Differential-Linear Weak Key Classes of IDEA

Philip Hawkes[1]

Department of Mathematics, University of Queensland, Brisbane, Australia.
pmh@maths.uq.edu.au

Abstract. Large weak key classes of IDEA are found for which membership is tested with a differential-linear test while encrypting with a single key. In particular, one in every 2^{65} keys for 8.5-round IDEA is weak. A related-key differential-linear attack on 4-round IDEA is presented which is successful for all keys. Large weak key classes are found for 4.5- to 6.5-round and 8-round IDEA for which membership of these classes is tested using similar related-key differential-linear tests.

Key words: IDEA, differential-linear cryptanalysis, related-key cryptanalysis, weak keys.

1 Introduction

The International Data Encryption Algorithm (IDEA) [14] is a 64-bit block cipher using a 128-bit key. IDEA consists of eight rounds of encryption (referred to as *full rounds*) followed by an *output transformation*. For this reason IDEA is said to be an 8.5-round cipher, and on occasion when the output transformation is omitted for the sake of analysis, we refer to the cipher as 8-round IDEA. Further, when the number of rounds is reduced to say 4 rounds, the resulting cipher is referred to as 4.5-round and 4-round IDEA depending on whether the output transformation is included or not.

The full 8.5-round version of IDEA is considered to be practically secure against differential cryptanalysis [2, 14] (see [13, 17, 12, 5]), linear cryptanalysis [16] (see [9]) and various generalizations of linear cryptanalysis (see [8, 10]). A related-key attack on 8.5-round IDEA has been proposed [11], although this attack utilized a weakness in the implementation rather than the algorithm. Successful attacks exist against IDEA with a reduced number of rounds. These attacks include: differential attacks against 2.5-round IDEA [17, 6]; a differential-linear cryptanalysis [4, 5] against 3-round IDEA; and a truncated differential attack against 3.5-round IDEA [12, 5]. The results obtained in this paper are extensions of the two following attacks.

A *weak key class* is a set of session keys for which membership can be determined with a relatively small workload. Daemen, Govaerts and Vandewalle [7] found two weak key classes of 8.5-round IDEA. In the first weak key class, consisting of 2^{23} session keys, membership is tested by confirming that a certain linear approximation holds with probability one, while in the second weak key class, consisting of 2^{51} session keys, membership is tested by confirming that a certain differential approximation holds with probability one. This work is extended in this paper by finding weak key classes for which membership is tested by confirming that a differential-linear approximation holds with probability one. These weak key classes are significantly larger than those found in [7]. In particular, the full 8.5-round IDEA has a weak key class containing 2^{63} session keys. Testing membership of this weak key class requires an average of 19.5 plaintexts. If the session key is weak, then the membership test recovers 72 bits of the session key.

In a *related-key attack* [1, 11] the attacker obtains the encryption of certain plaintext not only under the original session key K, which is unknown, but also under some other associated session keys $K' = f(K)$. Kelsey, Schneier and Wagner [11] found a related-key attack on 3.5-round IDEA using six chosen plaintexts encrypted under two related-keys. In this paper we extend this attack to a related-key differential-linear attack on 4-round IDEA which recovers 15 bits of information about the session key using an average of 38.3 chosen plaintexts encrypted under two related-keys. This is the first known attack on 4-round IDEA which is successful for all session keys. Every session key of the 4-round version of IDEA is susceptible to a related-key differential-linear attack. The attack is based on a related-key differential-linear approximation which holds with probability one for all session keys. A similar approach is used to detect membership of large weak key classes of IDEA with more rounds.

No feasible attacks have been proposed to attack IDEA with more than 3.5-rounds, so we focus our attention on IDEA with 4 or more rounds. Using the two methods above, we determine the largest known weak key classes of R-round and R.5-round IDEA, $4 \leq R \leq 8$. Table 1 provides a summary of the size of the weak key classes and the data complexity of the corresponding membership tests. Note that all session keys are weak keys for the related-key differential-linear attack on 4-round IDEA. Membership of the weak key classes of IDEA with between 4.5 and 6.5 rounds is tested by confirming that a related-key differential-linear approximation holds with probability one, as is membership of the weak key class of 8-round IDEA. Membership of the the remaining weak key classes is tested by confirming that a differential-linear approximation holds with probability one while encrypting with a single key.

R	4	4.5	5	5.5	6	6.5	7	7.5	8	8.5
Size ($\log_2$)	128	113	106	98	91	84	80	75	70	63
Av. Data Comp.	38.4	19.5	38.4	38.4	$2^{13.2}$	613	14.8	31.2	$2^{19.3}$	19.5

Table 1. Summary of the size ($\log_2$) of the weak key classes of R-round and R.5-round IDEA, $4 \leq R \leq 8$, and the average data complexities of the corresponding membership tests.

We begin introducing notation in §2. In §3 we construct differential-linear approximations which hold with probability one for a subset of the session keys. Weak key classes of R-round and R.5-round IDEA, $4 \leq R \leq 8$, are determined for which there is a differential-linear approximation of probability one. In §3.1 we describe an attack for testing membership of these weak key classes. In §4 we describe attacks which exploit related-key differential-linear approximations of probability one. The encryption process and key schedule of IDEA, and some results of Daemen, Govaerts and Vandewalle [7] are given in the Appendix.

2 Notation

IDEA is constructed from three group operations acting on 16-bit *subblocks*. These group operations are: bitwise exclusive-OR (XOR), denoted by $\oplus$; addition modulo 2^{16}, denoted by $\boxplus$; and multiplication modulo $2^{16}+1$ with the subblock $0\ldots0 \equiv 2^{16}$, denoted by $\odot$. The computation graph of the encryption process of IDEA is shown in Figure 2 in the Appendix. The full round function of IDEA consists of two "layers". The first layer is called the *key combining stage*, while the second layer contains the *multiplication-addition (MA) structure*. The 16-bit *subkeys* are determined from the session key as shown in Table 5, in the Appendix. Due to the subblock nature of the cipher, the input to the r-th round (and the output of the $(r-1)$-st round) is denoted $C^{(r)} = C_1^{(r)}C_2^{(r)}C_3^{(r)}C_4^{(r)}$.

For each plaintext P let $P^{[K]}$ denote P encrypted by the first key combining stage under the session key K. Also let C denote the encryption of P under the session key K, and $C^{[K]}$ denote the ciphertext C decrypted by one layer under the session key K. (By one layer, the author means either the output transformation, if encrypting with R.5-round IDEA, or the MA structure in the last round, if encrypting with R-round IDEA.)

