg, 2003.

[36] H. M. Yıldırım and E. Akyıldız, New Properties of IDEA Cipher Operations, National Cryptology Symposium I, METU, Proceedings Book, pp. 156-166, November 18-19-20, 2005.

[37] J. Kelsey, B. Schneier, and D. Wagner, Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES, Advances in Cryptology, CRYPT0'96, LNCS, vol 1109, pp 237-251, 1996.

[38] X. Zhang, Y. Zheng and H. Imai, Duality of Boolean Functions and Its Cryptographic Significance, Information and Communications Security, Proceedings of ICICS'97, Beijing , LNCS, Vol. 1334, pp. 159-169, Springer-Verlag, 1997.

APPENDIX A

IDEA, PES AND RIDEA BLOCK CIPHERS

A.1 Block cipher IDEA

A.1.1 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.

IDEA uses the algorithm used for the encryption in its decryption. For the decryption process of IDEA (Figure 2.1), the ciphertext
$\mathbf{Y} = (\mathbf{Y}_1, \mathbf{Y}_2, \mathbf{Y}_3, \mathbf{Y}_4)$ taken as an input and the decryption key subblocks $\mathbf{K}_i^{(r)}$ derived from the encryption key subblocks $\mathbf{Z}_i^{(r)}$. The decryption key subblocks $\mathbf{K}_i^{(r)}$ are computed as:

For $r = 2, 3, .., 8$,
$\left(\mathbf{K}_1^{(r)}, \mathbf{K}_2^{(r)}, \mathbf{K}_3^{(r)}, \mathbf{K}_4^{(r)}\right) = \left(\mathbf{Z}_1^{(10-r)}, -\mathbf{Z}_3^{(10-r)}, -\mathbf{Z}_2^{(10-r)}, \mathbf{Z}_4^{((10-r))^{-1}}\right)$;

Table A.1: 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	-	-

For $r = 1$ and 9,
$\left(\mathbf{K}_1^{(r)}, \mathbf{K}_2^{(r)}, \mathbf{K}_3^{(r)}, \mathbf{K}_4^{(r)}\right) = \left(\mathbf{Z}_1^{(10-r)}, -\mathbf{Z}_2^{(10-r)}, -\mathbf{Z}_3^{(10-r)}, \mathbf{Z}_4^{((10-r))^{-1}}\right)$;
For $r = 1, 2, .., 8$,
$\left(\mathbf{K}_5^{(r)}, \mathbf{K}_6^{(r)}\right) = \left(\mathbf{Z}_5^{(r)}, \mathbf{Z}_6^{(r)}\right)$;
where z^{-1} denotes the multiplicative inverse (modulo $2^{16} + 1$) of z , i.e., $\mathbf{Z} \odot \mathbf{Z}^{-1} = 1$ and $-z$ denotes the additive (modulo 2^{16}) of z, i.e., $-\mathbf{Z} \boxplus \mathbf{Z} = \mathbf{0}$.

A.2 Block Cipher PES

As it can be seen from the graph of the encryption of PES (see Figure A.2 and Figure 2.1), there is a minor changes between the block ciphers IDEA and PES. In fact it was stated by the designers of IDEA that *"The only essential modification is that a different (and simpler) permutation of subblocks is used at the end of each of the first 7 rounds. The software implementation of IDEA is in fact more efficient than that of PES"* [16]. Due to that change, the encryption algorithm and the formulation for the subblock keys used in PES is slightly changed in IDEA. Similar to the block

