A note on Weak Keys of PES, IDEA and some Extended Variants

Jorge Nakahara Jr*, Bart Preneel, Joos Vandewalle

Katholieke Universiteit Leuven, Dept. ESAT/COSIC, Belgium
{jorge.nakahara,bart.preneel,joos.vandewalle}@esat.kuleuven.ac.be

Version 0.17
Oct. 7, 2002

Abstract. This paper presents an analysis of the PES cipher in a similar setting as done by Daemen et al. at Crypto'93 for IDEA. The following results were obtained for 8.5 round PES: a linear weak-key class of size 2^{48}; two distinct differential weak-key classes of size 2^{41}; two differential-linear weak-key classes of size 2^{62}. For 17-round PES (double-PES): a linear weak-key class of size 2^7, and a differential weak-key class of size 2^7 were found. Daemen suggested a modified key schedule for IDEA in order to avoid weak keys. We found a differential weak-key class of size 2^{83} for 2.5-round IDEA under his redesigned key schedule, and differential-linear relations for 3.5-round IDEA.

Keywords: IDEA and PES ciphers, differential, linear and differential-linear weak-key classes, cryptanalysis.

1 Introduction

The Proposed Encryption Standard (PES) is an iterated block cipher designed by Lai and Massey in 1990 [5]. PES is a 64-bit block cipher, using a 128-bit key. PES iterates 8 similar rounds plus an output transformation (that is treated as a half round). Fig. 1 depicts the cipher structure.

The International Data Encryption Algorithm (IDEA) is a 64-bit block cipher, using a 128-bit key, designed by Lai, Massey and Murphy in 1991 (see [6]). It is an evolution of PES. IDEA is a candidate block cipher [8] to the NESSIE Project [9]. NESSIE is a project within the Information Societies Technology (IST) Program of the European Commission.

The block ciphers IDEA and PES use three group operations: addition modulo 2^{16}, represented by $\boxplus$, bitwise exclusive-or, denoted $\oplus$, and multiplication modulo $2^{16}+1$, denoted $\odot$, with the exception that 2^{16} is interpreted as 0. The overall structure of IDEA is depicted in Fig. 2.

The key schedule of IDEA and PES are identical and processes the initial 128-bit master key into fifty-two 16-bit subkeys. Each one of the eight rounds uses

* sponsored in part by GOA project Mefisto 2000/06 of the Flemish Government.

six subkeys, and the output transformation (OT) uses four subkeys. Initially, the 128-bit key is partitioned into eight 16-bit words, which are used as the first eight subkeys. Successive subkeys are generated by successively rotating left by 25 bits, the 128-bit register consisting of the previous eight subkeys; and partitioning the resulting register into eight 16-bit words, which represent the next eight subkeys. Table 1 shows the dependency of subkey bits on the master key bits, which is indexed from 0 (MSB: most significant bit) to 127 (LSB: least significant bit). Bit 0 is assumed to be positioned to the right of bit 127, that is, in a circular fashion, due to the rotation operation.