For $A \in \mathbb{Z}_2^m$, $m \geq 1$, let $A[i]$ represent the bit in position i of A, $0 \leq i \leq m-1$. Linear approximations between the input and output of the $r-$th round are represented by $\alpha^{(r)} \cdot C^{(r)} + \alpha^{(r+1)} \cdot C^{(r+1)} = \gamma_r$, where $\alpha^{(r)}, \alpha^{(r+1)} \in \mathbb{Z}_2^{64}$, $\gamma_r \in \{0,1\}$ and $\alpha^{(r)} \cdot C^{(r)} = \sum_{i=0}^{63} \alpha^{(r)}[i]C^{(r)}[i]$ (mod 2) is the binary inner product. The value $\alpha^{(r)}$ is known as the *mask* for $C^{(r)}$. Note that in any linear relation in this paper, addition is assumed to be modulo two. Due to the subblock nature of the cipher we often write masks for linear approximations in terms of subblocks, e.g. $\alpha^{(r)} = (\alpha_1^{(r)}, \alpha_2^{(r)}, \alpha_3^{(r)}, \alpha_4^{(r)})$. All differences in this paper are of the form $\Delta A = A \oplus A^*$, and we denote the 16-bit difference $10\ldots0 = 2^{15}$ by ν. Differences for differential characteristics are also written in terms of subblocks, e.g. $\delta^{(r)} = [\delta_1^{(r)}, \delta_2^{(r)}, \delta_3^{(r)}, \delta_4^{(r)}]$. Round brackets ( ) are used for masks, to distinguish these values from differences which use square brackets [ ].

3 Constructing Differential-Linear Approximations of Probability One

A *differential-linear approximation (DL-approximation)* is denoted by a triple $(\delta, \alpha, \epsilon)$ where $\delta, \alpha \in \mathbb{Z}_2^n \setminus \{0\}$ and $\epsilon \in \{0,1\}$, and the DL-approximation predicts that there exist plaintext pairs P, P^* such that $P^{[K]} \oplus P^{[K]*} = \delta$ and $\alpha \cdot C^{[K]} + \alpha \cdot C^{[K]*} = \epsilon$. The probability of the DL-approximation is defined as

$$\Pr(\alpha \cdot C^{[K]} + \alpha \cdot C^{[K]*} = \epsilon \mid P^{[K]} \oplus P^{[K]*} = \delta).$$

A ***differential-linear weak (DL-weak) key class*** $\mathcal{W}$ is a set of session keys for which some associated DL-approximation $(\delta, \alpha, \epsilon)$ holds with probability one. The one-round differential and linear approximations given in the Appendix can be used to construct DL-approximations $(\delta, \alpha, \epsilon)$ which hold with probability one for large DL-weak key classes, as shown in the following example.

Example 1. Let $\mathcal{W}$ consist of all session keys for which the 65-bit positions 0-18, 29-71 and 123-127 are zero. These positions are known as the ***weak bit positions.*** Consider 8.5-round IDEA. We show below that if the session key $K \in \mathcal{W}$ then the DL-approximation $(\delta, \alpha, \epsilon) = ([0, \nu, 0, \nu], (1, 1, 0, 0), 0)$ holds with probability one. Figure 1 shows how this DL-approximation is constructed.

First note that $\Delta P^{[K]} = [0, \nu, 0, \nu] \Rightarrow \Delta C^{(2)} = [0, 0, \nu, \nu]$ with probability one, due to the structure of IDEA. If $K \in \mathcal{W}$ then the subkeys $Z_4^{(2)}$, $Z_5^{(2)}$, $Z_5^{(3)}$, and $Z_4^{(4)}$ are either zero or one. Consequently, each of the following characteristics holds with probability one, as the appropriate subkeys are either zero or one:

$$\begin{aligned}
\Delta P^{[K]} &= [0, \nu, 0, \nu] \Rightarrow \Delta C^{(2)} = [0, 0, \nu, \nu], \text{for all subkeys;}\\
\Delta C^{(2)} &= [0, 0, \nu, \nu] \Rightarrow \Delta C^{(3)} = [0, \nu, \nu, 0], \text{ as } Z_4^{(2)}, Z_5^{(2)} \in \{0, 1\};\\
\Delta C^{(3)} &= [0, \nu, \nu, 0] \Rightarrow \Delta C^{(4)} = [0, \nu, 0, \nu], \text{ as } Z_5^{(3)} \in \{0, 1\};\\
\Delta C^{(4)} &= [0, \nu, 0, \nu] \Rightarrow \Delta C^{(5)} = [0, 0, \nu, \nu], \text{ as } Z_4^{(4)} \in \{0, 1\}.
\end{aligned}$$

These one-round differential characteristics are concatenated to form a 4-round differential characteristic $\Delta P^{[K]} = [0, \nu, 0, \nu] \Rightarrow \Delta C^{(5)} = [0, 0, \nu, \nu]$, which holds with probability one for all $K \in \mathcal{W}$. Note that $\Delta C^{(5)} = [0, 0, \nu, \nu] \Rightarrow \Delta C_1^{(6)} \oplus \Delta C_2^{(6)} = \nu$ with probability one, due to the structure of the round function. Therefore, if $K \in \mathcal{W}$, then

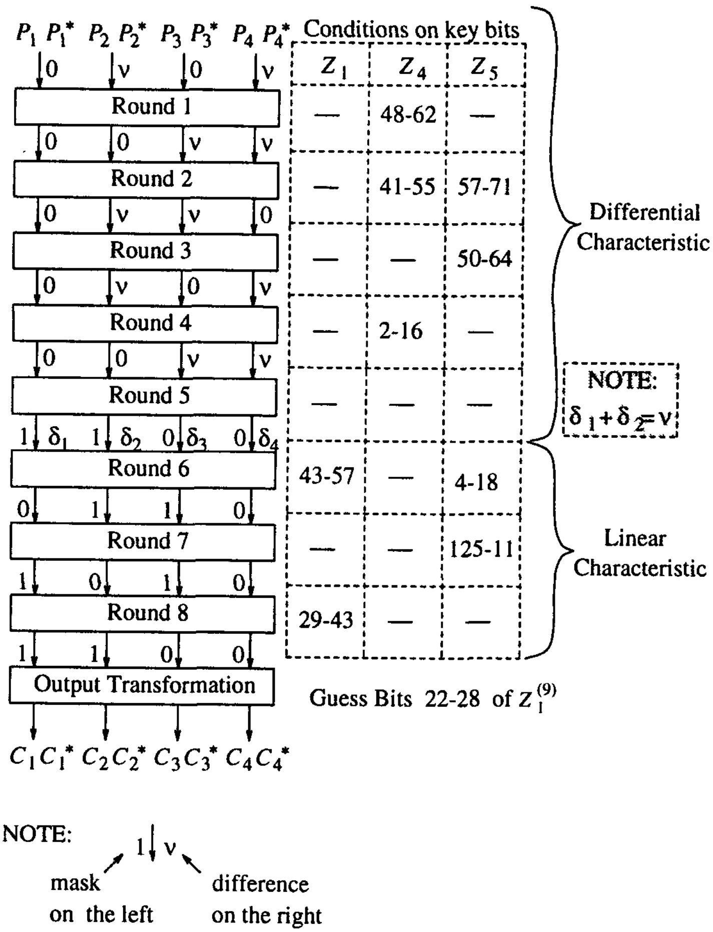
$$\Delta P^{[K]} = [0, \nu, 0, \nu] \Rightarrow \Delta C_1^{(6)} \oplus \Delta C_2^{(6)} = \nu. \tag{1}$$

