The Biryukov-Demirci Attack on IDEA and MESH Ciphers

Jorge Nakahara Jr*, Bart Preneel, Joos Vandewalle

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

Abstract. This report elaborates on an observation by Alex Biryukov on the computational graph of the IDEA cipher, and combines it with Demirci's attack presented at SAC'2002. Further, this attack is also applied to reduced-round versions of the MESH block ciphers. Particular features of these attacks are: (i) they require only known-plaintext (such as in linear cryptanalysis); (ii) they trade-off the number of known plaintext/ciphertext blocks for computing time.

1 Introduction

Alex Biryukov observed that in IDEA [2, 3] the two middle words in a block are only combined with subkeys or internal cipher data via two group operations: $\boxplus$ and $\oplus$, for the full cipher (and for any number of rounds). The first and fourth words in a block are combined only via $\oplus$ and $\odot$. Notice that this property does not hold in PES, where all words in a block are combined across the cipher via all the three group operations. This paper is organized as follows: Sect. 2 describes a known-plaintext attack on up to 4 rounds of IDEA; Sect. 2.1 applies the same reasoning for up to 2 rounds of MESH-64; Sect. 2.2 describes an equivalent attack for up to 2 rounds of MESH-96, and Sect. 2.3 describes an adapted attack for up to 2 rounds of MESH-128. Sect. 3 concludes the paper, comparing the attack complexities for reduced-round IDEA and MESH ciphers.

2 A Known-Plaintext on Reduced-Round IDEA

Let (n_i, q_i) and (r_i, s_i) denote the inputs and outputs to the i-th MA-box of IDEA, and (P_1, P_2, P_3, P_4), (C_1, C_2, C_3, C_4) be a plaintext and ciphertext blocks after 8.5 rounds. If one records the value of the input and output of only the two middle words in a block, the results are:

$$\begin{aligned}&((((((((P_2 \boxplus Z_2^{(1)}) \oplus r_1 \boxplus Z_3^{(2)}) \oplus s_2 \boxplus Z_2^{(3)}) \oplus r_3 \boxplus Z_3^{(4)}) \oplus s_4 \boxplus \\ &Z_2^{(5)}) \oplus r_5 \boxplus Z_3^{(6)}) \oplus s_6 \boxplus Z_2^{(7)}) \oplus r_7 \boxplus Z_3^{(8)}) \oplus s_8 \boxplus Z_3^{(9)} = C_3\,, \qquad (1)\end{aligned}$$

* Sponsored by a grant from the Katholieke Universiteit Leuven, and partially by GOA project Mefisto 2000/06 of the Flemish Government.

$$((((((((P_3 \boxplus Z_3^{(1)}) \oplus s_1 \boxplus Z_2^{(2)}) \oplus r_2 \boxplus Z_3^{(3)}) \oplus s_3 \boxplus Z_2^{(4)}) \oplus r_4 \boxplus \\ Z_3^{(5)}) \oplus s_5 \boxplus Z_2^{(6)}) \oplus r_6 \boxplus Z_3^{(7)}) \oplus s_7 \boxplus Z_2^{(8)}) \oplus r_8 \boxplus Z_2^{(9)} = C_2 \,. \qquad (2)$$

Equations (1) and (2) still hold if restricted only to the least significant bit. In this case, addition and bitwise exclusive-or become indistinguishable:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus r_1 \oplus Z_3^{(2)} \oplus s_2 \oplus Z_2^{(3)} \oplus r_3 \oplus Z_3^{(4)} \oplus s_4 \oplus Z_2^{(5)} \oplus \\ r_5 \oplus Z_3^{(6)} \oplus s_6 \oplus Z_2^{(7)} \oplus r_7 \oplus Z_3^{(8)} \oplus s_8 \oplus Z_3^{(9)} \oplus C_3) = 0 \,, \qquad (3)$$

$$\mathrm{lsb}_1(P_3 \oplus Z_3^{(1)} \oplus s_1 \oplus Z_2^{(2)} \oplus r_2 \oplus Z_3^{(3)} \oplus s_3 \oplus Z_2^{(4)} \oplus r_4 \oplus Z_3^{(5)} \oplus \\ s_5 \oplus Z_2^{(6)} \oplus r_6 \oplus Z_3^{(7)} \oplus s_7 \oplus Z_2^{(8)} \oplus r_8 \oplus Z_2^{(9)} \oplus C_2) = 0 \,. \qquad (4)$$