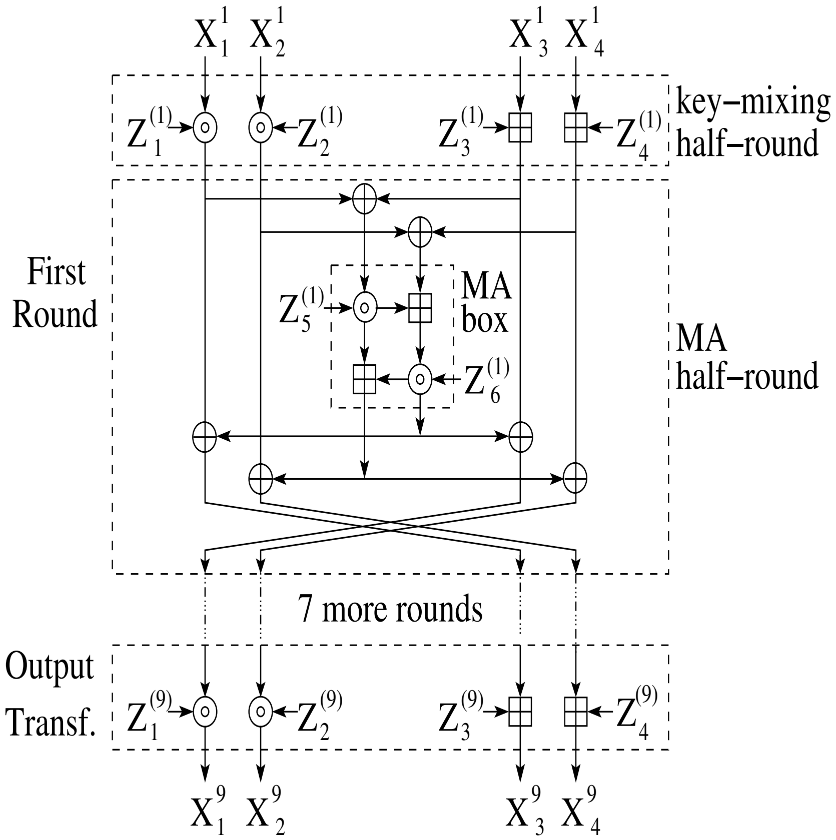

Fig. 1. Computational graph of the PES block cipher.

Some block ciphers like DES [2] and LOKI89 [7] are designed for a fixed number of rounds, which can be noticed in their key schedule algorithms: there is a fixed number of distinct round subkeys that can be generated. PES and IDEA, on the other hand, although defined with 8.5 rounds, can both be extended to

Table 1. Dependency of subkey bits on the master key bits of IDEA and PES.

r-th round	$Z_1^{(r)}$	$Z_2^{(r)}$	$Z_3^{(r)}$	$Z_4^{(r)}$	$Z_5^{(r)}$	$Z_6^{(r)}$
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
OT	22–37	38–53	54–69	70–85	—	—

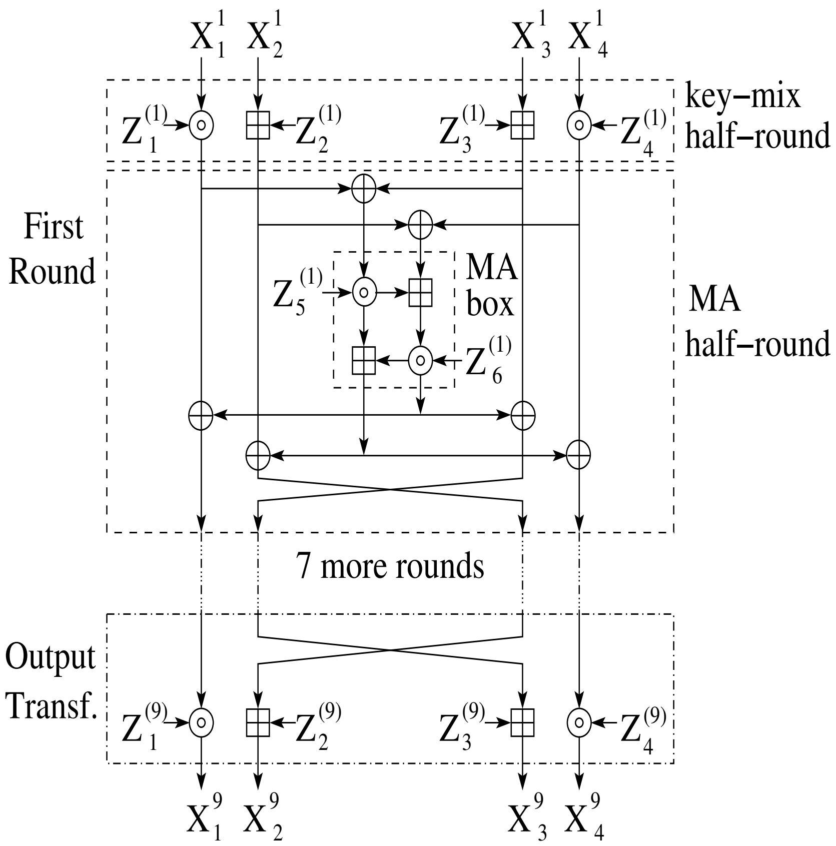

Fig. 2. Computational graph of the IDEA block cipher.