If $K \in \mathcal{W}$, then the subkeys $Z_1^{(6)}$, $Z_5^{(6)}$, $Z_5^{(7)}$ and $Z_1^{(8)}$ are also either zero or one. Thus, following from the results in the Appendix, the one-round linear characteristics

$$\begin{aligned}
1 \cdot C_1^{(6)} + 1 \cdot C_2^{(6)} + 1 \cdot C_2^{(7)} + 1 \cdot C_3^{(7)} = \gamma_6 &= 1 \cdot Z_1^{(6)} + 1 \cdot Z_2^{(6)} + 1 \cdot Z_5^{(6)},\\
1 \cdot C_2^{(7)} + 1 \cdot C_3^{(7)} + 1 \cdot C_1^{(8)} + 1 \cdot C_3^{(8)} = \gamma_7 &= 1 \cdot Z_2^{(7)} + 1 \cdot Z_3^{(7)} + 1 \cdot Z_5^{(7)} + 1,\\
1 \cdot C_1^{(8)} + 1 \cdot C_3^{(8)} + 1 \cdot C_1^{(9)} + 1 \cdot C_2^{(9)} = \gamma_8 &= 1 \cdot Z_1^{(8)} + 1 \cdot Z_3^{(8)} + 1,
\end{aligned}$$

hold with probability one. These one-round linear characteristics are concatenated to form the linear characteristic

$$1 \cdot C_1^{(6)} + 1 \cdot C_2^{(6)} + 1 \cdot C_1^{(9)} + 1 \cdot C_2^{(9)} = \gamma_K = \sum_{i=6}^{8} \gamma_i, \tag{2}$$


P_1 P_1^* P_2 P_2^* P_3 P_3^* P_4 P_4^*
0 v 0 v
Round 1
0 0 v v
Round 2
0 v v 0
Round 3
0 v 0 v
Round 4
0 0 v v
Round 5
1 δ_1 1 δ_2 0 δ_3 0 δ_4
Round 6
0 1 1 0
Round 7
1 0 1 0
Round 8
1 1 0 0
Output Transformation
$C_1C_1^*$ $C_2C_2^*$ $C_3C_3^*$ $C_4C_4^*$
Conditions on key bits
Differential Characteristic
NOTE: $\delta_1+\delta_2=v$
Linear Characteristic
Guess Bits 22-28 of $Z_1^{(9)}$
NOTE:
1 v
mask on the left
difference on the right

Z_1	Z_4	Z_5
—	48-62	—
—	41-55	57-71
—	—	50-64
—	2-16	—
—	—	—
43-57	—	4-18
—	—	125-11
29-43	—	—

Fig. 1. The DL-approximation $(\delta, \alpha, \epsilon) = ([0, \nu, 0, \nu], (1, 1, 0, 0), 0)$ for 8.5-round IDEA which holds with probability one and the corresponding conditions on the session key bits. The bits 22-28 of the subkey $Z_1^{(9)}$ in the last round are guessed.

which holds with probability one whenever $K \in \mathcal{W}$. Combining (1) and the linear relation (2), we see that if $P^{[K]} \oplus P^{[K]*} = [0, \nu, 0, \nu]$ then

$$\begin{aligned} &1 \cdot C_1^{(9)} + 1 \cdot C_2^{(9)} + 1 \cdot C_1^{(9)*} + 1 \cdot C_2^{(9)*} \\ &= 1 \cdot C_1^{(6)} + 1 \cdot C_2^{(6)} + 1 \cdot C_1^{(6)*} + 1 \cdot C_2^{(6)*} \;=\; 1 \cdot (\Delta C_1^{(6)} \oplus \Delta C_2^{(6)}) = 1 \cdot \nu = 0, \end{aligned}$$

whenever the $K \in \mathcal{W}$. That is, whenever the session key $K \in \mathcal{W}$, the DL-approximation $(\delta, \alpha, \epsilon) = ([0, \nu, 0, \nu], (1, 1, 0, 0), 0)$ holds with probability one. □

To test if a DL-approximation $(\delta, \alpha, \epsilon)$ holds with probability one, the attacker must guess enough information about the subkeys in the first round to obtain pairs P and P^* for which $\Delta P^{[K]} = \delta$, and enough information about the subkeys in the last round to determine $\alpha \cdot C^{[K]} + \alpha \cdot C^{[K]*}$ from the corresponding ciphertexts C and C^*.

Example 2. Consider the DL-approximation $(\delta, \alpha, \epsilon) = ([0, \nu, 0, \nu], (1, 1, 0, 0), 0)$ and the associated DL-weak key class $\mathcal{W}$ discussed in Example 1. Note that $Z_4^{(1)} = 0$ whenever $K \in \mathcal{W}$, and therefore $\Delta P_i^{[K]} = \nu$ if and only if $\Delta P_i = \nu$, $i \in \{2, 4\}$, (see the Appendix). Thus, if $K \in \mathcal{W}$, then $\Delta P^{[K]} = [0, \nu, 0, \nu]$ if and only $\Delta P = [0, \nu, 0, \nu]$. To determine if the DL-approximation holds with probability one, the attacker must obtain the encryptions of plaintext pairs P, P^* for which $P \oplus P^* = [0, \nu, 0, \nu]$ and then determine whether $1 \cdot C_1^{[K]} + 1 \cdot C_2^{[K]} + 1 \cdot C_1^{[K]*} + 1 \cdot C_2^{[K]*} = 0$, from the corresponding ciphertext pairs. The attacker can obtain $1 \cdot C_2^{[K]} + 1 \cdot C_2^{[K]*}$ from $1 \cdot C_2^{[K]} + 1 \cdot C_2^{[K]*} = 1 \cdot C_3 + 1 \cdot C_3^*$. However, to obtain $1 \cdot C_1^{[K]} + 1 \cdot C_1^{[K]*}$, the attacker needs to determine the value of $Z_1^{(9)}$, and from this calculate $C_1^{[K]} = C_1 \odot (Z_1^{(9)})^{-1}$. We call a value Z^* a *candidate for the value of* $Z_1^{(9)}$ if it is a possible value for $Z_1^{(9)}$ when $K \in \mathcal{W}$. Note that $Z_1^{(9)}$ consists of the bits in positions 22-37 of K, and if $K \in \mathcal{W}$ then the 9 least significant bits (LSBs) of $Z_1^{(9)}$ are zero, and there are $2^7 = 128$ candidates for the value of $Z_1^{(9)}$. For each candidate Z^* the attacker tests to see if