If the LSB values of (r_i, s_i) could be discovered, or only their xor value, then two key bits of information, $\mathrm{lsb}_1(Z_2^{(1)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Z_3^{(4)} \oplus Z_2^{(5)} \oplus Z_3^{(6)} \oplus Z_2^{(7)} \oplus Z_3^{(8)} \oplus Z_3^{(9)})$, and $\mathrm{lsb}_1(Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(3)} \oplus Z_2^{(4)} \oplus Z_3^{(5)} \oplus Z_2^{(6)} \oplus Z_3^{(7)} \oplus Z_2^{(8)} \oplus Z_2^{(9)})$, could be derived for IDEA, and similarly for any number of rounds. The following analysis combines this observation by Biryukov, and the approach by Demirci in [1]. The analysis starts with the first 1.5-round of IDEA (Fig. 1).

Let $(X_1^{(i)}, X_2^{(i)}, X_3^{(i)}, X_4^{(i)})$ denote the input to the i-th round, and $(Y_1^{(i)}, Y_2^{(i)}, Y_3^{(i)}, Y_4^{(i)})$ the output after the i-th key mixing. The value n_1 can be computed as follows:

$$n_1 = (P_1 \odot Z_1^{(1)}) \oplus (P_3 \boxplus Z_3^{(1)}) = (Y_1^{(2)} \odot (Z_1^{(2)})^{-1}) \oplus (Y_2^{(2)} \boxminus Z_2^{(2)}) \,. \qquad (5)$$

Using Demirci's relation [1] for the least significant bits of (r_1, s_1):

$$\mathrm{lsb}_1(r_1 \oplus s_1) = \mathrm{lsb}_1(n_1 \odot Z_5^{(1)}) \,. \qquad (6)$$

Following the input and output of the two middle words in a block gives:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus r_1 \oplus Z_3^{(2)}) = \mathrm{lsb}_1(Y_3^{(2)}) \,, \qquad (7)$$

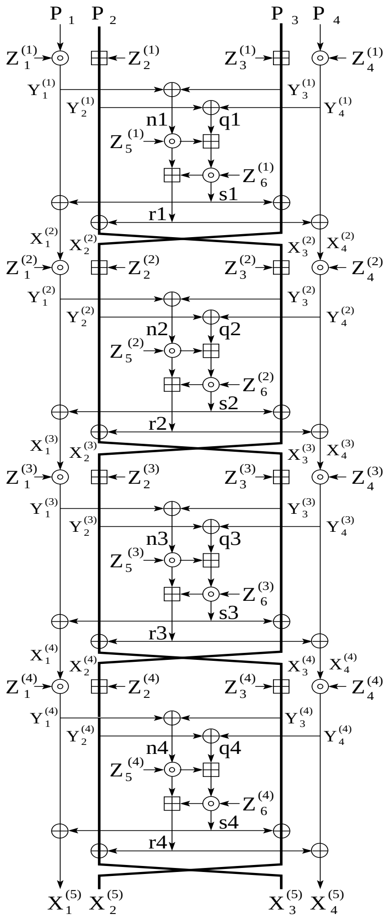
$$\mathrm{lsb}_1(P_3 \oplus Z_3^{(1)} \oplus s_1 \oplus Z_2^{(2)}) = \mathrm{lsb}_1(Y_2^{(2)}) \,. \qquad (8)$$

From the xor-combination of (6), (7) and (8):

$$\mathrm{lsb}_1(Y_2^{(2)} \oplus Y_3^{(2)} \oplus Z_2^{(2)} \oplus Z_3^{(2)} \oplus P_2 \oplus Z_2^{(1)} \oplus P_3 \oplus Z_3^{(1)}) = \mathrm{lsb}_1(n_1 \odot Z_5^{(1)}) \,. \quad (9)$$

From (5), (9) and the key overlapping property in the key schedule of IDEA, the following expression provides 33 user key bits of information: $Z_1^{(1)}$, $Z_3^{(1)}$, $Z_5^{(1)}$, $\mathrm{lsb}_1(Z_2^{(2)} \oplus Z_3^{(2)} \oplus Z_2^{(1)})$, using only known plaintext:

$$\mathrm{lsb}_1(Y_2^{(2)} \oplus Y_3^{(2)} \oplus Z_2^{(2)} \oplus Z_3^{(2)} \oplus P_2 \oplus Z_2^{(1)} \oplus P_3 \oplus Z_3^{(1)} \oplus \\ Z_5^{(1)} \odot ((P_1 \odot Z_1^{(1)}) \oplus (P_3 \boxplus Z_3^{(1)}))) = 0 \,. \qquad (10)$$