an arbitrarily large number of rounds, by simply allowing the key schedule to keep on generating 16-bit subkey words in the same way. Some observations will be made concerning these extended variants of PES and IDEA, denoted r-round PES and r-round IDEA, where r denotes the number of full rounds. Versions including the output transformation will be denoted with the prefix r.5-round.

In [1], Daemen et al. described a class of 2^{23} keys (out of a key space of size 2^{128}) for IDEA, that exhibits a linear relation with probability one. These linear relations[1] assume that the multiplicative round subkeys $Z_i^{(r)}$, $i \in \{1,4,5,6\}$ are either[2] 0 or 1. This is called the weak-key assumption. These keys are called weak, because their values make the non-linear modular multiplication become a linear operation.

Table 2 contains a summary of one-round linear relations and one-round characteristics for PES, under the weak-key assumption. The same notation as in [1] is used: $\alpha^{(r)} \rightarrow \alpha^{(r+1)}$ denotes that the input bit mask $\alpha^{(r)}$ causes the output bit mask $\alpha^{(r+1)}$ after one round with (maximum) bias 1/2. Similarly, $\delta^{(r)} \rightarrow \delta^{(r+1)}$ denotes that the input exclusive-or difference $\delta^{(r)}$ causes the output exclusive-or difference $\delta^{(r+1)}$ after one round, with probability one, where $\nu = 2^{15} = 8000_x$. Each 4-tuple corresponds to a bit mask or input difference for the four 16-bit words in a block.

Table 2. One-round linear relations and characteristics for PES.

Linear Relation	Differential Characteristic	Conditions on the subkeys			
$\alpha^{(r)} \rightarrow \alpha^{(r+1)}$	$\delta^{(r)} \rightarrow \delta^{(r+1)}$	$Z_1^{(r)}$	$Z_2^{(r)}$	$Z_5^{(r)}$	$Z_6^{(r)}$
$(0,0,0,1) \rightarrow (0,0,0,1)$	$(0,0,0,\nu) \rightarrow (\nu,0,\nu,\nu)$	-	-	-	$\{0,1\}$
$(0,0,1,0) \rightarrow (0,1,1,1)$	$(0,0,\nu,0) \rightarrow (0,0,\nu,0)$	-	-	$\{0,1\}$	$\{0,1\}$
$(0,0,1,1) \rightarrow (0,1,1,0)$	$(0,0,\nu,\nu) \rightarrow (\nu,0,0,\nu)$	-	-	$\{0,1\}$	-
$(0,1,0,0) \rightarrow (0,1,0,0)$	$(0,\nu,0,0) \rightarrow (\nu,\nu,\nu,0)$	-	$\{0,1\}$	-	$\{0,1\}$
$(0,1,0,1) \rightarrow (0,1,0,1)$	$(0,\nu,0,\nu) \rightarrow (0,\nu,0,\nu)$	-	$\{0,1\}$	-	-
$(0,1,1,0) \rightarrow (0,0,1,1)$	$(0,\nu,\nu,0) \rightarrow (\nu,\nu,0,0)$	-	$\{0,1\}$	$\{0,1\}$	-
$(0,1,1,1) \rightarrow (0,0,1,0)$	$(0,\nu,\nu,\nu) \rightarrow (0,\nu,\nu,\nu)$	-	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$
$(1,0,0,0) \rightarrow (1,1,0,1)$	$(\nu,0,0,0) \rightarrow (\nu,0,0,0)$	$\{0,1\}$	-	$\{0,1\}$	$\{0,1\}$
$(1,0,0,1) \rightarrow (1,1,0,0)$	$(\nu,0,0,\nu) \rightarrow (0,0,\nu,\nu)$	$\{0,1\}$	-	$\{0,1\}$	-
$(1,0,1,0) \rightarrow (1,0,1,0)$	$(\nu,0,\nu,0) \rightarrow (\nu,0,\nu,0)$	$\{0,1\}$	-	-	-
$(1,0,1,1) \rightarrow (1,0,1,1)$	$(\nu,0,\nu,\nu) \rightarrow (0,0,0,\nu)$	$\{0,1\}$	-	-	$\{0,1\}$
$(1,1,0,0) \rightarrow (1,0,0,1)$	$(\nu,\nu,0,0) \rightarrow (0,\nu,\nu,0)$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	-
$(1,1,0,1) \rightarrow (1,0,0,0)$	$(\nu,\nu,0,\nu) \rightarrow (\nu,\nu,0,\nu)$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$	$\{0,1\}$
$(1,1,1,0) \rightarrow (1,1,1,0)$	$(\nu,\nu,\nu,0) \rightarrow (0,\nu,0,0)$	$\{0,1\}$	$\{0,1\}$	-	$\{0,1\}$
$(1,1,1,1) \rightarrow (1,1,1,1)$	$(\nu,\nu,\nu,\nu) \rightarrow (\nu,\nu,\nu,\nu)$	$\{0,1\}$	$\{0,1\}$	-	-

