Square Attacks on Reduced-Round PES and IDEA Block Ciphers

Jorge Nakahara Jr*[1], Paulo S.L.M. Barreto[2],
Bart Preneel[1], Joos Vandewalle[1], and Hae Y. Kim[2]

[1] Katholieke Universiteit Leuven, Dept. ESAT/COSIC, Leuven, Belgium
{jorge.nakahara,bart.preneel,joos.vandewalle}@esat.kuleuven.ac.be
[2] Universidade de São Paulo, Dept. Engenharia Eletrônica, São Paulo, Brazil.
{paulob,hae}@lps.usp.br

Abstract. This paper reports on variants of the Square attack applied to reduced-round versions of the PES and IDEA block ciphers. Attacks on 2.5 rounds of IDEA require $3 \cdot 2^{16}$ chosen-plaintexts and recover 78 key bits. A new kind of attack, the Square related-key attack, is applied on 2.5 rounds of IDEA and recovers 32 key bits, with 2 chosen-plaintexts and 2^{17} related keys. Similar results hold for 2.5 rounds of PES. Implementations of the attacks on 32-bit block mini-versions of both ciphers confirmed the expected computational complexity. Although our attacks do not improve on previous approaches, this report shows new variants of the Square attack on word-oriented block ciphers like IDEA and PES.

1 Introduction

The Square attacks described in this paper are extensions of the original attack against the Square block cipher [6]. They confirm the suitability of the basic attack technique to ciphers whose structure is not related to Square. In particular, we introduce the novel concept of a Square *related-key attack*.

This paper is organized as follows. Sect. 2 gives a description of the IDEA block cipher, its key schedule and round structure. Sect. 3 introduces the main concepts of the Square attack and its use against reduced-round IDEA variants, including a Square related-key attack. Sect. 4 gives a description of the PES cipher, and the Square attacks against reduced-round PES variants. Sect. 5 presents the results of this report and compares its complexity with previous known attacks.

2 The IDEA Block Cipher

The International Data Encryption Algorithm (IDEA) is a 64-bit block cipher, using a 128-bit key, designed by Lai and Massey in 1991 (see [15, 18–20]).

* sponsored in part by GOA project Mefisto 2000/06

IDEA is a candidate block cipher to the NESSIE Project [16]. NESSIE is a project within the Information Societies Technology (IST) Programme of the European Commission (Key Action II, Action Line II.4.1).

The block cipher IDEA iterates eight rounds plus an output transformation. IDEA uses three algebraic operations: addition modulo 2^{16} represented by $\boxplus$, bitwise exclusive-or, by $\oplus$, and multiplication modulo $2^{16}+1$, by $\odot$, with the exception that 2^{16} is interpreted as 0. For decryption, an additional operation, the subtraction modulo 2^{16}, denoted by $\boxminus$, is used. Before describing the round structure of IDEA, the subkey generation process will be explained.

2.1 Key Schedule of IDEA

The key schedule of IDEA processes the initial 128-bit key into fifty-two 16-bit subkeys. Each one of the eight rounds uses 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 as follows:

- the 128-bit block consisting of the previous eight subkeys is rotated left by 25 bits.
- the resulting block is partitioned 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 supposed to be positioned to the right of bit 127, that is, in a circular fashion, due to the rotation operation.

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

i-th round	Z_1^i	Z_2^i	Z_3^i	Z_4^i	Z_5^i	Z_6^i
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	—	—

2.2 One Round of IDEA

Let $X^i = (X_1^i, X_2^i, X_3^i, X_4^i)$ be the input block to the i-th round of IDEA, where $1 \leq i \leq 8$, and $X_j^i \in \mathbb{Z}_2^{16}$, with $1 \leq j \leq 4$. The first operation in a round is a subkey mixing layer. Let $Z^i = (Z_1^i,\ Z_2^i,\ Z_3^i,\ Z_4^i,\ Z_5^i,\ Z_6^i)$, with $Z_j^i \in \mathbb{Z}_2^{16}$, for $1 \leq j \leq 6$ represent the six subkey words used in the i-th round of IDEA. The output of the subkey layer is $T^i = (T_1^i, T_2^i, T_3^i, T_4^i) = (X_1^i \odot Z_1^i,\ X_2^i \boxplus Z_2^i,\ X_3^i \boxplus Z_3^i,\ X_4^i \odot Z_4^i)$. Further, $X_5^i = T_1^i \oplus T_3^i$ and $X_6^i = T_2^i \oplus T_4^i$ are computed as the inputs into a multiplication-addition (MA) structure, together with Z_5^i and Z_6^i, resulting in: $X_8^i = (X_6^i \boxplus (X_5^i \odot Z_5^i)) \odot Z_6^i$ and $X_7^i = (X_5^i \odot Z_5^i) \boxplus X_8^i$. Next, X_7^i and X_8^i are combined with T^i resulting in: $X^{i+1} = (X_1^{i+1}, X_3^{i+1}, X_2^{i+1}, X_4^{i+1}) = ((X_1^i \odot Z_1^i) \oplus X_8^i,\ (X_2^i \boxplus Z_2^i) \oplus X_7^i,\ (X_3^i \boxplus Z_3^i) \oplus X_8^i,\ (X_4^i \odot Z_4^i) \oplus X_7^i)$. The round output swaps the two middle words: $(X_1^{i+1}, X_2^{i+1}, X_3^{i+1}, X_4^{i+1})$. The subkey mixing layer is called a *half-round* (see Fig. 1). The output transformation (OT) is identical to a subkey mixing layer.