P_1 P_2 P_3 P_4
$Z_1^{(1)}$ $Z_2^{(1)}$ $Z_3^{(1)}$ $Z_4^{(1)}$
$Y_1^{(1)}$ $Y_2^{(1)}$ $Y_3^{(1)}$ $Y_4^{(1)}$
n1 q1
$Z_5^{(1)}$ $Z_6^{(1)}$
s1 r1
$X_1^{(2)}$ $X_2^{(2)}$ $X_3^{(2)}$ $X_4^{(2)}$
$Z_1^{(2)}$ $Z_2^{(2)}$ $Z_3^{(2)}$ $Z_4^{(2)}$
$Y_1^{(2)}$ $Y_2^{(2)}$ $Y_3^{(2)}$ $Y_4^{(2)}$
n2 q2
$Z_5^{(2)}$ $Z_6^{(2)}$
s2 r2
$X_1^{(3)}$ $X_2^{(3)}$ $X_3^{(3)}$ $X_4^{(3)}$
$Z_1^{(3)}$ $Z_2^{(3)}$ $Z_3^{(3)}$ $Z_4^{(3)}$
$Y_1^{(3)}$ $Y_2^{(3)}$ $Y_3^{(3)}$ $Y_4^{(3)}$
n3 q3
$Z_5^{(3)}$ $Z_6^{(3)}$
s3 r3
$X_1^{(4)}$ $X_2^{(4)}$ $X_3^{(4)}$ $X_4^{(4)}$
$Z_1^{(4)}$ $Z_2^{(4)}$ $Z_3^{(4)}$ $Z_4^{(4)}$
$Y_1^{(4)}$ $Y_2^{(4)}$ $Y_3^{(4)}$ $Y_4^{(4)}$
n4 q4
$Z_5^{(4)}$ $Z_6^{(4)}$
s4 r4
$X_1^{(5)}$ $X_2^{(5)}$ $X_3^{(5)}$ $X_4^{(5)}$

Fig. 1. The first 4 rounds of IDEA.

Expression (10) consists of 9 $\oplus$'s, 2 $\odot$'s and one $\boxplus$, equivalent to 16 $\oplus$'s, or 16/30= 8/15 of the cost of 1.5-round IDEA. Expression (10) provides a one-bit condition to recover 33 key bits (numbered 0–15, 32–47, and the xor of bits numbered 31, 40, 127) with about 33 known plaintext/ciphertext pairs, and time complexity about $\frac{8}{15} \cdot 2^{33} \approx 2^{32}$ 1.5-round IDEA computations. Notable features of this attack are: (i) it is a known-plaintext attack without any (weak-key) assumption; (ii) a relatively small number of known plaintexts is required.

An attack on 2.5-round IDEA (Fig. 1) follows a similar procedure. Note that the xor of the LSBs of the input and output of the two middle words in a block for 2.5 rounds results in:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus r_1 \oplus Z_3^{(2)} \oplus s_2 \oplus Z_2^{(3)}) = \mathrm{lsb}_1(Y_2^{(3)})\,, \tag{11}$$

$$\mathrm{lsb}_1(P_3 \oplus Z_3^{(1)} \oplus s_1 \oplus Z_2^{(2)} \oplus r_2 \oplus Z_3^{(3)}) = \mathrm{lsb}_1(Y_3^{(3)})\,. \tag{12}$$

Using Demirci's relation [1] for one-round IDEA, results in:

$$\mathrm{lsb}_1(r_1 \oplus s_1) = \mathrm{lsb}_1(Z_5^{(1)} \odot ((P_1 \odot Z_1^{(1)}) \oplus (P_3 \boxplus Z_3^{(1)})))\,, \tag{13}$$

$$\mathrm{lsb}_1(r_2 \oplus s_2) = \mathrm{lsb}_1(Z_5^{(2)} \odot ((Y_1^{(3)} \odot (Z_1^{(3)})^{-1}) \oplus (Y_2^{(3)} \boxminus Z_2^{(3)})))\,. \tag{14}$$