[1] It is called a linear factor in [1].
[2] Or -1 and 1, respectively, in [1].

Based on Table 2, the largest weak-key class for PES uses the one-round iterative linear relation $(0,0,0,1) \to (0,0,0,1)$, which holds with probability one. For the full 8.5-round PES, the weak-key assumption requires that bits numbered 13–48, 66–94, and 109–123 be zero (according to the key schedule). This leaves key bits 0–12, 49–65, 95–108, and 124–127 unrestricted resulting in a weak-key class of size 2^{48}. The bit masks for each intermediate round of PES are shown in Table 3, where $\mathrm{msb}_n(Z)$ indicates that the n most significant bits of subkey Z are zero.

Table 3. The largest linear weak-key class of PES.

Round r	Linear Relation	$\mathrm{msb}_{15}(Z_6^{(r)})$	Weak-key class size
1	$(0,0,0,1) \to (0,0,0,1)$	80–94	2^{113}
2	$(0,0,0,1) \to (0,0,0,1)$	73–87	2^{106}
3	$(0,0,0,1) \to (0,0,0,1)$	66–80	2^{99}
4	$(0,0,0,1) \to (0,0,0,1)$	34–48	2^{84}
5	$(0,0,0,1) \to (0,0,0,1)$	27–41	2^{77}
6	$(0,0,0,1) \to (0,0,0,1)$	20–34	2^{70}
7	$(0,0,0,1) \to (0,0,0,1)$	13–27	2^{63}
8	$(0,0,0,1) \to (0,0,0,1)$	109–123	2^{48}
OT	$(0,0,0,1) \to (0,0,0,1)$	–	2^{48}

It can be observed that the linear weak-key class in Table 3 could be extended beyond 8.5 rounds. For example the one-round linear relation $(0,0,0,1) \to (0,0,0,1)$ iterated for 16 rounds of PES holds for a weak-key class of size 2^{10}; for 17-round PES this relation holds only for the all-zero key. The one-round linear relation $(0,1,0,1) \to (0,1,0,1)$ holds for 17-round PES for a weak-key class of size 2^7; for 17.5-round PES, this linear relation only holds for the all-zero key (this all-zero key is actually the only key for which there is a linear relation holding for r-round PES, for any r).