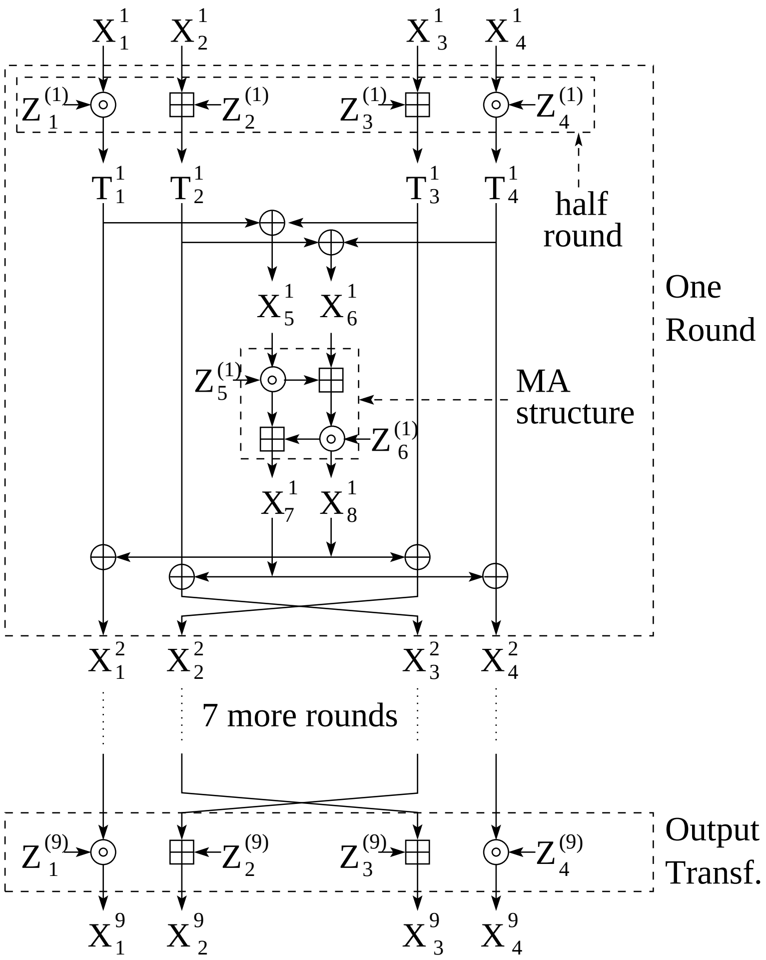

Fig. 1. Encryption scheme of IDEA block cipher

3 The SQUARE attack

The SQUARE attack is a chosen-plaintext attack which explores the byte-wise structure of the SQUARE block cipher [6]. Moreover, this technique can be applied similarly to other ciphers whose encryption scheme processes data blocks in fixed-size words at a time. Some definitions concerning the SQUARE attack are the following:

Definition 1. (Word Status)
An active *word stands for an n-bit quantity which assumes all 2^n possible values. An active word contains, therefore, a permutation of 2^n values: $0, \ldots, 2^n - 1$. Analogously, a* passive *word always assumes a fixed value. Words which are neither active nor passive are termed* garbled.

For SQUARE, $n = 8$, and for PES and IDEA the SQUARE analysis will be initially performed with $n = 16$. The following definition generalizes the original concept presented in [6]:

Definition 2. (Λ-set)
A Λ-set is a set of 2^n blocks whose n-bit words, at any position, are either active, passive or garbled.

Definition 3. (Balanced Words in a Λ-set)
Let x_i^j be the j-th value of the n-bit word at the i-th position on a Λ-set. Whenever

$$\bigoplus_{j=0}^{2^n-1} x_i^j = 0$$

the word x_i, at the i-th position, is said to be balanced *over the given Λ-set.*

Notice that both active and passive words always satisfy the property of balanced words. Garbled words can also be balanced, but not always.

A SQUARE attack starts by carefully choosing a Λ-set such that the balanced words propagate for as many rounds as possible across the cipher. By following the propagation of balanced words through the cipher rounds, it is possible to identify a pattern of active, passive and garbled words across several rounds. This pattern is traced while the Λ-sets in successive rounds contain at least one balanced word. In the round just following the one in which no more balanced words are found, an attack is made by using the property of balanced words to distinguish subkeys in the round right after the last balanced words. A similar strategy can be employed to attack rounds before the initial Λ-set.

The status of words in a Λ-set will be shortly denoted by: 'A' for an *active* word, 'P' for a *passive* word, '?' for a garbled word, and '$*$' for a balanced word. Some observations regarding the propagation of active words in IDEA, according to the different cipher operations, are the following:

Theorem 1. *(Propagation Rules for Words in a Λ-set)*
In a round of IDEA the active, passive and garbled status of a word change

according to the cipher operation and the input words' status. Table 2 summarizes the change of words' status according to the operator used and the status of its inputs. The status of the input data are depicted in the first line and the leftmost column in each sub-table.

Table 2. Input and output word status across IDEA operators

$\oplus$	A	P	$?$
A	$A/P/?$	A	$?$
P	A	P	$?$
$?$	$?$	$?$	$A/P/?$

$\boxplus$	A	P	$?$
A	$P/?$	A	$?$
P	A	P	$?$
$?$	$?$	$?$	$A/P/?$

$\odot$	A	P	$?$
A	$P/?$	A	$A/?$
P	A	P	$?$
$?$	$A/?$	$?$	$P/?$

In the sub-tables in Table 2, if both words are active or garbled, most probably their result will be garbled. There is, though, a small probability that the result will be either passive or active. That phenomenon depends on the input words being arranged in a particular order, and on the operator used.