Combining (11), (12), (13), and (14) gives a one-bit condition, that involves 90 user key bits (numbered 64–79, 0–15, 32–47, 57–72, 89–104, 105–120, and the exclusive-or of key bits numbered 31, 47, 40, 120, 8), according to the key schedule of IDEA:

$$\begin{aligned}\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus P_3 \oplus Z_3^{(1)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Y_2^{(3)} \oplus Z_2^{(2)} \oplus Z_3^{(3)} \oplus Y_3^{(3)}) = \\ \mathrm{lsb}_1(r_1 \oplus s_1) \oplus \mathrm{lsb}_1(r_2 \oplus s_2) = \mathrm{lsb}_1(Z_5^{(1)} \odot ((P_1 \odot Z_1^{(1)}) \oplus \\ (P_3 \boxplus Z_3^{(1)}))) \oplus \mathrm{lsb}_1(Z_5^{(2)} \odot ((Y_1^{(3)} \odot (Z_1^{(3)})^{-1}) \oplus (Y_2^{(3)} \boxminus Z_2^{(3)})))\,.\end{aligned} \tag{15}$$

Expression (15) contains 12 $\oplus$'s, 4 $\odot$'s and 2 $\boxplus$'s, equivalent to 26 $\oplus$'s or 26/52 of the cost of 2.5-round IDEA. Expression (15) allows recovery of subkey bits $Z_1^{(1)}$, $Z_3^{(1)}$, $Z_5^{(1)}$, $Z_5^{(2)}$, $Z_1^{(3)}$, $Z_2^{(3)}$, and $\mathrm{lsb}_1(Z_2^{(1)} \oplus Z_3^{(1)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Z_2^{(2)} \oplus Z_3^{(3)})$, with about 90 known plaintexts, and $\frac{26}{52} \cdot 2^{90} = 2^{89}$ 2.5-round IDEA computations.

An attack on 3.5-round IDEA (Fig. 1) follows a similar procedure. Note that the exclusive-or of the LSBs of the input and output of the two middle words in a block, for 3.5 rounds, gives:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus r_1 \oplus Z_3^{(2)} \oplus s_2 \oplus Z_2^{(3)} \oplus r_3 \oplus Z_3^{(4)}) = \mathrm{lsb}_1(Y_3^{(4)})\,, \tag{16}$$

$$\mathrm{lsb}_1(P_3 \oplus Z_3^{(1)} \oplus s_1 \oplus Z_2^{(2)} \oplus r_2 \oplus Z_3^{(3)} \oplus s_3 \oplus Z_2^{(4)}) = \mathrm{lsb}_1(Y_2^{(4)})\,. \tag{17}$$

Combining (16) and (17) gives:

$$\begin{aligned}\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Z_3^{(4)} \oplus P_3 \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(3)} \oplus \\ Z_2^{(4)} \oplus Y_3^{(4)} \oplus Y_2^{(4)}) = \mathrm{lsb}_1(r_1 \oplus s_1) \oplus \mathrm{lsb}_1(r_2 \oplus s_2) \oplus \mathrm{lsb}_1(r_3 \oplus s_3)\,,\end{aligned} \tag{18}$$

Using Demirci's relation [1] for one-round IDEA, results in:

$$\begin{aligned}\mathrm{lsb}_1(r_2 \oplus s_2) = \mathrm{lsb}_1(Z_5^{(2)} \odot ((Y_1^{(3)} \odot (Z_1^{(3)})^{-1}) \oplus (Y_2^{(3)} \boxminus Z_2^{(3)}))) = \\ \mathrm{lsb}_1(Z_5^{(2)} \odot ((((Y_1^{(4)} \odot (Z_1^{(4)})^{-1} \oplus s_3) \odot (Z_1^{(3)})^{-1}) \oplus \\ ((Y_3^{(4)} \boxminus Z_3^{(4)}) \oplus r_3 \boxminus Z_2^{(3)})))\,,\end{aligned} \tag{19}$$

$$\mathrm{lsb}_1(r_3 \oplus s_3) = \mathrm{lsb}_1(Z_5^{(3)} \odot ((Y_1^{(4)} \odot (Z_1^{(4)})^{-1}) \oplus (Y_2^{(4)} \boxminus Z_2^{(4)})))\,. \tag{20}$$