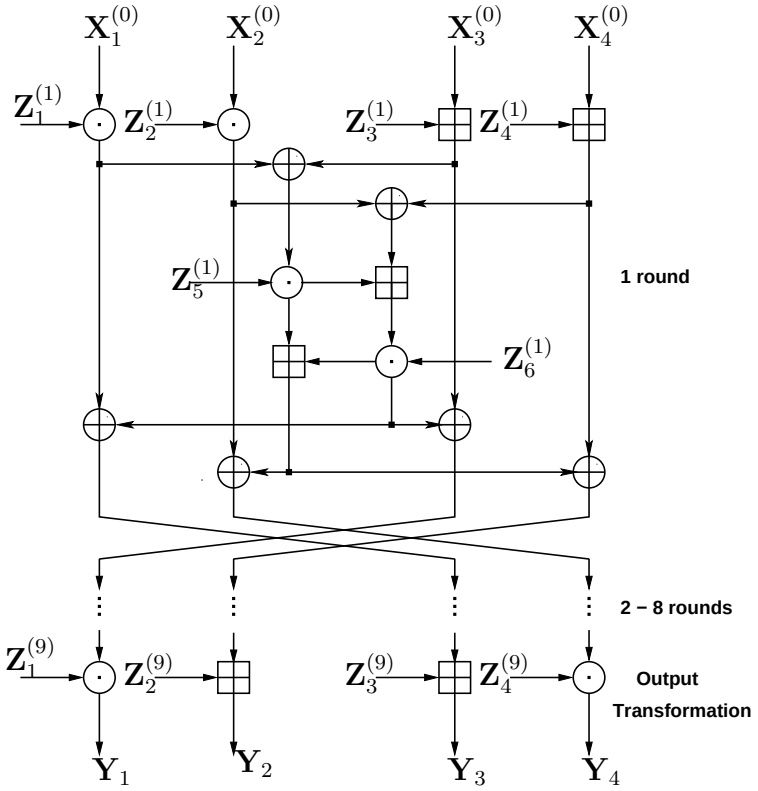

Figure A.1: Computational graph for the encryption process of the PES cipher

cipher IDEA, PES encrypts blocks of 64 bits plaintext to blocks of 64 bits ciphertext with 128 bit key and uses the same operations $\boxplus$, $\odot$ and $\bigoplus$.

A.3 Block Cipher RIDEA

By changing MA-structure slightly, so-called RMA (Reverse MA) structure was introduced. It is clear that this modification is minor and it does not change any other structure of IDEA like operations, encryption-decryption similarity and key scheduling algoritm. This slightly modified version of IDEA having the RMA-structure, the block cipher RIDEA (Reverse IDEA)

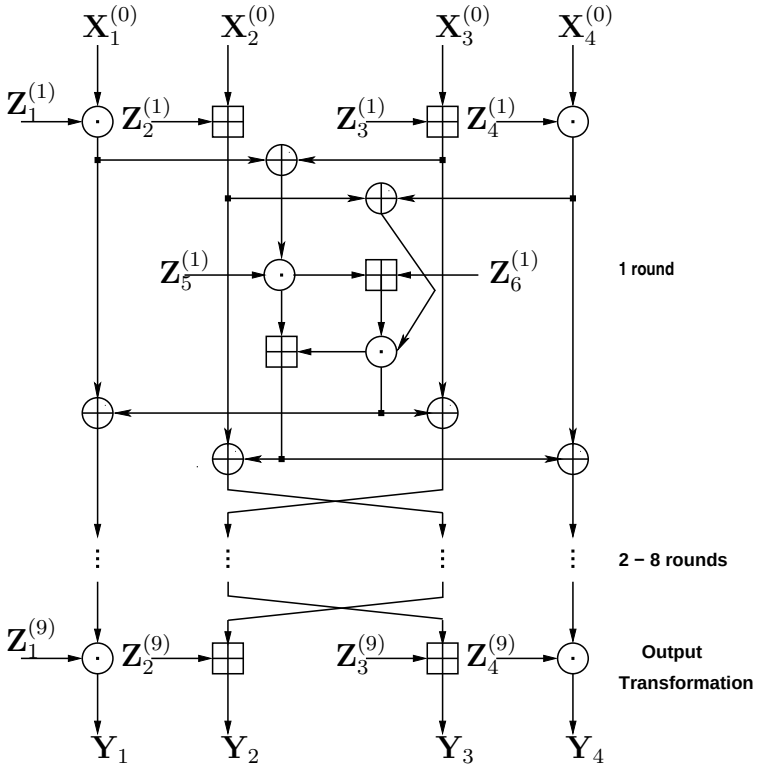

Figure A.2: Computational graph for the encryption process of the RIDEA cipher

was proposed as a variant of IDEA [33] and [35]. According to calculations given in [33],[35], it was believed that RMA-structure not only provides the required diffusion but also increases the nonlinearity of IDEA.