3.1 Attacks on Reduced-Round Versions of IDEA

A terminology that will be used extensively concerning the status change of Λ-sets is the following: $(A\ P\ P\ P) \rightarrow (?\ ?\ ?\ ?)$, for example, will denote that the input Λ-set whose four 16-bit words have status $(A\ P\ P\ P)$, respectively, results after one round of IDEA, in the output Λ-set whose four words have status $(?\ ?\ ?\ ?)$, in the given order. Chains of 4-tuples represent status of data words across multiple rounds. For example, $(P\ P\ A\ A) \rightarrow (P\ A\ A\ A) \rightarrow (A\ A\ A\ A)$ means that $(P\ P\ A\ A) \rightarrow (P\ A\ A\ A)$ and $(P\ A\ A\ A) \rightarrow (A\ A\ A\ A)$ across two consecutive rounds.

Also, let $P^i = (P_1^i, P_2^i, P_3^i, P_4^i)$ denote the i-th plaintext block and $C^i = (C_1^i, C_2^i, C_3^i, C_4^i)$ the corresponding i-th ciphertext block in a Λ-set. The number of attacked rounds will be made clear from the context.

An important terminology for a Square attack is the following:

Definition 4. *(An nR-Attack)*
An nR-attack stands for a Square *attack on n rounds of a cipher, using the property of balanced words to distinguish some subkey bits surrounding a chain of Λ-sets. For IDEA and PES, n can be fractional in case half-rounds are included in the attack.*

The best Square attacks on IDEA, employing 16-bit words, use the following Λ-set chains:

$$(P\ A\ P\ P) \rightarrow (A\ A\ *\ A) \rightarrow (?\ ?\ ?\ ?) \tag{1}$$

$$(A\ P\ A\ P) \rightarrow (A\ A\ P\ P) \rightarrow (?\ ?\ ?\ ?) \tag{2}$$

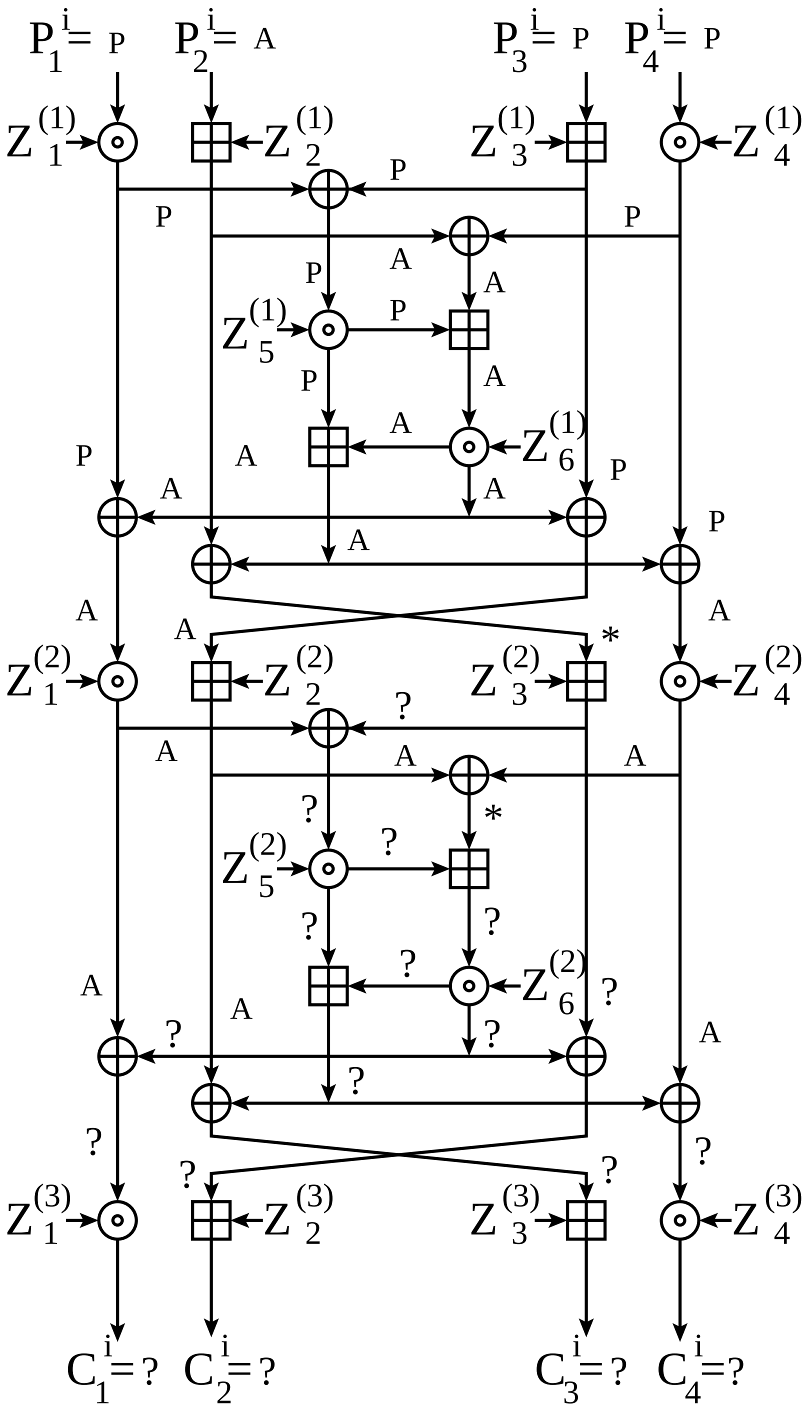

Fig. 2. 0.5R-attack on 2.5 rounds of IDEA using chain (1)