Concerning differential characteristics, and referring to the middle column in Table 2, the largest differential weak-key class of PES uses the one-round iterative characteristic $(\nu,0,\nu,0) \to (\nu,0,\nu,0)$ that holds with probability one. The propagation of differences across PES and the restrictions on the subkey words are detailed in Table 4.

The differential weak-key class in Table 4 assumes that the key bits 0–14, 22–57 and 75–110 are zero. Key bits 15–21, 58–74 and 111–127 can be arbitrary, which implies a differential weak-key class of size 2^{41}. The characteristic in Table 4 can also be iterated beyond 8.5 rounds. For example, when iterated to 17 rounds of PES, the one-round characteristic $(\nu,0,\nu,0) \to (\nu,0,\nu,0)$ holds for a weak-key class of size 2^7. For 17.5-round PES, the characteristic holds only for the all-zero key, (the all-zero key has the peculiarity that it is the only key for which the characteristic in Table 4 can be iterated for r-round PES for any r).

Another weak-key class for PES is detailed in Table 5.

Table 4. Differential weak-key class of PES.

Round r	Differential	$\mathrm{msb}_{15}(Z_1^{(r)})$	Weak-Key class size
1	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	0–14	2^{113}
2	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	96–110	2^{98}
3	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	89–103	2^{91}
4	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	82–96	2^{84}
5	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	75–89	2^{77}
6	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	43–57	2^{62}
7	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	36–50	2^{55}
8	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	29–43	2^{48}
OT	$(\nu,0,\nu,0) \to (\nu,0,\nu,0)$	22–36	2^{41}

Table 5. Another differential weak-key class of PES.

Round r	Differential	$\mathrm{msb}_{15}(Z_2^{(r)})$	Weak-Key Class Size
1	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	16–30	2^{113}
2	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	112–126	2^{98}
3	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	105–119	2^{91}
4	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	98–112	2^{84}
5	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	91–105	2^{77}
6	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	59–73	2^{62}
7	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	52–66	2^{55}
8	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	45–59	2^{48}
OT	$(0,\nu,0,\nu) \to (0,\nu,0,\nu)$	38–52	2^{41}

It can be observed that the differential weak-key class in Table 5 assumes that the key bits numbered 16–30, 38–73, and 91–126 be all zero. This leaves the key bits 0–15, 31–37, 74–90 and 127 to be arbitrary, which implies a weak-key class of size 2^{41}, like in Table 4, but notice that both key classes are distinct, for they do not share the same restriction on many key bits.

In [3], Hawkes describes a differential-linear distinguisher for IDEA, under weak-key assumptions. The attack uses the characteristic depicted in Table 6, where $\delta_1 \oplus \delta_2 = \nu$.

Table 6. Differential-linear relation of IDEA.

Round r	Differential-Linear Relation	$\mathrm{msb}_{15}(Z_1^{(r)})$	$\mathrm{msb}_{15}(Z_4^{(r)})$	$\mathrm{msb}_{15}(Z_5^{(r)})$
1	$(0,\nu,0,\nu) \rightarrow (0,0,\nu,\nu)$	–	48–62	–
2	$(0,0,\nu,\nu) \rightarrow (0,\nu,\nu,0)$	–	41–55	57–71
3	$(0,\nu,\nu,0) \rightarrow (0,\nu,0,\nu)$	–	–	50–64
4	$(0,\nu,0,\nu) \rightarrow (0,0,\nu,\nu)$	–	2–16	–
5	$(0,0,\nu,\nu) \rightarrow (\delta_1,\delta_2,\delta_3,\delta_4)$	–	–	–
6	$(1,1,0,0) \rightarrow (0,1,1,0)$	43–57	–	4–18
7	$(0,1,1,0) \rightarrow (1,0,1,0)$	–	–	125–11
8	$(1,0,1,0) \rightarrow (1,1,0,0)$	29–43	–	–

This characteristic holds with probability one, for a differential-linear weak-key class of size 2^{63} for which key bits 19–28, 72–124 are arbitrary.