$$1 \cdot (C_1 \odot (Z^*)^{-1}) + 1 \cdot C_3 + 1 \cdot (C_1^* \odot (Z^*)^{-1}) + 1 \cdot C_3^* = 0, \tag{3}$$

whenever $\Delta P = [0, \nu, 0, \nu]$. If (3) holds for the ciphertext pair C, C^*, then C, C^* is said to be a *DL-right pair for* Z^*. Therefore, if the session key $K \in \mathcal{W}$, and $Z^* = Z_1^{(9)}$, then all ciphertext pairs will be DL-right pairs for Z^* when $\Delta P = [0, \nu, 0, \nu]$.[1]

The attacker can compute a table beforehand to avoid calculating (3) explicitly for each ciphertext pair and candidate Z^*. For each $C_1 \in \mathbb{Z}_2^{16}$ the attacker computes the 128-bit vector $\mathbf{A}_{C_1}$ where for $0 \leq i \leq 127$, $\mathbf{A}_{C_1}[i] = 1 \cdot (C_1 \odot (Z^*)^{-1})$ where $Z^* = i \cdot 2^9$. The vector $\mathbf{A}_{C_1}$ contains the possible values of $1 \cdot (C_1 \odot (Z^*)^{-1})$ for every candidate Z^*. The 2^{16} vectors $\mathbf{A}_{C_1}$ are stored in a table which is 1 megabyte in size. For each ciphertext pair C, C^* the attacker calculates the 128-bit vector $\mathbf{B}$ with $\mathbf{B}[i] = 1 + 1 \cdot (C_3 \oplus C_3^*)$ for $0 \leq i \leq 127$, and determines the 128-bit vector $\mathbf{V} = \mathbf{A}_{C_1} \oplus \mathbf{A}_{C_1^*} \oplus \mathbf{B}$. For $0 \leq i \leq 127$, $\mathbf{V}[i] = 1$ if and only if (3) holds for $Z^* = i \cdot 2^9$. Hence, determining $\mathbf{V}$ is equivalent to determining if (3) holds or not for every candidate for the value of $Z_1^{(9)}$. □

[1] *Remark.* Some session keys in this DL-weak key class are also members of a weak key class for which the differential characteristic $\Delta P = [0, \nu, 0, \nu] \Rightarrow \Delta C^{(10)} = [0, \nu, \nu, 0]$ holds with probability one. As $C_1 = C_1^*$ for all ciphertext pairs, all ciphertext pairs will be DL-right pairs for every value of $Z_1^{(9)}$, and the value of $Z_1^{(9)}$ cannot be determined. A simple method to avoid this situation is to first test for membership of weak key classes for which a differential characteristic holds with probability one.

In Example 2, the subkey $Z_4^{(1)}$ is fixed to zero for all $K \in \mathcal{W}$. However, this is not always the case. For example, to obtain pairs for P and P^* for which $\Delta P^{[K]} = \delta = [0, 0, \nu, \nu]$, the attacker may be required to guess the value of $Z_4^{(1)}$. For each candidate Z for the value of $Z_4^{(1)}$, the attacker determines a pair $P_4(Z), P_4^*(Z)$ for which $(P_4(Z) \odot Z) \oplus (P_4^*(Z) \odot Z) = \nu$. To increase the speed of the attack, these pairs are computed beforehand and stored in a table. The size of the table depends on the number of candidates, and would be at most 256 kilobytes in size. The attacker obtains the encryptions of plaintexts P and P^* for which $\Delta P_1 = \Delta P_2 = 0$, $\Delta P_3 = \nu$, $P_4 = P_4(Z)$ and $P_4^* = P_4^*(Z)$. Such a plaintext pair is called a *δ-pair for Z*. The attacker then tests each candidate Z^* for the value of the subkey in the last round to see if the corresponding ciphertext pairs are DL-right pairs for Z^*.

3.1 Testing Membership

Consider a DL-approximation $(\delta, \alpha, \epsilon)$ for which the corresponding DL-weak key class $\mathcal{W}$ has b weak bit positions (so there are 2^{128-b} DL-weak keys in this class). Suppose that t_1 bits of a subkey in the first round and t_2 bits of a subkey in the last round are guessed. Let Z and Z^* be candidates for the values of the subkeys in the first and last rounds respectively.

It can be shown that if C, C^* is a DL-right pair for Z^* then C, C^* is also a DL-right pair for $(0 \odot Z^*)$. If both values are candidates, then the attacker need only test one of these values. However, as $0 \odot Z^* = \overline{Z^*} \boxplus 2$ it follows that only one of Z^* and $0 \odot Z^*$ has the LSB equal to zero. In Example 2, the 9 LSB's of $Z_1^{(9)}$ are zero, and thus there is only one value of Z^* and $0 \odot Z^*$ which is a candidate for the value of $Z_1^{(9)}$. However, if all 16 bits of a subkey in the last round are guessed, then the attacker needs only test one candidate out of Z^* and $0 \odot Z^*$. Thus, only 2^{15} candidates Z^* are tested, and we assume, for the purposes of calculating the data complexity, that $t_2 = 15$. Similarly, if C, C^* is δ-pair for Z then C, C^* is also a δ-pair for $(0 \odot Z)$. Thus, if $t_1 = 16$, we reduce this to $t_1 = 15$. A candidate, for example Z, is said to be *consistent with K* if either Z or $0 \odot Z$ is the correct value of the subkey in the first round, otherwise it is *inconsistent.*

If $K \in \mathcal{W}$ and both candidates Z and Z^* are consistent with K, then the triple (K, Z, Z^*) is said to be *complete*, otherwise it is *incomplete.* The aim of a *differential-linear weak key (DL-weak key) membership test* is to either find a complete triple (K, Z, Z^*) (thus showing $K \in \mathcal{W}$ and determining the values of the subkeys guessed), or show that for all candidates Z and Z^*, the triples (K, Z, Z^*) are incomplete (thus showing $K \notin \mathcal{W}$). If the triple (K, Z, Z^*) is complete then for every δ-pair for Z, the corresponding ciphertext pair is a DL-right pair for Z^*. However, for each incomplete triple (K, Z, Z^*) there are many δ-pairs for Z for which the corresponding ciphertext pairs are not DL-right pairs for Z^*. A *DL-test* on the triple (K, Z, Z^*) consists of obtaining the encryptions of a δ-pair for Z, and determining if the corresponding ciphertext pair is a DL-right pair for Z^*. If the corresponding ciphertext pair is a DL-right pair for Z^*, then the triple *passes the DL-test* for that plaintext pair, otherwise the triple *fails*. A triple (K, Z, Z^*) can be shown to be incomplete by failing just one DL-test. We can show that if the triple (K, Z, Z^*) passes each of $1.18(b+t_1+t_2+8)$ DL-tests then $\Pr((K, Z, Z^*)$ is complete$) > 1-2^{-8} = 99.6\%$. The value $1.18(b+t_1+t_2+8)$ is called the *weak key bound*, denoted β, for a DL-weak key membership test. If a triple passes each of β DL-tests then the triple (K, Z, Z^*) is assumed to be complete and $K \in \mathcal{W}$. A DL-weak key membership test on a DL-weak key class proceeds as follows.