A 0.5R-attack on 2.5 rounds of IDEA can be made using chain (1). This attack exploits the property that $(C_3^i \odot Z_3^{(3)^{-1}}) \oplus (C_4^i \boxminus Z_4^{(3)})$ is balanced, to discover two subkeys $Z_3^{(3)}$ and $Z_4^{(3)}$. The MSB of $Z_3^{(3)}$, though, cannot be uniquely determined. In order to filter out wrong 31-bit key candidates, two Λ-set are used. This amounts to $2 \cdot 2^{16}$ chosen-plaintexts and $2^{1+16+31} = 2^{48}$ partial 2.5-round IDEA decryptions (see Fig. 2).

Chain (2) can be used in an attack that exploits further the kind of permutation behind an active word. A 1R-attack can be made on 2.5 rounds of IDEA, using (2), consisting of a 0.5R-attack at the beginning and a 0.5R-attack at the end of 2.5 rounds. The attack uses a Λ-set with the first and third words *both active and containing the same permutation*. Subkeys $Z_1^{(1)}$ and $Z_3^{(1)}$ are guessed by multiplying the first active word in the Λ-set by (a candidate subkey for) $Z_1^{(1)^{-1}}$ and adding the third active word with (a candidate subkey for) $-Z_3^{(1)}$. When the correct subkey pair $(Z_1^{(1)}, Z_3^{(1)})$ is found, the active word, which is the exclusive-or of the corresponding outputs after the subkey mixing, will be equal and therefore will *cancel out*, generating a passive word. This passive word will propagate through the MA structure inside the first round and will not affect any of the two original active words. At the end of the second round, the following two values might be active for the correct keys: $(C_1^i \odot Z_1^{(3)^{-1}}) \oplus (C_2^i \boxminus Z_2^{(3)})$, and $(C_3^i \boxminus Z_3^{(3)}) \oplus (C_4^i \odot Z_4^{(3)^{-1}})$. See Fig. 3. Therefore, it is possible to discover two more subkey pairs. When the correct $(Z_1^{(1)}, Z_3^{(1)})$ is used, both $(Z_1^{(3)}, Z_2^{(3)})$ and $(Z_3^{(3)}, Z_4^{(3)})$ can be computed separately. According to the key schedule of IDEA, $Z_1^{(1)}$ and $Z_3^{(3)}$ share bits 0-8 of the master key, and similarly, $Z_1^{(1)}$ and $Z_4^{(3)}$ share bits 9-15 (see Table 1). Therefore, the 4-tuple $(Z_1^{(1)}, Z_3^{(1)}, Z_3^{(3)}, Z_4^{(3)})$ consists of 48 non-overlapping key bits. Nonetheless, the MSB of the additive subkey $Z_3^{(1)}$ is not uniquely determined. Therefore, to discover the correct 47 key bits with high probability, three Λ-sets are used. This reduces the chance of a wrong subkey being filtered to $(2^{-16})^3 = 2^{-48}$. The initial computational cost of this attack is $3 \cdot 2^{16}$ chosen-plaintexts and $3 \cdot 2^{16+47} = 3 \cdot 2^{63}$ partial 2.5-round IDEA decryptions. Once $(Z_1^{(1)}, Z_3^{(1)})$ are discovered, they can be used to find $(Z_1^{(3)}, Z_2^{(3)})$ (except for the MSB of $Z_2^{(3)}$) with two Λ-sets and $2 \cdot 2^{16} \cdot 2^{31} = 2^{48}$ partial 2.5-round IDEA decryptions. Notice that $(Z_1^{(3)}, Z_2^{(3)})$ and $(Z_1^{(1)}, Z_3^{(1)})$ do not share any master key bits via the key schedule.

3.2 Larger Word Sizes

Up to now, words have been defined as being 16 bits wide. An intuitive idea for a variant SQUARE attack is to use larger word sizes, for example, in steps of 16-bits: 32 bits, 48 bits, or 64 bits.

Using Λ-set with 32-bit words, let $P^i = (P_1^i, P_2^i, P_3^i, P_4^i)$ be the blocks in a Λ-set $(0 \leq i < 2^{32})$, and $W^i = (W_{1,2}^i, W_{1,3}^i, W_{1,4}^i, W_{2,3}^i, W_{2,4}^i, W_{3,4}^i)$ denote, in the given order, the possible 32-bit words made out of the concatenation of two 16-bit words from P^i. The pairs of words taken from P^i are indicated by the sub-