For PES, one of the largest differential-linear distinguishers combines a 3-round characteristic with a 5-round linear relation. It is described in Table 7, where $\delta_2 \oplus \delta_4 = \nu$. This characteristic holds for a differential-linear weak-key class of size 2^{62}, in which key bits 15–44, 74–90, and 113–127 can be arbitrary.

Table 7. Differential-linear relation of PES.

Round r	Differential-Linear Relation	$\mathrm{msb}_{15}(Z_1^{(r)})$	$\mathrm{msb}_{15}(Z_2^{(r)})$
1	$(\nu,0,\nu,0) \rightarrow (\nu,0,\nu,0)$	0–14	–
2	$(\nu,0,\nu,0) \rightarrow (\nu,0,\nu,0)$	96–110	–
3	$(\nu,0,\nu,0) \rightarrow (\delta_1,\delta_2,\delta_3,\delta_4)$	–	–
4	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	98–112
5	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	91–105
6	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	59–73
7	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	52–66
8	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	45–59

A second differential-linear characteristic for PES holds for a weak-key class also of size 2^{62}. It is depicted in Table 8, and key bits 15–44, 74–88, and 111–127 can be arbitrary.

Table 8. Another differential-linear relation of PES.

Round r	Differential-Linear Relation	$\mathrm{msb}_{15}(Z_1^{(r)})$	$\mathrm{msb}_{15}(Z_2^{(r)})$
1	$(\nu,0,\nu,0) \rightarrow (\nu,0,\nu,0)$	0–14	–
2	$(\nu,0,\nu,0) \rightarrow (\nu,0,\nu,0)$	96–110	–
3	$(\nu,0,\nu,0) \rightarrow (\nu,0,\nu,0)$	89–103	–
4	$(\nu,0,\nu,0) \rightarrow (\delta_1,\delta_2,\delta_3,\delta_4)$	–	–
5	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	91–105
6	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	59–73
7	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	52–66
8	$(0,1,0,1) \rightarrow (0,1,0,1)$	–	45–59

In [1] Daemen et al. suggested a modified key schedule for IDEA in order to avoid linear and differential attacks under weak-key assumptions. The modification consisted in xoring each 16-bit key word with the constant value $0dae_x = 0000110110101110_2$. This modified key schedule implies, under weak-key assumptions, that some key bits be simultaneously '0' and '1', a contradiction. This new key schedule avoids all differential, linear and differential-linear attacks shown previously for PES and IDEA.

For Daemen's redesigned IDEA key schedule the longest characteristic identified has 2.5 rounds, and is shown in Table 9 [3]. It requires that key bits 9–12, 15, 18, 20, 41–44, 47, 50, 52, 64–67, 70, 73, 75 be zero, and key bits 13, 14, 16, 17, 19, 21–23, 45, 46, 48, 49, 51, 53–55, 68, 69, 71, 72, 74, 76–78 be one. In total, 45 key bits are restricted which represents a class of $2^{128-45} = 2^{83}$ differential weak keys.

Table 9. 2.5-round differential for IDEA with Daemen's new key schedule.

Round r	Differential	$\mathrm{msb}_{15}(Z_1^{(r)})$	$\mathrm{msb}_{15}(Z_4^{(r)})$
1	$(0,\nu,\nu,0) \rightarrow (0,\nu,0,\nu)$	64–78	–
2	$(0,\nu,0,\nu) \rightarrow (0,0,\nu,\nu)$	–	41–55
2.5	$(0,0,\nu,\nu) \rightarrow (0,0,\nu,\nu)$	–	9–23

The longest linear relation found for IDEA with the modified key schedule has 2.5 rounds. It requires that key bits 2–5, 8,11,13,34–37,40,43,45, 66–69,72, 75,77 be zero, and bits 6,7,9,10,12,14–16,38,39,41,42,44,46–48, 70, 71, 73, 74, 76, 78–80 be one. In total, 45 key bits are restricted which represent a class of 2^{83} weak linear keys. The relation starts at the third rounds and is depicted in Table 10).