Differential-Linear Weak Key Membership Test

Step 1. Let Z be a candidate for the value of the subkey guessed in the first round.
Step 2. Conduct DL-tests on the triples (K, Z, Z^*) for every candidate Z^* for the value of the subkey guessed in the last round until either every triple fails a DL-test, or a triple (K, Z, Z^*) passes each of β DL-tests.
Step 3. If all triples using candidate Z fail a DL-test, then try another candidate for the value of the subkey guessed in the first round and return to Step 2. Otherwise, the triple (K, Z, Z^*) which passed all β DL-tests is assumed to be complete, and $K \in \mathcal{W}$, and the subkey guessed in the first round (last round) is either Z or $0 \odot Z$ (Z^* or $0 \odot Z^*$). □

Example 3. Recall from Example 2 that there is only one candidate $Z_1^{(4)} = 0$ in the first round for the DL-weak key class $\mathcal{W}$ in Example 1. The corresponding DL-weak key membership test consists of conducting DL-tests on the triples $(K, 0, Z^*)$ where Z^* has the 9 LSB's equal to zero. The vectors $\mathbf{V}$ defined in Example 2 are used to simultaneously conduct DL-tests on the triples $(K, 0, Z^*)$ for all candidates Z^*. The attacker sets every bit of a 128-bit vector $\mathbf{X}$ to one, and for each ciphertext pair the attacker determines $\mathbf{V}$ and updates $\mathbf{X} = \mathbf{V} \wedge \mathbf{X}$ where $\wedge$ denotes the bitwise AND operation. After testing $\beta = 1.18(65+0+7+8) = 95$ pairs, if $\mathbf{X}[i] = 1$, then the triple $(K, 0, i \cdot 2^9)$ passes the DL-test for all ciphertext pairs tested. If there is only one such value i, then $K \in \mathcal{W}$, $Z_1^{(9)} = i \cdot 2^9$ and the attacker has recovered $65 + 7 = 72$ bits of the session key. If there is more than one value of i, which is unlikely to occur, then the attacker can continue conducting DL-tests to eliminate the incomplete triples. If $\mathbf{X} = 0$, then for each candidates Z^*, the triple $(K, 0, Z^*)$ fails at least one DL-test and $K \notin \mathcal{W}$. □

If a triple (K, Z, Z^*) is complete, then the DL-weak key membership test will require β δ-pairs for Z, which corresponds to 2β encryptions. We can show that for each candidate Z, an average of E_{t_2} δ-pairs for Z are required before each incomplete triple (K, Z, Z^*) fails a DL-test, where E_{t_2}, $0 \leq t_2 \leq 15$, is given in Table 2. If $K \notin \mathcal{W}$, then all candidates Z must be tested. Therefore, a total of $2^{t_1} E_{t_2}$ plaintext pairs or $2^{t_1+1} E_{t_2}$ encryptions on average are required to show that each incomplete triple fails a DL-test, and thus $K \notin \mathcal{W}$. As most session keys are not DL-weak, this then is the average data complexity of the DL-weak key membership test. For example, the average data complexity of the membership test described in Example 3 is $E_7 = 9.74$ pairs, which corresponds to

t_2	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
E_{t_2}	2.25	3.05	4.04	5.12	6.23	7.40	8.57	9.74	10.9	12.1	13.3	14.5	15.6	16.8	18.0	19.2

Table 2. The value of E_{t_2}, $0 \leq t_2 \leq 15$.

19.5 encryptions. The use of precomputed tables reduces the process complexity during a membership test to at most three table look-ups for each plaintext pair tested. Table 3 contains the details for the largest DL-weak key classes for R-round and R.5-round IDEA, $4 \leq R \leq 8$. DL-weak key classes can also be found using the decryption key schedule. These DL-weak key classes have been found to offer no increase in size over the DL-weak key classes using the encryption key schedule.

R	δ	α	b	Weak Bit Positions	Bits Guessed		β	Av. Data Comp.
					First Round	Last Round		
4	D_1	$(1,1,0,0)$	29	50-78	48-49	-	18	18
4.5	D_2	$(1,0,1,0)$	31	41-71	-	75-90	64	38.4
5	D_1	$(1,0,1,0)$	44	50-71, 75-96	48-49	-	64	18
5.5	D_2	$(1,0,1,0)$	46	2-16, 41-71	-	-	64	4.5
6	D_2	$(0,1,1,0)$	46	2-16, 41-71	-	17-18	67	8.1
6.5	D_2	$(0,1,1,0)$	48	2-18, 41-71	-	-	67	4.5
7	D_2	$(1,1,0,0)$	48	2-18, 41-71	-	0-1, 125-127	72	14.8
7.5	D_2	$(1,1,0,0)$	53	0-18, 41-71, 125-127	-	29-40	87	31.2
8	D_2	$(1,1,0,0)$	62	0-25, 41-71, 123-127	-	93-108	101	38.4
8.5	D_2	$(1,1,0,0)$	65	0-18, 29-71, 125-127	-	22-28	95	19.5

Table 3. DL-weak key classes of R-round and R.5-round IDEA, $4 \leq R \leq 8$. The corresponding differential-linear approximations are of the form $(\delta, \alpha, \epsilon)$ where $\delta \in \{D_1 = [0,0,\nu,\nu], D_2 = [0,\nu,0,\nu]\}$ is given in the second column, α is given in the third column and $\epsilon = 0$.

4 Related-Key Differential-Linear Attacks

The membership tests presented in §3 are based on testing pairs of plaintexts which have been encrypted under the same session key. The membership tests presented in the current section are different in that the plaintext pairs P, P^* are encrypted under two *related-keys* K and K' which differ in a certain bit position. Otherwise, the concept is identical. The plaintext pairs are chosen to cancel out the differences in the subkeys in the first round, so that after a few rounds of encryption, some corresponding intermediate ciphertext subblocks are the same. The attacker then tests if linear approximation between $C^{[K]}$ and $C^{[K']*}$ holds by guessing the value of a subkey in the last round.