APPENDIX B

LIST OF NEW LINEAR RELATIONS FOR 1-ROUND IDEA

Table B.1: List of new linear relations for 1-round IDEA, based on linear relations of Table 3.1, 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
1	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	-	-
2	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{0})$	1	-	-	$2k$	∓ 1	$\mp 2^{15}$	∓ 1
3	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k+1$	∓ 1	∓ 1	∓ 2
4	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	-	-	$2k$	∓ 1	∓ 1	∓ 2
5	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1
6	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	-	∓ 2
7	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1})$	1	-	-	$2k+1$	-	$\mp 2^{15}$	∓ 1
8	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	-	$2k+1$	∓ 1	∓ 1	∓ 2
9	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	-	$2k$	-	$\mp 2^{15}$	∓ 2
10	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	1	-	-	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 2
11	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2
12	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	1	∓ 2	$2k$	$2k+1$	∓ 2	-	-
13	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k+1$	$2k$	∓ 2	∓ 1	∓ 1
14	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k$	$2k$	∓ 2	∓ 1	∓ 1
15	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	-	-	$2k+1$	∓ 1	-	∓ 2
16	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	1	-	-	$2k+1$	∓ 1	$\mp 2^{15}$	-
17	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k$	$\mp 2^{15}$	-	∓ 2
18	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 2	-	$2k$	$\mp 2^{15}$	∓ 1	-
19	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 1	-	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 2
20	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1

Table B.1 (cont'd)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6
21	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1
22	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2
23	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	$\mp 2^{15}$	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	-
24	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	0	-	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2
25	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k$	$\mp 2^{15}$	∓ 1	∓ 2
26	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 1
27	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 1	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	-
28	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k$	$2k+1$	∓ 2	∓ 1	-
29	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	1	∓ 2	-	$2k$	-	∓ 1	∓ 2
30	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	1	∓ 2	-	$2k$	-	∓ 1	-
31	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1
32	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	0	∓ 2	-	$2k+1$	∓ 1	-	∓ 2
33	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	-	-	$2k$	$\mp 2^{15}$	-	∓ 2
34	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k+1$	∓ 1	∓ 1	∓ 2
35	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	∓ 1	$2k+1$	-	∓ 2	∓ 1	-
36	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	∓ 1	$2k$	$2k+1$	∓ 2	-	∓ 2
37	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k+1$	-	$\mp 2^{15}$	-
38	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 2	-	$2k+1$	∓ 1	-	-
39	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2
40	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	-	-	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2
41	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2
42	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 2	-	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 1
43	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	1	∓ 1	-	$2k$	-	$\mp 2^{15}$	∓ 1
44	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{3})$	1	-	$2k+1$	-	∓ 2	-	-
45	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	1	-	$2k$	-	∓ 2	∓ 1	-
46	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 2
47	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k+1$	$2k$	∓ 2	-	∓ 1
48	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 2	-	$2k$	∓ 1	∓ 1	∓ 1
49	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	0	∓ 1	$2k$	-	∓ 2	-	∓ 1
50	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	1	∓ 2	-	$2k+1$	-	$\mp 2^{15}$	-
51	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	-	$2k+1$	-	-	∓ 2
52	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	-	$2k$	∓ 1	$\mp 2^{15}$	-
53	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k$	$\mp 2^{15}$	∓ 1	∓ 2
54	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k$	$2k+1$	∓ 2	-	∓ 1
55	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 1
56	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	0	$\mp 2^{15}$	$2k+1$	-	∓ 2	-	-
57	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	-
58	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{2})$	0	∓ 2	$2k$	$2k$	∓ 2	-	∓ 2
59	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 1	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	-
60	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1
61	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 2	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	-
62	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	-	∓ 2
63	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{2})$	1	-	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1
64	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{2})$	1	-	$2k$	-	∓ 2	-	∓ 1
65	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 2	-	$2k+1$	-	-	∓ 1
66	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{3})$	1	-	$2k$	$2k$	∓ 2	$\mp 2^{15}$	-