To solve (19), the individual values of r_3 and s_3 are needed:

$$\begin{aligned}s_3 = (((Y_1^{(4)} \odot (Z_1^{(4)})^{-1}) \oplus (Y_2^{(4)} \boxminus Z_2^{(4)})) \odot Z_5^{(3)} \boxplus \\ ((Y_3^{(4)} \boxminus Z_3^{(4)}) \oplus (Y_4^{(4)} \odot (Z_4^{(4)})^{-1})) \odot Z_6^{(3)})\,,\end{aligned} \tag{21}$$

$$r_3 = s_3 \boxplus (((Y_1^{(4)} \odot (Z_1^{(4)})^{-1}) \oplus (Y_2^{(4)} \boxminus Z_2^{(4)})) \odot Z_5^{(3)}) \,. \tag{22}$$

Combining (13), (18), (19), (20), (21) and (22) contains 14 $\odot$'s, 10 $\boxplus$'s and 20 $\oplus$'s, which is equivalent to 72 $\oplus$'s. This combination gives a one-bit distinguisher to recover 112 key bits (numbered 0–17, 32–47, 50–127), according to the key schedule of IDEA, using about 112 known plaintexts, and $\frac{72}{74} \cdot 2^{112} \approx 2^{112}$ 3.5-round IDEA computations. The subkeys involved are $Z_1^{(1)}$, $Z_3^{(1)}$, $Z_5^{(1)}$, $Z_5^{(2)}$, $Z_1^{(3)}$, $Z_2^{(3)}$, $Z_5^{(3)}$, $Z_6^{(3)}$, $Z_1^{(4)}$, $Z_2^{(4)}$, $Z_3^{(4)}$, $Z_4^{(4)}$, and $\mathrm{lsb}_1(Z_2^{(1)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Z_3^{(4)} \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(3)} \oplus Z_2^{(4)})$.

An attack on 4-round IDEA (Fig. 1) follows a similar procedure. Note that the exclusive-or of the LSBs of the input and output of the two middle words in a block, for 4 rounds, gives:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus r_1 \oplus Z_3^{(2)} \oplus s_2 \oplus Z_2^{(3)} \oplus r_3 \oplus Z_3^{(4)} \oplus s_4) = \mathrm{lsb}_1(X_2^{(5)}) \,, \tag{23}$$

$$\mathrm{lsb}_1(P_3 \oplus Z_3^{(1)} \oplus s_1 \oplus Z_2^{(2)} \oplus r_2 \oplus Z_3^{(3)} \oplus s_3 \oplus Z_2^{(4)} \oplus r_4) = \mathrm{lsb}_1(X_3^{(5)}) \,. \tag{24}$$

Combining (23) and (24) results in:

$$\begin{aligned}\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Z_3^{(4)} \oplus P_3 \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(3)} \oplus \\ Z_2^{(4)} \oplus X_3^{(5)} \oplus X_2^{(5)}) = \mathrm{lsb}_1(r_1 \oplus s_1) \oplus \mathrm{lsb}_1(r_2 \oplus s_2) \oplus \\ \mathrm{lsb}_1(r_3 \oplus s_3) \oplus \mathrm{lsb}_1(r_4 \oplus s_4) \,.\end{aligned} \tag{25}$$

Using Demirci's relation for one-round IDEA, results in:

$$\mathrm{lsb}_1(r_2 \oplus s_2) = \mathrm{lsb}_1(Z_5^{(2)} \odot ((P_1 \odot Z_1^{(1)} \oplus s_1) \odot Z_1^{(2)} \oplus (((P_2 \boxplus Z_2^{(1)}) \oplus r_1) \boxplus Z_3^{(2)}))) \,, \tag{26}$$

$$\mathrm{lsb}_1(r_3 \oplus s_3) = \mathrm{lsb}_1(Z_5^{(3)} \odot ((Y_1^{(4)} \odot (Z_1^{(4)})^{-1}) \oplus (Y_2^{(4)} \boxminus Z_2^{(4)}))) \,. \tag{27}$$

$$\mathrm{lsb}_1(r_4 \oplus s_4) = \mathrm{lsb}_1((X_1^{(5)} \oplus X_2^{(5)}) \odot Z_5^{(4)}) \,, \tag{28}$$