This approach is used to develop the first known attack on 4-round IDEA which is successful for all session keys. The attack is an extension of the related-key attack on 3.5-round IDEA found by Kelsey, Schneier and Wagner [11]. Large weak key classes of IDEA with more than four rounds are found for which membership is checked using a similar technique. The membership tests are based on testing if related-key differential-linear approximations hold with probability one. A *related-key differential-linear approximation (RKDL-approximation)* is denoted by a triple $(k_\Delta, \alpha, \epsilon)$ where $0 \leq k_\Delta \leq 127$, $\alpha \in \mathbb{Z}_2^n \setminus \{0\}$ and $\epsilon \in \{0,1\}$, and the RKDL-approximation predicts that there exist plaintext pairs P, P^* such that $P^{[K]} = P^{[K']*}$ and $\alpha \cdot C^{[K]} + \alpha \cdot C^{[K']*} = 0$, where K and K' differ in bit position k_Δ. Note that P is encrypted to C under K and P^* is encrypted to C^* under K'. The probability of the RKDL-approximation is defined as

$$\Pr(\alpha \cdot C^{[K]} + \alpha \cdot C^{[K']*} = \epsilon \mid P^{[K]} = P^{[K']*}),$$

where K' differs from K in bit position k_Δ. A *related-key differential-linear weak (RKDL-weak) key class* $\mathcal{W}$ is a set of session keys for which some associated RKDL-approximation $(k_\Delta, \alpha, \epsilon)$ holds with probability one. In the following example we construct a RKDL-approximation for 4-round IDEA which holds with probability one for all session keys. Thus, all session keys are RKDL-weak keys of 4-round IDEA.

Example 4. Consider 4-round IDEA. Suppose that K and K' are two session keys which differ in bit position 16. Let $Z_i^{(r)}$ and $Z_i^{(r)*}$, $1 \leq i \leq 6$, $1 \leq r \leq 4$, denote the subkeys generated from the keys K and K' respectively. Observe that $Z_i^{(r)} = Z_i^{(r)*}$, $1 \leq i \leq 6$, $1 \leq r \leq 4$ with the exceptions being $Z_2^{(1)} = Z_2^{(1)*} \oplus \nu$, $Z_4^{(3)} = Z_4^{(3)*} \oplus 2^8$ and $Z_4^{(4)} = Z_4^{(4)*} \oplus 2$. If $P^{[K]} = P^{[K']*}$, then $C^{(2)} = C^{(2)*}$, $C^{(3)} = C^{(3)*}$ and

$$\begin{aligned}
&1 \cdot C_2^{[K]} + 1 \cdot C_3^{[K]} + 1 \cdot C_2^{[K']*} + 1 \cdot C_3^{[K']*} \\
&\quad = 1 \cdot (C_2^{(3)} \boxplus Z_2^{(3)}) + 1 \cdot (C_3^{(3)} \boxplus Z_3^{(3)}) + 1 \cdot (C_2^{(3)*} \boxplus Z_2^{(3)*}) + 1 \cdot (C_3^{(3)*} \boxplus Z_3^{(3)*}) \\
&\qquad\quad + 1 \cdot \Big(\big((C_1^{(3)} \odot Z_1^{(3)}) \oplus (C_2^{(3)} \boxplus Z_2^{(3)})\big) \odot Z_5^{(3)}\Big) \\
&\qquad\quad + 1 \cdot \Big(\big((C_1^{(3)*} \odot Z_1^{(3)*}) \oplus (C_2^{(3)*} \boxplus Z_2^{(3)*})\big) \odot Z_5^{(3)*}\Big) \;=\; 0.
\end{aligned}$$

Therefore, the RKDL-approximation $(k_\Delta, \alpha, \epsilon) = (16, (0,1,1,0), 0)$ holds with probability one for all session keys. That is, all session keys are RKDL-weak keys. □

RKDL-weak key classes of IDEA with more rounds contain session keys for which certain subkeys are either zero or one, so that appropriate linear approximations hold with probability one, as with DL-weak key classes. These RKDL-weak key classes are exploited using a *related-key differential-linear weak key*

(RKDL-weak key) membership test. As with a DL-weak key membership test, the aim of a RKDL-weak key membership test is to either find a complete triple (K, Z, Z^*) (thus showing $K \in \mathcal{W}$ and determining the values of the subkeys guessed), or show that for all candidates Z and Z^*, the triples (K, Z, Z^*) are incomplete (thus showing $K \notin \mathcal{W}$). The attack on 4-round IDEA only determines the value of the guessed subkey, as all session keys are already known to be RKDL-weak.

Let Z and Z^* be candidates for the values of the subkeys guessed in the first and last rounds respectively when encrypting under K. A *k_Δ-pair for Z* is a pair of plaintexts P, P^* such that if Z is consistent with K, then $P^{[K]} = P^{[K']*}$. For example, if $k_\Delta = 0$ then $Z_1^{(1)*} = \nu \oplus Z_1^{(1)}$ and a k_Δ-pair for Z satisfies $P_1 \odot Z = P_1^* \odot (Z \oplus \nu)$ and $P_i^* = P_i$, $i \in \{2, 3, 4\}$. In Example 4, $Z_2^{(1)} = \nu \oplus Z_2^{(1)*}$ as $k_\Delta = 16$, and therefore $P^{[K]} = P^{[K']*} \Leftrightarrow P \oplus P^* = [0, \nu, 0, 0]$. Thus, when attacking 4-round IDEA, no subkeys are guessed in the first round and all k_Δ-pairs satisfy $P \oplus P^* = [0, \nu, 0, 0]$.

To determine if the RKDL-approximation holds with probability one, the attacker must obtain $\alpha \cdot C^{[K]} + \alpha \cdot C^{[K']*}$ from the corresponding ciphertexts by guessing subkeys in the last round. For example, in attacking 4-round IDEA, we note that the linear approximation $1 \cdot C_2^{[K]} + 1 \cdot C_3^{[K]} = 1 \cdot C_2 + 1 \cdot C_3 + 1 \cdot ((C_1 \oplus C_3) \odot Z_5^{(4)})$ holds with probability one, due to the structure of the round function. Now, as $Z_5^{(4)} = Z_5^{(4)*}$, it follows that if $Z^* \in \left\{Z_5^{(4)}, 0 \odot Z_5^{(4)}\right\}$, then

$$\begin{aligned} 1 \cdot C_2 + 1 \cdot C_3 + 1 \cdot ((C_1 \oplus C_3) \odot Z^*) & \\ +1 \cdot C_2^* + 1 \cdot C_3^* + 1 \cdot ((C_1^* \oplus C_3^*) \odot Z^*) &= 0, \end{aligned} \tag{4}$$

for all ciphertext pairs C and C^* when attacking 4-round IDEA. A pair of ciphertexts for which (4) holds is called a *RKDL-right pair for Z^**. RKDL-right pairs are defined similarly when attacking further rounds.