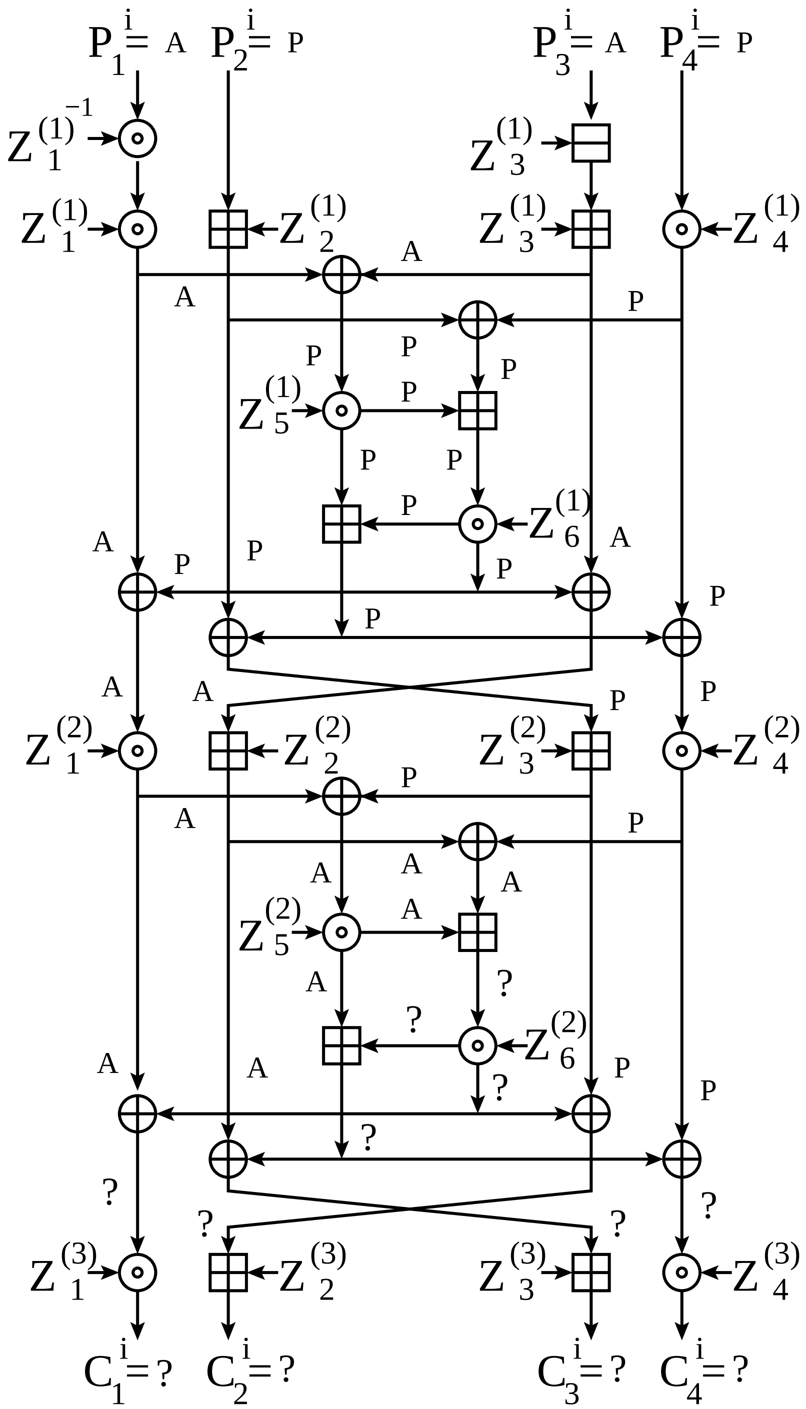

Fig. 3. 1R-attack on 2.5 rounds of IDEA using chain (2)

indexes in W^i. Let $X^i = (X_1^i, X_2^i, X_3^i, X_4^i)$ represent the blocks of output Λ-sets after one IDEA round, and let $Y^i = (Y_1^i, Y_2^i, Y_3^i, Y_4^i)$ represent the blocks of the output Λ-sets after two IDEA rounds. In the following chain (3), $W_{1,2}^i = P_1^i||P_2^i$ was made an active 32-bit word, and $W_{3,4}^i = P_3^i||P_4^i$ was made a passive 32-bit word, leading to the following pattern of Λ-sets:

$$(A\ *\ *\ *\ *\ P) \rightarrow (A\ *\ *\ *\ A\ *) \rightarrow (?\ ?\ ?\ ?\ ?\ ?) \tag{3}$$

Chain (3) indicates that, after one round, the 32-bit words $X_1^i||X_2^i$ and $X_2^i||X_4^i$ are active, and all the others pairs are passive. After two rounds, all 32-bit concatenations of two Y_i^j's are garbled. Nonetheless, analysis of 16-bit words indicate that $Y_1^i \oplus Y_2^i$ and $Y_3^i \oplus Y_4^i$ are both balanced. The chain (3) can, therefore, be used in a 0.5R-attack on 2.5 rounds of IDEA, to discover the subkey pairs $(Z_1^{(3)}, Z_2^{(3)})$ and $(Z_3^{(3)}, Z_4^{(3)})$. The MSB of both $Z_2^{(3)}$ and $Z_3^{(3)}$ are not uniquely determined, though. Therefore, the property of balanced words can discover 31 key bits at a time. In order to filter only the correct subkey values, with high probability, one (enlarged) plaintext Λ-set is used. This corresponds to 2^{32} chosen-plaintexts, and $2^{32+31} = 2^{63}$ partial 2.5-round IDEA decryptions per subkey pair.