To solve (26), the individual values of r_1 and s_1 are needed:

$$s_1 = (((P_1 \odot Z_1^{(1)}) \oplus (P_3 \boxplus Z_3^{(1)})) \odot Z_5^{(1)} \boxplus ((P_2 \boxplus Z_2^{(1)}) \oplus (P_4 \odot Z_4^{(1)}))) \odot Z_6^{(1)} \,, \tag{29}$$

$$r_1 = s_1 \boxplus ((P_1 \odot Z_1^{(1)}) \oplus (P_3 \boxplus Z_3^{(1)})) \odot Z_5^{(1)} \,. \tag{30}$$

To solve (27), the individual values of $Y_1^{(4)}$ and $Y_2^{(4)}$ are needed:

$$Y_1^{(4)} = X_1^{(5)} \oplus s_4 = X_1^{(5)} \oplus ((X_1^{(5)} \oplus X_2^{(5)}) \odot Z_5^{(4)} \boxplus (X_3^{(5)} \oplus X_4^{(5)})) \odot Z_6^{(4)} \,, \tag{31}$$

$$Y_2^{(4)} = X_3^{(5)} \oplus r_4 = X_3^{(5)} \oplus (s_4 \boxplus (X_1^{(5)} \oplus X_2^{(5)}) \odot Z_5^{(4)}) \,. \tag{32}$$

Combining (13), (25), (26), (27), (28), (29), (30), (31), and (32) results in 17 $\odot$'s, 11 $\boxplus$'s and 25 $\oplus$'s, which is equivalent to about 87 $\oplus$'s. This combination gives a one-bit distinguisher to recover 114 key bits (numbered 0-113 according to the key schedule of IDEA), requiring about 114 known plaintexts and $\frac{87}{88} \cdot 2^{114} \approx 2^{114}$

4-round IDEA computations. The subkeys involved are $Z_1^{(1)}$, $Z_2^{(1)}$, $Z_3^{(1)}$, $Z_4^{(1)}$, $Z_5^{(1)}$, $Z_6^{(1)}$, $Z_5^{(2)}$, $Z_1^{(2)}$, $Z_3^{(2)}$, $Z_5^{(3)}$, $Z_1^{(4)}$, $Z_2^{(4)}$, $Z_5^{(4)}$, $Z_6^{(4)}$, and $\mathrm{lsb}_1(Z_2^{(1)} \oplus Z_3^{(2)} \oplus Z_2^{(3)} \oplus Z_3^{(4)} \oplus Z_3^{(1)} \oplus Z_2^{(2)} \oplus Z_3^{(3)} \oplus Z_2^{(4)})$.

An attack on 4.5 rounds would involve all 128 key bits and therefore, not more efficient than exhaustive key search.

2.1 The Biryukov-Demirci Attack on MESH-64

Similar attacks to the previous section can be applied to at most two rounds of MESH-64 [4], with an effort less than that of exhaustive key search.

To attack 1.5-round MESH-64, there are two possible trails to follow in the graph of Fig. 2.

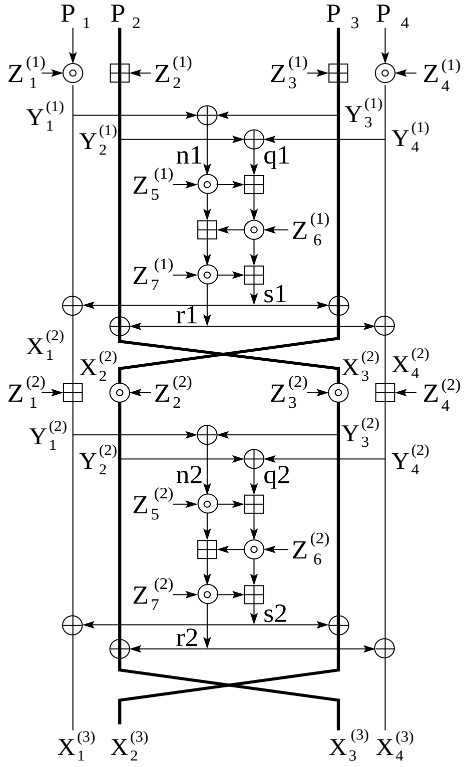


Fig. 2. The first 2 rounds of MESH-64.