Table B.1 (cont'd)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6
67	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2
68	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	-	-	$2k+1$	$\mp 2^{15}$	-	∓ 2
69	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 1	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2
70	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 2	-	$2k$	-	-	∓ 2
71	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0})$	0	-	-	$2k+1$	-	$\mp 2^{15}$	-
72	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	1	$\mp 2^{15}$	-	$2k$	-	$\mp 2^{15}$	∓ 1
73	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	1	-	-	$2k+1$	-	∓ 1	∓ 2
74	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	-	∓ 2	-	∓ 1
75	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2
76	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	-	$2k+1$	-	-	∓ 2
77	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	-	$2k$	∓ 1	$\mp 2^{15}$	-
78	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 1	-	$2k$	-	∓ 1	∓ 2
79	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	1	$\mp 2^{15}$	-	-	-	∓ 1	∓ 1
80	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	∓ 1	$2k$	$2k$	∓ 2	-	∓ 2
81	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{0})$	1	-	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1
82	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	0	∓ 2	-	$2k+1$	$\mp 2^{15}$	-	∓ 2
83	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{2})$	0	-	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1
84	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2
85	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k$	$2k$	∓ 2	∓ 1	∓ 2
86	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	-	-	$2k$	$\mp 2^{15}$	∓ 1	∓ 2
87	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 1	$2k+1$	$2k+1$	∓ 2	-	∓ 2
88	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	-	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2
89	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	1	-	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2
90	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k+1$	$2k+1$	∓ 2	∓ 1	-
91	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
92	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{2})$	0	-	$2k$	$2k$	∓ 2	-	∓ 2
93	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	$\mp 2^{15}$	$2k+1$	-	∓ 2	∓ 1	-
94	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	-	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 1
95	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2
96	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	1	-	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	-
97	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k$	$2k$	∓ 2	$\mp 2^{15}$	-
98	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2
99	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	-	$2k$	-	-	∓ 2
100	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	0	-	$2k+1$	-	∓ 2	∓ 1	-
101	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k$	∓ 1	$\mp 2^{15}$	∓ 2
102	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
103	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 1	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	-
104	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1
105	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	0	-	-	$2k$	-	-	∓ 2
106	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	-	$2k$	-	∓ 1	∓ 2
107	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	1	∓ 2	-	$2k+1$	-	∓ 1	∓ 1
108	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	-	$2k$	-	$\mp 2^{15}$	-
109	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k$	-	∓ 2	∓ 1	∓ 1
110	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	1	∓ 1	$2k+1$	-	∓ 2	-	∓ 1