Increasing the word size in a Λ-set to 48-bit words, the following terminology applies: let $W^i = (W_{1,2,3}^i, W_{1,2,4}^i, W_{1,3,4}^i, W_{2,3,4}^i)$ denote, in the given order, the possible 48-bit words consisting of the concatenation of three words from P^i, which are indicated by the sub-indexes of W^i. Let $Y^i = (Y_1^i, Y_2^i, Y_3^i, Y_4^i)$ represent the blocks of the output Λ-sets after two IDEA rounds.

$$(*\ A\ *\ *) \rightarrow (*\ *\ *\ *) \rightarrow (?\ ?\ ?\ ?) \tag{4}$$

Chain (4) shows that $W_{1,2,4}^i = P_1^i||P_2^i||P_4^i$ is an active 48-bit word and all the other 48-bit combinations of the input Λ-set are balanced. P_3^i is passive. The 48-bit word combinations of the second round are all balanced. The 48-bit word combinations after two rounds are all garbled, but it was detected that $Y_1^i \oplus Y_2^i$ and $Y_3^i \oplus Y_4^i$ are balanced, and this property is lost after 2.5 rounds. This allows a 0.5R-attack on 2.5 rounds of IDEA to discover $Z_1^{(3)}$ and the 15 LSBs of $Z_2^{(3)}$. In order to filter out wrong subkey candidates, one (enlarged) Λ-set is used, which amounts to 2^{48} chosen-plaintexts and $2^{48+31} = 2^{79}$ partial 2.5-round decryptions.

3.3 A SQUARE Related-Key Attack on IDEA

The following chain (5) is an iterative[1] one-round chain of Λ-sets for IDEA (and PES), using 16-bit active words:

$$(P\ P\ P\ P) \rightarrow (P\ P\ P\ P) \tag{5}$$

Up to now, it was assumed that only the plaintexts were chosen, and the key was kept fixed (passive). A SQUARE related-key attack consists of keeping the

[1] meaning that it can be chained with itself

plaintext fixed but making some subkeys active[2]. Suppose $Z_1^{(1)}$ is made active, running through all 2^{16} possible values. According to the key schedule of IDEA, if $Z_1^{(1)}$ is active, no other full subkey will be active. That is because of the left rotation by 25 bits per 128-bit block in the subkey generation. This rotation amount makes the active portion of $Z_1^{(1)}$ straddle 16-bit word boundaries for all the other subkeys used in the next 8.5 rounds, and be split into two neighboring words (neither of them being active). Only after $25 \cdot 128$ such rotations will some subkey be active. It means $25 \cdot 128 \cdot 8/6 \approx 2^{12}$ rounds. Nonetheless, if two *consecutive* master 16-bit key words were made active, and with the same permutation, for example, $Z_1^{(2)}$ and $Z_2^{(2)}$, then seven subkeys would be active across the 8.5 rounds of IDEA: $Z_1^{(2)}$, $Z_2^{(2)}$, $Z_2^{(3)}$, $Z_2^{(4)}$, $Z_3^{(5)}$, $Z_3^{(6)}$, $Z_6^{(8)}$ (see Table 1). The following Λ-set chain results by setting subkeys $Z_1^{(2)}$ and $Z_2^{(2)}$ active:

$$(P\ P\ P\ P) \rightarrow (P\ P\ P\ P) \rightarrow (?\ ?\ ?\ ?) \tag{6}$$

A 0.5R-attack can be made on 2.5-round IDEA, using chain (6). Although the input to the third round is made of all garbled words, it is a fact that $Y_1^i \oplus Y_2^i$ and $Y_3^i \oplus Y_4^i$ are both active. The 16-bit word $Y_1^i \oplus Y_2^i$ being active, can be used to discover the 7 (passive) LSBs of $Z_1^{(3)}$, with one chosen-plaintext. This amounts to $2^{16+7} = 2^{23}$ partial 2.5-round IDEA decryptions.

The 16-bit word $Y_3^i \oplus Y_4^i$ can be used to discover the 9 LSBs of Z_3^3 and the full Z_4^3 (all these bits are passive). To filter out wrong 25-bit subkey candidates under 2^{16} related keys, two distinct plaintext blocks are required. This amounts to two chosen-plaintexts, all encrypted under 2^{16} related keys, resulting in $2^{1+16+25} = 2^{37}$ partial 2.5-round IDEA decryptions.

4 The PES Block Cipher

The Proposed Encryption Standard (PES) is a 64-bit block cipher, using a 128-bit key, designed by Lai and Massey in 1990 (see [19]) and was a predecessor to IDEA. PES iterates eight rounds plus an output transformation.

4.1 A PES Round

A PES round is very similar to an IDEA round. The main differences are in the order of the operations in a subkey mixing layer, and the fixed permutation of words between rounds. While in IDEA a subkey mixing layer is composed as: $(X_1^i \odot Z_1^{(i)}, X_2^i \boxplus Z_2^{(i)}, X_3^i \boxplus Z_3^{(i)}, X_4^i \odot Z_4^{(i)})$ for an input X^i, in PES, this layer is represented by: $(X_1^i \odot Z_1^{(i)}, X_2^i \odot Z_2^{(i)}, X_3^i \boxplus Z_3^{(i)}, X_4^i \boxplus Z_4^{(i)})$. Besides, the permutation of words $(A\ B\ C\ D)$, between rounds, in IDEA has the form $(A\ B\ C\ D) \rightarrow (A\ C\ B\ D)$ while in PES, it is $(A\ B\ C\ D) \rightarrow (C\ D\ A\ B)$.

[2] This is not to be confused with the related-key attack presented in [9], which uses the structure of the Square attack in a rather different way.

4.2 Key Schedule of PES

The key-schedule of PES is the same as the one used for IDEA (see Sect. 2.1).