A *RKDL-test* on the triple (K, Z, Z^*) consists of obtaining the encryptions of a k_Δ-pair for Z, and determining if the corresponding ciphertext pair is a RKDL-right pair for Z^*. If the corresponding ciphertext pair is a RKDL-right pair for Z^*, then the triple *passes the RKDL-test* for that plaintext pair, otherwise the triple *fails.* The RKDL-weak membership tests follow DL-weak key membership tests, where RKDL-tests are conducted in the place of DL-tests. The weak key bound β is determined as with a DL-weak key membership test. As the RKDL-approximation to 4-round IDEA holds with probability one for all keys, a weak key bound does not apply. Table 4 contains details of RKDL-weak key classes of R-round and R.5-round IDEA, $4 \leq R \leq 6$, and 8-round IDEA. The RKDL-weak key class of 8-round IDEA corresponds to a RKDL-approximation to the decryption algorithm, rather than the encryption algorithm. The average data complexity is determined as with a DL-weak key membership test. Tables are computed beforehand, as with DL-weak key membership tests, to reduce the process complexity to at most three table look-ups for each plaintext pair tested.

Related-Key Differential-Linear Weak Key Attack

Step 1. Let Z be a candidate for the value of the subkey guessed in the first round.
Step 2. Conduct RKDL-tests on the triples (K, Z, Z^*) for every candidate Z^* for the value of the subkey guessed in the last round until either every triple fails a RKDL-test, or a triple (K, Z, Z^*) passes each of β RKDL-tests.
Step 3. If all triples using candidate Z fail a RKDL-test, then try another candidate for the value of the subkey guessed in the first round and return to Step 2. Otherwise, the triple (K, Z, Z^*) which passed all β RKDL-tests is assumed to be complete, and $K \in \mathcal{W}$, and the subkey guessed in the first round (last round) is either Z or $0 \odot Z$ (Z^* or $0 \odot Z^*$). □

R	k_Δ	α	b	Weak Bit Positions	Bits Guessed		β	Average Data Comp.
					First Round	Last Round		
4	16	$(0,1,1,0)$	0	-	-	18-33	-	38.4
4.5	16	$(1,1,0,0)$	15	82-96	-	75-81	36	19.5
5	16	$(1,1,0,0)$	30	75-96	-	11-26	54	38.4
5.5	16	$(1,1,0,0)$	30	18-32, 75-89	-	43-58	63	38.4
6	0	$(0,1,1,0)$	37	11-25, 75-96	0-10	-	67	$2^{13.2}$
6.5	0	$(1,0,1,0)$	44	4-25, 75-89	0-3	36-51	84	614
8	111	$(1,1,0,0)$	58	50-71, 75-110	111-124	0-15	112	$2^{19.3}$

Table 4. The largest RKDL-weak key classes for R-round and R.5-round IDEA, $4 \leq R \leq 6$, and 8-round IDEA. Membership of the RKDL-weak key class of 8-round IDEA is tested using decryption, while the remaining RKDL-weak key classes are tested using encryption. The corresponding RKDL-approximations are of the form $(k_\Delta, \alpha, \epsilon)$ where k_Δ is given in the second column, α is given in the third column and $\epsilon = 0$.

5 Conclusion

New weak key classes have been found for IDEA which are significantly larger than those previously known. The linear key schedule and the choice of group operations contribute the size of these weak key classes. We note that if key distribution and exchange protocol allow, then the attacker can determine the bits in the weak bit positions of an unknown session key by altering these bits until the appropriate test indicates that the resulting session key is weak. We recommend that the key schedule of IDEA be altered so that IDEA has no weak keys, and key distribution and exchange protocol be analyzed to ensure that known weak key classes cannot be exploited.

Acknowledgments

Many thanks to Diane Donovan and Luke O'Connor for their help and suggestions. I would also like to thank an anonymous referee for the suggestion to use vectors and precomputed tables. This suggestion greatly reduced the process complexity of the membership tests.

References

1. E. Biham. New types of cryptanalysis attacks using related keys. *Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, T. Helleseth ed., Springer-Verlag,* pages 398–409, 1994.
2. E. Biham and Shamir A. Differential cryptanalysis of DES-like cryptosystems. *Advances in Cryptology, CRYPTO'90, Lecture Notes in Computer Science, vol. 537, A. J. Menezes and S. A. Vanstone ed., Springer-Verlag,* pages 2–21, 1991.
3. E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. Technical Report 708, Technion, Israel Institute of Technology, Haifa, Israel, 1991. Also presented at Advances in Cryptology, CRYPTO'92, Lecture Notes in Computer Science, vol. 740, E. F. Brickell ed., Springer-Verlag, pages 487-496, 1993.
4. J. Borst. Differential-linear cryptanalysis of IDEA. Technical Report ESAT-COSIC Technical Report 96-2, Department of Electrical Engineering, Katholieke Universiteit Leuven, Febr. 1997.
5. J. Borst, L. R. Knudsen, and V. Rijmen. Two attacks on reduced IDEA (extended abstract). *Advances in Cryptology, EUROCRYPT'97, Lecture Notes in Computer Science, vol. 1233, W. Fumy ed., Springer-Verlag,* pages 1–13, 1997.
6. J. Daemen, R. Govaerts, and J. Vandewalle. Cryptanalysis of 2,5 rounds of IDEA (extended abstract). Technical Report ESAT-COSIC Technical Report 93/1, Department of Electrical Engineering, Katholieke Universiteit Leuven, March 1993.
7. J. Daemen, R. Govaerts, and J. Vandewalle. Weak keys for IDEA. *Advances in Cryptology, CRYPTO'93, Lecture Notes in Computer Science, vol. 773, D. Stinson ed., Springer-Verlag,* pages 224–231, 1994.
8. C. Harpes, G. G. Kramer, and J.L. Massey. Generalisation of linear cryptanalysis and the applicability of Matsui's piling-up lemma. *Advances in Cryptology, EUROCRYPT'95, Lecture Notes in Computer Science, vol. 921, L. C. Guillou, J. Quiquater eds., Springer-Verlag,* pages 24–38, 1995.
9. P. Hawkes and L. O'Connor. On applying linear cryptanalysis to IDEA. *Advances in Cryptology, ASIACRYPT'96, Lecture Notes in Computer Science, vol. 1163, K. Kim, T. Matsumoto eds., Springer-Verlag,* pages 105–115, 1996.
10. T. Jakobsen. Correlation attacks on block ciphers. Master's Thesis, Department of Mathematics, Technical University of Denmark, January, 1996.
11. J. Kelsey, B. Schneier, and D. Wagner. Key-schedule cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. *Advances in Cryptology, CRYPTO'96, Lecture Notes in Computer Science, vol. 1109, N. Koblitz ed., Springer-Verlag,* pages 237–251, 1996.
12. L. R. Knudsen and V. Rijmen. Truncated differentials of IDEA. Technical Report ESAT-COSIC Technical Report 97-1, Department of Electrical Engineering, Katholieke Universiteit Leuven, Febr. 1997.