Table B.1 (cont'd)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6
111	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1})$	0	-	-	$2k$	-	$\mp 2^{15}$	∓ 1
112	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 2	-	$2k$	∓ 1	∓ 1	∓ 2
113	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	$2k$	∓ 2	-	∓ 2
114	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k$	$2k$	∓ 2	∓ 1	-
115	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	-	$2k+1$	∓ 1	-	∓ 2
116	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 1	-	$2k+1$	-	∓ 1	∓ 2
117	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	∓ 1	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	-
118	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 2	-	$2k+1$	∓ 1	∓ 1	-
119	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k+1$	$\mp 2^{15}$	∓ 1	∓ 2
120	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{2})$	1	∓ 2	$2k+1$	$2k+1$	∓ 2	-	∓ 1
121	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	-	∓ 2
122	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	1	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	-
123	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 2	-	$2k+1$	-	∓ 1	∓ 2
124	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 2	-	$2k+1$	$\mp 2^{15}$	-	-
125	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	0	-	-	$2k+1$	-	$\mp 2^{15}$	∓ 2
126	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{2})$	1	∓ 2	$2k+1$	$2k$	∓ 2	-	∓ 2
127	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{0})$	0	-	-	$2k+1$	∓ 1	$\mp 2^{15}$	∓ 1
128	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{2})$	0	-	$2k+1$	-	∓ 2	-	∓ 1
129	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
130	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{3})$	0	-	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	-
131	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	1	-	-	$2k$	-	∓ 1	∓ 2
132	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 1	-	$2k$	∓ 1	$\mp 2^{15}$	∓ 1
133	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	-	$2k$	-	-	∓ 2
134	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{2})$	0	-	$2k$	$2k+1$	∓ 2	-	∓ 2
135	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 2	-	$2k$	$\mp 2^{15}$	∓ 1	∓ 1
136	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k+1$	-	∓ 2	∓ 1	∓ 1
137	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k$	∓ 1	$\mp 2^{15}$	∓ 2
138	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
139	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	1	∓ 2	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	-
140	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 1	-	$2k+1$	-	$\mp 2^{15}$	∓ 1
141	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 2	-	$2k+1$	-	-	-
142	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1
143	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	1	∓ 1	-	$2k+1$	-	$\mp 2^{15}$	∓ 2
144	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{2})$	0	-	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2
145	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k$	$2k$	∓ 2	∓ 1	∓ 2
146	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	∓ 1	$2k+1$	$2k$	∓ 2	-	∓ 2
147	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k$	-	$\mp 2^{15}$	-
148	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 1	-	$2k+1$	∓ 1	$\mp 2^{15}$	-
149	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 2	-	$2k$	-	$\mp 2^{15}$	∓ 1
150	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	-	∓ 2	-	∓ 1
151	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0})$	1	∓ 2	-	$2k+1$	∓ 1	-	∓ 1
152	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k+1$	∓ 1	-	∓ 2
153	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	-	$2k+1$	-	∓ 1	∓ 2
154	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{2})$	1	-	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 2

Table B.1 (cont'd)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6
155	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	1	∓ 2	-	$2k$	∓ 1	-	∓ 2
156	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 2	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1
157	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	0	-	-	$2k$	∓ 1	$\mp 2^{15}$	-
158	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	-
159	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k+1$	-	∓ 2	$\mp 2^{15}$	∓ 2
160	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{2})$	0	-	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 2
161	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2
162	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{3},\mathbf{2})$	1	∓ 2	$2k$	$2k+1$	∓ 2	-	∓ 2
163	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	0	∓ 2	-	$2k$	-	∓ 1	∓ 1
164	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{2})$	1	-	$2k+1$	$2k$	∓ 2	-	∓ 2
165	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{3})$	0	-	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	-
166	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	-	∓ 2	∓ 1	∓ 1
167	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k$	-	∓ 2	$\mp 2^{15}$	∓ 2
168	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1})$	0	$\mp 2^{15}$	-	$2k+1$	-	$\mp 2^{15}$	∓ 1
169	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{2})$	1	-	$2k$	$2k+1$	∓ 2	∓ 1	∓ 2
170	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	$\mp 2^{15}$	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	-
171	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	-	$2k$	∓ 1	-	∓ 2
172	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	1	$\mp 2^{15}$	-	$2k+1$	-	$\mp 2^{15}$	∓ 2
173	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2
174	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k$	$2k+1$	∓ 2	∓ 1	∓ 1
175	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	$2k$	∓ 2	∓ 1	∓ 2
176	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k+1$	$2k$	∓ 2	∓ 1	-
177	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	-	$2k+1$	$\mp 2^{15}$	-	∓ 2
178	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{2})$	0	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	-	∓ 2
179	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k$	-	∓ 2	∓ 1	∓ 1
180	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	1	∓ 2	$2k+1$	$2k$	∓ 2	-	-
181	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1})$	0	-	-	$2k+1$	-	-	∓ 2
182	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{3})$	0	∓ 2	$2k$	$2k$	∓ 2	-	-
183	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k$	$2k+1$	∓ 2	∓ 1	∓ 2
184	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	-
185	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{0})$	0	-	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1
186	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{2})$	0	-	$2k$	-	∓ 2	∓ 1	∓ 1
187	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 2	-	$2k+1$	-	∓ 1	-
188	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{2})$	1	-	$2k+1$	-	∓ 2	∓ 1	∓ 1
189	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0})$	1	-	-	$2k$	∓ 1	-	∓ 2
190	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0})$	$(\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 1	-	$2k$	-	$\mp 2^{15}$	∓ 2
191	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 2
192	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k$	∓ 1	$\mp 2^{15}$	∓ 1
193	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	-
194	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 1
195	$(\mathbf{0},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{0})$	0	-	-	$2k+1$	∓ 1	∓ 1	∓ 2
196	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1
197	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2
198	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k$	∓ 1	-	∓ 2