4.3 Attacks on Reduced-Round PES

One of the best SQUARE attacks against PES, using Λ-set with 16-bit words, is:

$$(P\ A\ P\ P) \rightarrow (A\ A\ A\ *) \rightarrow (?\ ?\ ?\ ?) \tag{7}$$

Chain (7) allows a 0.5R-attack on 2.5 rounds of PES. The attack discover the subkey pair $(Z_1^{(3)}, Z_3^{(3)})$ (except for the MSB of $Z_3^{(3)}$) by checking if $(C_1^i \odot Z_1^{(3)^{-1}}) \oplus (C_3^i \boxminus Z_3^{(3)})$ is balanced. To filter out wrong subkey candidates, two plaintext Λ-sets are used. The attack complexity is $2 \cdot 2^{16}$ chosen-plaintexts and $2 \cdot 2^{16} \cdot 2^{31} = 2^{48}$ partial 2.5-round PES decryptions. Simulations using PES(32), the 32-bit block mini-version of PES, corroborate the expected complexity figures.

Similar to IDEA, an alternative attack on PES can use larger word sizes, for example, 32 bits wide. Using the same terminology as in Sect. 3.2, the following Λ-set pattern was analysed.

$$(A\ *\ *\ *\ *\ P) \rightarrow (A\ A\ *\ *\ *\ *) \rightarrow (?\ ?\ ?\ ?\ ?\ ?) \tag{8}$$

The chain (8) of Λ-sets indicates that the input 32-bit value $P_1^i||P_2^i$ is active, $P_3^i||P_4^i$ is passive, and all other four 32-bit combinations are balanced. After one round, the combinations $X_1^i||X_2^i$ and $X_1^i||X_3^i$ are active, and all the others are passive. After two rounds, all 32-bit concatenation of two Y_i^j's are garbled. Nonetheless, analysis of 16-bit words, indicate that $Y_1^i \oplus Y_3^i$ and $Y_2^i \oplus Y_4^i$ are both balanced. The chain (8) can, therefore, be used in a 0.5R-attack on 2.5 rounds of PES, to discover subkey pairs $(Z_1^{(3)}, Z_3^{(3)})$ and $(Z_2^{(3)}, Z_4^{(3)})$, except for the MSBs of the additive subkeys: $Z_3^{(3)}$ and $Z_4^{(3)}$. The property of balanced words is applied to a 16-bit value. To filter out wrong subkey candidates, one (enlarged) plaintext Λ-set is used, which corresponds to 2^{32} chosen-plaintexts. The attack makes 2^{32+31} partial 2.5-round PES decryptions. Simulations on PES(32) corroborate the expected complexity and Λ-set requirements.

5 Conclusions

This report presented several variants of SQUARE attack applied to reduced-round versions of IDEA and PES block ciphers. The SQUARE attacks presented do not endanger the security of IDEA or PES, but we demonstrated several new variants of the original SQUARE attack, including a novel related-key attack. Besides, we illustrated that the SQUARE attack is not restricted to SQUARE-like ciphers.

Previous attacks made on IDEA and PES include:

- linear cryptanalysis experiments on IDEA, reported in [1], found no apparent weakness(es); analysis reported in [14] show that a fraction of at most $2^{-100.8}$ of all 52 possible (independent) subkeys of IDEA is susceptible to a linear cryptanalytic attack.
- in [3], experiments made on IDEA(32) showed that the 32-bit block mini-version of IDEA may not be secure against differential cryptanalysis, under certain theoretical hypothesis. These experiments though, were not extended to the real 64-bit block IDEA.
- a timing attack (see [12]) *on implementations* of the full 8.5-round IDEA, that depends on the number of multiplicative keys that are zero, is reported in [10] that can recover 80 master key bits, requiring the encryption of 2^{20} random plaintext blocks. Nonetheless, such attacks can be countered by careful implementation of the $\odot$ operation using logarithms and anti-logarithm table lookups in $GF(2^{16}+1)$.
- in [8], a set of 2^{23} weak IDEA keys could be identified by a membership test that checked if a certain linear approximation held with probability one. A second set of 2^{51} weak-keys could be identified by a membership test that checked if a differential held with probability one. An extended analysis of weak-key classes was presented in [13].

Table 3 compares the complexity of different chosen-plaintext attacks on IDEA.

Concerning the PES cipher, we list the previous (and sole known) differential attack requirements along with the SQUARE attacks in Table 4.

6 Acknowledgement

We have the pleasure to thank Dr. Rich Schroeppel for many suggestions and comments which improved readability of a previous draft of this paper.

References

1. C. Harpes, *"Cryptanalysis of Iterated Block Ciphers," ETH series in Information Processing*, J.L. Massey, Ed., Vol. 7, Hartung-Gorre Verlag, Konstanz, 1996.
2. E. Biham, A. Biryukov, A. Shamir, *"Miss-in-the-Middle Attacks on IDEA, Khufu and Khafre," Fast Software Encryption, LNCS 1636*, L.R. Knudsen, Ed., Springer-Verlag, 1999, pp. 124–138.
3. G. Hornauer, W. Stephan, R. Wernsdorf, *"Markov Ciphers and Alternating Groups," Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 453–460.
4. J. Borst, *"Differential-Linear Cryptanalysis of IDEA," Department of Electrical Engineering, ESAT–COSIC Technical Report 96/2, 14 pages.*
5. J. Borst, L. Knudsen, V. Rijmen, *"Two Attacks on Reduced IDEA (extended abstract)," Advances in Cryptology, Proceedings Eurocrypt'97, LNCS 1233*, W. Fumy, Ed., Springer-Verlag, 1997, pp. 1–13.
6. J. Daemen, L. R. Knudsen, V. Rijmen, *"The Block Cipher* SQUARE*," Fast Software Encryption, LNCS 1267*, E. Biham, Ed., Springer-Verlag, 1997, pp. 149–165.