The longest differential-linear relation found for IDEA with modified key schedule has 3.5 rounds and requires that key bits 64–67, 70,73, 75, 41–44, 47,

[3] We made a program to search exhaustively for the longest characteristic, and 2.5 rounds is the longest one found.

Table 10. 2.5-round linear relation for IDEA with Daemen's new key schedule.

Round r	Linear Relation	$\text{msb}_{15}(Z_4^{(r)})$	$\text{msb}_{15}(Z_6^{(r)})$
3	$(0,1,0,0) \rightarrow (0,0,0,1)$	–	66–80
4	$(0,0,0,1) \rightarrow (0,0,1,0)$	2–16	34–48
4.5	$(0,0,1,0) \rightarrow (0,0,1,0)$	–	–

50, 52, 9–12, 15, 18, 20, 82–85, 88, 91, 93 be zero, and key bits 68, 69, 71, 72, 74, 76–78, 45, 46, 48, 49, 51, 53–55, 13,14,16,17,19,21–23, 86,87,89,90,92,94–96 be one. These restrictions on 60 key bits result in a differential-linear weak-key class of size $2^{128-60} = 2^{68}$. Details are depicted in Table 11.

Table 11. 3.5-round differential-linear relation for IDEA with Daemens's new key schedule.

Round r	Differential or Lin. Relation	$\text{msb}_{15}(Z_1^{(r)})$	$\text{msb}_{15}(Z_4^{(r)})$	$\text{msb}_{15}(Z_5^{(r)})$
1	$(0,\nu,\nu,0) \rightarrow (0,\nu,0,\nu)$	–	–	64–78
2	$(0,\nu,0,\nu) \rightarrow (0,0,\nu,\nu)$	–	41–55	–
3	$(0,0,\nu,\nu) \rightarrow (\delta_1,\delta_2,\delta_3,\delta_4)$	–	9–23	–
3.5	$(1,0,1,0) \rightarrow (1,1,0,0)$	–	–	–
4	$(1,1,0,0) \rightarrow (1,1,0,0)$	82–96	–	–

For PES with modified key schedule, the longest differential found has 2.5 rounds. It requires that key bits 66–69, 72 75, 77, 82–85, 88, 91, 93, 34–37, 40, 43, 45 be zero, and key bits 70, 71, 73, 74, 76, 78–80, 86, 87, 89, 90, 92, 94–96, 38, 39, 41, 42, 44, 46–48 be one. These 45 restricted bits represent a class of 2^{83} weak differential keys for PES. It is depicted in Table 12.

Table 12. 2.5-round differential for PES with Daemen's new key schedule.

Round r	Differential	$\text{msb}_{15}(Z_1^{(r)})$	$\text{msb}_{15}(Z_6^{(r)})$
3	$(0,0,0,\nu) \rightarrow (\nu,0,\nu,\nu)$	–	66–80
4	$(\nu,0,\nu,\nu) \rightarrow (0,0,0,\nu)$	82–96	34–48
4.5	$(0,0,0,\nu) \rightarrow (0,0,0,\nu)$	–	–

The longest linear relation found for PES with Daemens' new key schedule has 2.5 rounds. It requires that key bits 66–69, 72, 75, 77,34–37,40,43,45 be zero, and key bits 70,71,73,74, 76,78–80,38,39,41,42,44,46–48 be one. These restrictions on 30 key bits represent a weak linear key class of size 2^{98}, that is depicted in Table 13.

Table 13. 2.5-round linear relation for PES with Daemen's new key schedule.