Table B.1 (cont'd)

	ϕ	ψ	ω	λ	z_1	z_2	z_3	z_4	z_5	z_6
199	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 2	-	$2k$	∓ 1	∓ 1	-
200	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	∓ 1	$2k$	$2k$	∓ 2	$\mp 2^{15}$	-
201	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{3},\mathbf{3},\mathbf{1},\mathbf{0})$	1	∓ 2	-	$2k+1$	$\mp 2^{15}$	-	∓ 1
202	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 2	-	$2k$	$\mp 2^{15}$	∓ 1	∓ 2
203	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	$\mp 2^{15}$	-	$2k+1$	$\mp 2^{15}$	-	∓ 2
204	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2
205	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	1	∓ 2	-	$2k$	$\mp 2^{15}$	-	∓ 2
206	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	1	∓ 2	-	$2k+1$	$\mp 2^{15}$	∓ 1	-
207	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{2})$	1	-	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
208	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	$\mp 2^{15}$	-	$2k+1$	∓ 1	$\mp 2^{15}$	-
209	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	1	∓ 2	-	$2k+1$	-	-	∓ 2
210	$(\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{2})$	0	-	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
211	$(\mathbf{0},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{3})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	0	-	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	-
212	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 2
213	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	∓ 1	-	$2k$	∓ 1	∓ 1	∓ 2
214	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	0	∓ 1	$2k$	-	∓ 2	∓ 1	-
215	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{2})$	0	-	$2k+1$	$2k$	∓ 2	∓ 1	∓ 2
216	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{0},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	0	∓ 2	-	$2k+1$	-	$\mp 2^{15}$	∓ 1
217	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 2
218	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k$	$2k+1$	∓ 2	∓ 1	∓ 2
219	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{2})$	1	-	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2
220	$(\mathbf{0},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{3},\mathbf{0},\mathbf{2},\mathbf{2})$	0	-	$2k$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2
221	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{0})$	1	∓ 1	-	$2k+1$	-	$\mp 2^{15}$	-
222	$(\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 1	-	$2k$	$\mp 2^{15}$	$\mp 2^{15}$	∓ 1
223	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{2})$	1	-	$2k$	$2k$	∓ 2	∓ 1	∓ 2
224	$(\mathbf{1},\mathbf{0},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{1})$	0	∓ 2	-	$2k+1$	∓ 1	$\mp 2^{15}$	-
225	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 1	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 2
226	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0})$	1	-	-	$2k$	-	$\mp 2^{15}$	-
227	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{0},\mathbf{3},\mathbf{3})$	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{0})$	0	∓ 1	-	$2k$	$\mp 2^{15}$	-	∓ 2
228	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{3})$	$(\mathbf{0},\mathbf{1},\mathbf{0},\mathbf{0})$	0	∓ 1	-	-	$\mp 2^{15}$	∓ 1	∓ 1