Table 3. Comparison of attack requirements on reduced-round IDEA

Attack Type	Date	Reference	#Attacked Rounds	Key Bits Found	# Chosen Plaintexts	Time (†)
Differential	1993	[17]	2	32	2^{10}	2^{42}
Differential	1993	[7]	2.5	32	2^{10}	2^{32}
Differential	1993	[17]	2.5	96	2^{10}	2^{106}
Related-Key Differential	1996	[10]	3	32	6	$6 \cdot 2^{32}$
Differential-Linear	1996	[5]	3	32	2^{30}	2^{44}
Differential	1996	[4]	3	32	2^{30}	$0.75 \cdot 2^{44}$
Truncated Differential	1997	[11, 5]	3.5	48	2^{56}	2^{67}
Miss-in-the-middle	1998	[2]	3.5	64	$2^{38.5}$	2^{53}
Miss-in-the-middle	1998	[2]	4	69	2^{37}	2^{70}
Related-Key (♯) Differential-Linear	1998	[13]	4	15	38.3	—
Miss-in-the-Middle	1998	[2]	4.5	80	2^{64}	2^{112}
SQUARE attack	2000	chain (2)	2.5	78	$3 \cdot 2^{16}$	$3 \cdot 2^{63} + 2^{48}$
SQUARE attack	2000	chain (3)	2.5	31	2^{32}	2^{63}
SQUARE attack	2000	chain (4)	2.5	31	2^{48}	2^{79}
SQUARE Related-Key	2001	chain (6)	2.5	32	2	$2^{37} + 2^{23}$

(†) the item *Time* in Table 3 denotes the number of times the specified number of IDEA rounds needs to be computed.
(♯) the differential-linear attack requires two related keys.

Table 4. Comparison of attack requirements on reduced-round PES

Attack	Date	Reference	#Attacked Rounds	Key Bits Found	# Chosen Plaintexts	Time (‡)
Differential	1991	[20]	7	96	2^{64}	2^{160}
SQUARE attack	2000	chain (7)	2.5	31	2^{17}	2^{48}
SQUARE attack	2001	chain (8)	2.5	31	2^{32}	2^{63}
SQUARE Related-Key	2001	chain (6)	2.5	32	2	$2^{37} + 2^{23}$

(‡) the item *Time* in Table 4 denotes the number of times the specified number of PES rounds needs to be computed.

7. J. Daemen, R. Govaerts, J. Vandewalle, *"Cryptanalysis of 2.5 Rounds of IDEA (Extended Abstract)," Department of Electrical Engineering, ESAT–COSIC Technical Report 93/1, Mar. 1993, pp. 1–6.*
8. J. Daemen, R. Govaerts, J. Vandewalle, *"Weak Keys for IDEA," Advances in Cryptology, Proceedings Crypto'93, LNCS 773*, D.R. Stinson, Ed., Springer-Verlag, 1994, pp. 224–231.
9. N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, and D. Whiting, "Improved Cryptanalysis of RIJNDAEL," to appear in *Fast Software Encryption'00*, Springer-Verlag.
10. J. Kelsey, B. Schneier, D. Wagner, *"Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER and Triple-DES," Advances in Cryptology, Proceedings Crypto'96, LNCS 1109*, N. Koblitz, Ed., Springer-Verlag, 1996, pp. 237–251.
11. L.R. Knudsen, V. Rijmen, *"Truncated Differentials of IDEA," Department of Electrical Engineering, ESAT–COSIC Technical Report 97/1, 10 pages.*
12. P.C. Kocher, *"Timing Attack Cryptanalysis of Diffie-Hellman, RSA and Other Systems," Advances in Cryptology, Proceedings Crypto'96, LNCS 1109*, N. Koblitz, Ed., Springer-Verlag, 1996, pp. 104–113.
13. P. Hawkes, *"Differential-Linear Weak Key Classes of IDEA," Advances in Cryptology, Proceedings Eurocrypt'98, LNCS 1403*, K. Nyberg, Ed., Springer-Verlag, 1998, pp. 112–126.
14. P. Hawkes, L. O'Connor, *"On Applying Linear Cryptanalysis to IDEA," Advances in Cryptology, Proceedings Asiacrypt'96, LNCS 1163*, K. Kim and T. Matsumoto, Eds., Springer-Verlag, 1996, pp. 105–115.
15. Mediacrypt AG, *"The IDEA Block Cipher,"* submission to the NESSIE Project – available at `http://cryptonessie.org`.
16. NESSIE Project – New European Schemes for Signatures, Integrity and Encryption – available at `http://cryptonessie.org`.
17. W. Meier, *"On the Security of the IDEA Block Cipher," Advances in Cryptology, Proceedings Eurocrypt'93, LNCS 765*, T. Helleseth, Ed., Springer-Verlag, 1994, pp. 371–385.
18. X. Lai, *"On the Design and Security of Block Ciphers," Hartung-Gorre Verlag, Konstanz, 1992.*
19. X. Lai, J.L. Massey, *"A Proposal for a New Block Encryption Standard," Advances in Cryptology, Proceedings Eurocrypt'90, LNCS 473*, I.B. Damgård, Ed., Springer-Verlag, 1991, pp. 389–404.
20. X. Lai, J.L. Massey, S. Murphy, *"Markov Ciphers and Differential Cryptanalysis," Advances in Cryptology, Proceedings Eurocrypt'91, LNCS 547*, D.W. Davies, Ed., Springer-Verlag, 1991, pp. 17–38.