Round r	Linear Relation	$\text{msb}_{15}(Z_6^{(r)})$
3	$(0,0,0,1) \rightarrow (0,0,0,1)$	66–80
4	$(0,0,0,1) \rightarrow (0,0,0,1)$	34–48
4.5	$(0,0,0,1) \rightarrow (0,0,0,1)$	–

2 Conclusions

One linear weak-key class of size 2^{48}, and at least two distict differential weak-key classes, both of size 2^{41}, were identified for the PES block cipher, in a similar setting as done by Daemen et al. for IDEA. It was observed that the weak keys can be identified for linear as well as differential attacks for up to 17 rounds[4] of PES.

For IDEA, Daemen et al. described a linear weak-key class of size 2^{23}, and a differential weak-key class of size 2^{51}.

At least two differential-linear weak-key classes for PES were identified. Each has size 2^{62} and have in commom 60 key bits. The largest differential-linear characteristic described by Hawkes in [3] has size 2^{63}.

Finally, it was also noticed that linear weak-keys of size 2^{10} exist for 17-round PES, which is equivalent to double-PES. Besides a differential weak-key class of size 2^7 was identified for 17-round PES.

The new key schedule of IDEA and PES suggested by Daemen is quite effective against all these attacks and our exhaustive search could find only a 2.5-round differential and linear relation for them. Moreover, a 3.5-round differential-linear relation for IDEA was also found. The reduced-round differential, linear and differential-linear relations did not necessarily start from the first cipher round, but depend on the key schedule algorithm in order to reduce the number of key bits restricted. The original key schedule of PES and IDEA implies that different rounds of these ciphers have an asymmetric structure, and their security analysis require more care than in Feistel ciphers such as DES, since different sections of these ciphers do not have the same level of security.

References

1. J. Daemen, R. Govaerts, J. Vandewalle: Weak Keys for IDEA, Advances in Cryptology, Proceedings of Crypto 93 (D.R. Stinson, ed.), Lecture Notes in Computer Science, Springer-Verlag, New York, 773 (1994) 224–231.
2. FIPS PUB 46: Data Encryption Standard (DES), Federal Information Processing Standards Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington, DC, Jan. 15, 1977.

[4] It is interesting to compare the number of weak keys in DES, 10, to that of double-PES, 2^{10}, since both are 64-bit block ciphers with about 16 rounds, but while DES has a 56-bit key, PES has a 128-bit key.

3. P.M. Hawkes: Differential-Linear Weak Key Classes of IDEA, Advances in Cryptology, Proceedings of Eurocrypt 98 (K. Nyberg, ed.) Lecture Notes in Computer Science, Springer-Verlag, New York, 1403 (1998) 112–126.
4. X. Lai: On the Design and Security of Block Ciphers, Hartung-Gorre Verlag, Konstanz, (1992).
5. X. Lai, J.L. Massey: A Proposal for a New Block Encryption Standard, Advances in Cryptology, Proceedings of Eurocrypt 90 (I.B. Damgård, ed.), Lecture Notes in Computer Science,Springer-Verlag, New York, 473 (1990) 389–404.
6. X. Lai, J.L. Massey, S. Murphy: Markov Ciphers and Differential Cryptanalysis, Advances in Cryptology, Eurocrypt'91, (D.W. Davies, ed.), Lecture Notes in Computer Science, Springer-Verlag, Berlin-Heidelberg, 547 (1991) 17–38.
7. L. Brown, J. Pieprzyk, J. Seberry: LOKI - A Cryptographic Primitive for Authentication and Secrecy Applications, Advances in Cryptology, Proceedings of Auscrypt 90, (J. Seberry and J. Pieprzyk, eds.), Lecture Notes in Computer Science, Springer-Verlag, New York, 453 (1990) 229–236.
8. Mediacrypt AG: The IDEA Block Cipher, Submission to the NESSIE Project at `http://cryptonessie.org`.
9. NESSIE Project: New European Schemes for Signatures, Integrity and Encryption at `http://cryptonessie.org`.