229	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{2})$	1	∓ 1	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	∓ 1
230	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{0},\mathbf{3},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{2},\mathbf{3})$	1	-	$2k+1$	$2k+1$	∓ 2	$\mp 2^{15}$	-
231	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{2},\mathbf{3},\mathbf{2})$	1	-	$2k+1$	$2k+1$	∓ 2	-	∓ 2
232	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{0})$	0	∓ 2	-	$2k+1$	∓ 1	∓ 1	∓ 1
233	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1},\mathbf{0},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{2})$	1	∓ 2	$2k$	$2k$	∓ 2	-	∓ 1
234	$(\mathbf{1},\mathbf{3},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{2},\mathbf{3},\mathbf{2},\mathbf{3})$	0	$\mp 2^{15}$	$2k$	$2k$	∓ 2	$\mp 2^{15}$	-
235	$(\mathbf{1},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{1},\mathbf{0},\mathbf{0},\mathbf{3})$	$(\mathbf{2},\mathbf{3},\mathbf{0},\mathbf{1})$	0	∓ 1	-	$2k+1$	$\mp 2^{15}$	$\mp 2^{15}$	-
236	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{3},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	0	∓ 2	$2k$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
237	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{2})$	1	∓ 2	$2k+1$	$2k$	∓ 2	$\mp 2^{15}$	∓ 1
238	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{0},\mathbf{0})$	$(\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1})$	$(\mathbf{1},\mathbf{1},\mathbf{3},\mathbf{3})$	0	∓ 1	$2k+1$	-	∓ 2	-	-
239	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{3},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	0	$\mp 2^{15}$	$2k$	$2k+1$	∓ 2	∓ 1	∓ 2
240	$(\mathbf{1},\mathbf{1},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{1},\mathbf{2},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{0},\mathbf{0})$	1	$\mp 2^{15}$	-	$2k$	∓ 1	∓ 1	∓ 2
241	$(\mathbf{1},\mathbf{2},\mathbf{2},\mathbf{1},\mathbf{1},\mathbf{1})$	$(\mathbf{3},\mathbf{2},\mathbf{3},\mathbf{1})$	$(\mathbf{0},\mathbf{3},\mathbf{2},\mathbf{2})$	1	$\mp 2^{15}$	$2k+1$	$2k+1$	∓ 2	∓ 1	∓ 2
242	$(\mathbf{1},\mathbf{3},\mathbf{0},\mathbf{1},\mathbf{1},\mathbf{0})$	$(\mathbf{3},\mathbf{2},\mathbf{0},\mathbf{1})$	$(\mathbf{0},\mathbf{1},\mathbf{2},\mathbf{3})$	0	$\mp 2^{15}$	$2k$	-	∓ 2	∓ 1	-

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name:	Yıldırım, Hamdi Murat
Nationality:	Turkish (TC)
Date and Place of Birth:	26 March 1975, Ankara
Marital Status:	Married
Phone:	+90 543 844 00 55
email:	hmurat@bilkent.edu.tr

EDUCATION

Degree	**Institution**	**Year of Graduation**
M.S.	METU Information Systems	2002
M.S.	METU Mathematics	2000
B.Sc.	METU Mathematics	1997
High School	Bahçelievler Cumhuriyet Lisesi, Ankara	1992

WORK EXPERIENCE

Year	**Place**	**Enrollment**
2005- Present	Bilkent Univ. Dept. of CTIS	Instructor
1998-2005	METU Department of Mathematics	Research Assistant

PUBLICATIONS

H. M. Yıldırım, Nonlinearity Properties of the Mixing Operations of the Block Cipher IDEA, Lecture Notes in Computer Science 2904, pp. 68-81, Springer-Verlag, 2003.

HOBBIES

Computer Technologies, Bicycling, Basketball, Music