13. X. Lai. *On the design and security of block ciphers.* ETH Series in Information Processing, editor J. Massey, Hartung-Gorre Verlag Konstanz, 1992.
14. X. Lai, J. Massey, and S. Murphy. Markov ciphers and differential cryptanalysis. *Advances in Cryptology, EUROCRYPT'91, Lecture Notes in Computer Science, vol. 547, D. W. Davies ed., Springer-Verlag,* pages 17–38, 1991.
15. S. K. Langford and M. E. Hellman. Differential-linear cryptanalysis. *Advances in Cryptology, CRYPTO'94, Lecture Notes in Computer Science, vol. 839, Y. G. Desmedt ed., Springer-Verlag,* pages 17–25, 1994.
16. M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, T. Helleseth ed., Springer-Verlag,* pages 386–397, 1994.
17. W. Meier. On the security of the IDEA block cipher. *Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, T. Helleseth ed., Springer-Verlag,* pages 371–385, 1994.

Appendix

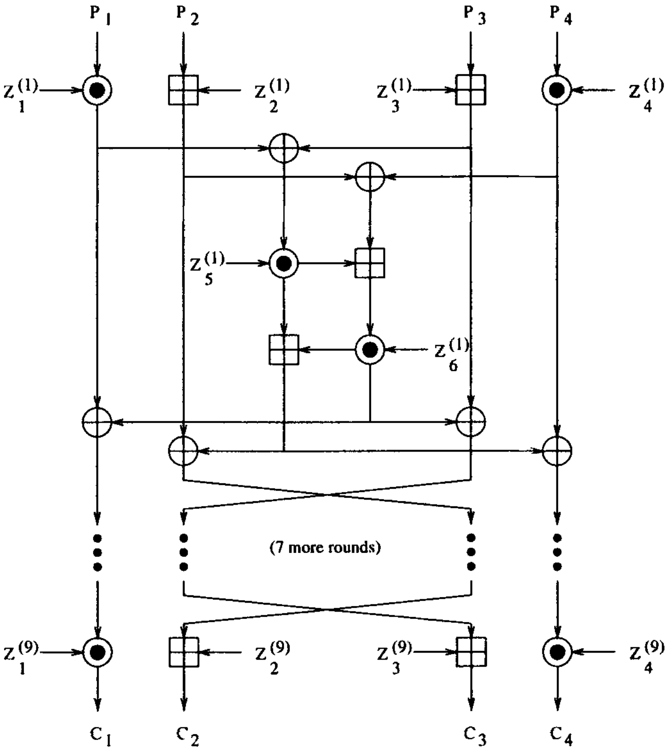


Fig. 2. The computational graph of the encryption process of the IDEA cipher.

r	Z_1	Z_2	Z_3	Z_4	Z_5	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	-	-

Table 5. Deriving the round keys from the 128-bit session key, where the session key bits are indexed with the MSB indexed by 0 and the LSB indexed by 127.

Daemen, Govaerts and Vandewalle [7] noted that for all $A \in \mathbb{Z}_2^{16}$, $0 \odot A = \overline{A} \boxplus 2$, where $\overline{A}$ is the bitwise complement of A. Consequently, the following hold with probability one:[2]

$$\begin{aligned} A \oplus A^* = 2^{m-1} = \nu &\Leftrightarrow (A \boxplus Z) \oplus (A^* \boxplus Z) = \nu, && \text{for all } Z \in \mathbb{Z}_2^{16}; \\ A \oplus A^* = \nu &\Leftrightarrow (A \odot Z) \oplus (A^* \odot Z) = \nu, && \text{if and only if } Z \in \{0,1\}; \\ 1 \cdot A + 1 \cdot Z &= 1 \cdot (A \boxplus Z), && \text{for all } Z \in \mathbb{Z}_2^{16}; \\ 1 \cdot A + 1 \cdot Z + 1 &= 1 \cdot (A \odot Z), && \text{if } Z \in \{0,1\}. \end{aligned}$$

Using these properties, Daemen, Govaerts and Vandewalle [7] found one-round linear and differential characteristics which hold with probability one when certain subkeys are either zero or one. Of these, the following one-round linear and differential characteristics are used in this paper:

$$\begin{aligned} 1 \cdot C_2^{(r)} + 1 \cdot C_3^{(r)} + 1 \cdot C_1^{(r+1)} + 1 \cdot C_3^{(r+1)} &= 1 \cdot Z_2^{(r)} + 1 \cdot Z_3^{(r)} + 1 \cdot Z_5^{(r)} + 1, \\ &\quad \text{if } Z_5^{(r)} \in \{0,1\}; \\ 1 \cdot C_1^{(r)} + 1 \cdot C_3^{(r)} + 1 \cdot C_1^{(r+1)} + 1 \cdot C_2^{(r+1)} &= 1 \cdot Z_1^{(r)} + 1 \cdot Z_3^{(r)} + 1, \\ &\quad \text{if } Z_1^{(r)} \in \{0,1\}; \\ 1 \cdot C_1^{(r)} + 1 \cdot C_2^{(r)} + 1 \cdot C_2^{(r+1)} + 1 \cdot C_3^{(r+1)} &= 1 \cdot Z_1^{(r)} + 1 \cdot Z_2^{(r)} + 1 \cdot Z_5^{(r)}, \\ &\quad \text{if } Z_1^{(r)}, Z_5^{(r)} \in \{0,1\}; \end{aligned}$$

$$\begin{aligned} \Delta C^{(r)} = [0,0,1,1] &\Leftrightarrow \Delta C^{(r+1)} = [0,1,1,0], && \text{if } Z_4^{(r)}, Z_5^{(r)} \in \{0,1\}; \\ \Delta C^{(r)} = [0,1,0,1] &\Leftrightarrow \Delta C^{(r+1)} = [0,0,1,1], && \text{if } Z_4^{(r)} \in \{0,1\}; \\ \Delta C^{(r)} = [0,1,1,0] &\Leftrightarrow \Delta C^{(r+1)} = [0,1,0,1], && \text{if } Z_5^{(r)} \in \{0,1\}. \end{aligned}$$

[2] The second result here was verified by testing all values of $Z \in \mathbb{Z}_2^{16}$.