- Consider the trails involving the two middle words in a block:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus r_1) = \mathrm{lsb}_1(Y_3^{(2)} \odot (Z_3^{(2)})^{-1})\,, \tag{33}$$

$$\mathrm{lsb}_1(P_3 \oplus Z_3^{(1)} \oplus s_1) = \mathrm{lsb}_1(Y_2^{(2)} \odot (Z_2^{(2)})^{-1})\,. \tag{34}$$

  Combining (33) and (34) results in:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus P_3 \oplus Z_3^{(1)} \oplus Y_3^{(2)} \odot (Z_3^{(2)})^{-1} \oplus Y_2^{(2)} \odot (Z_2^{(2)})^{-1}) = \mathrm{lsb}_1(r_1 \oplus s_1)\,. \tag{35}$$

  The right-hand side of (35) can be represented as:

$$\begin{aligned} \mathrm{lsb}_1(r_1 \oplus s_1) = \quad & \mathrm{lsb}_1((((P_1 \odot Z_1^{(1)}) \oplus (P_3 \boxplus Z_3^{(1)})) \odot Z_5^{(1)} \boxplus \\ & \quad ((P_2 \boxplus Z_2^{(1)}) \oplus (P_4 \odot Z_4^{(1)}))) \odot Z_6^{(1)}) & (36) \\ = \mathrm{lsb}_1&((((Y_1^{(2)} - Z_1^{(2)}) \oplus (Y_2^{(2)} \odot (Z_2^{(2)})^{-1})) \odot Z_5^{(1)} \boxplus \\ & ((Y_3^{(2)} \odot (Z_3^{(2)})^{-1}) \oplus (Y_4^{(2)} \boxminus Z_4^{(2)}))) \odot Z_6^{(1)})\,. & (37) \end{aligned}$$

  Expressions (35) and (36) involve 7 $\oplus$, 6 $\odot$ and 3 $\boxplus$, which is equivalent to 30 $\oplus$. These expressions provide a one-bit condition to recover 128 key bits of information: $Z_1^{(1)}$, $Z_2^{(1)}$, $Z_3^{(1)}$, $Z_4^{(1)}$, $Z_5^{(1)}$, $Z_6^{(1)}$, $Z_2^{(2)}$, and $Z_3^{(2)}$. According to the key schedule of MESH-64:

$$\begin{aligned} Z_2^{(2)} &= (((Z_1^{(1)} \boxplus Z_2^{(1)}) \oplus Z_3^{(1)} \boxplus Z_6^{(1)}) \oplus Z_7^{(1)} \boxplus Z_1^{(2)}) \lll 7 \oplus c_8\,, \\ Z_3^{(2)} &= (((Z_2^{(1)} \boxplus Z_3^{(1)}) \oplus Z_4^{(1)} \boxplus Z_7^{(1)}) \oplus Z_1^{(2)} \boxplus Z_2^{(2)}) \lll 7 \oplus c_9\,, \end{aligned} \tag{38}$$

  which implies that the values of $Z_2^{(2)}$, and $Z_3^{(2)}$ cannot be deduced from the other subkey words, namely there is not similar overlap property such as in IDEA, to reduce the time complexity. The attack requirements are 128 known plaintexts and about $\frac{30}{34} \cdot 2^{128} \approx 2^{128}$ 1.5-round MESH-64 computations.

  Expressions (35) and (37) provide a one-bit condition to recover 128 key bits of information: $Z_1^{(1)}$, $Z_2^{(1)}$, $Z_3^{(1)}$, $Z_4^{(1)}$, $Z_5^{(1)}$, $Z_6^{(1)}$, $Z_3^{(2)}$, $Z_2^{(2)}$. The attack requirements are 128 known plaintexts and 2^{128} computations of (35) and (37).

- Consider the trails involving the first and 4th words in a block:

$$\mathrm{lsb}_1(P_1 \odot Z_1^{(1)} \oplus s_1) = \mathrm{lsb}_1(Y_1^{(2)} \oplus Z_1^{(2)})\,, \tag{39}$$

$$\mathrm{lsb}_1(P_4 \odot Z_4^{(1)} \oplus r_1) = \mathrm{lsb}_1(Y_4^{(2)} \oplus Z_4^{(2)})\,. \tag{40}$$

  Combining (39) and (40) results in:

$$\mathrm{lsb}_1(P_1 \odot Z_1^{(1)} \oplus P_4 \odot Z_4^{(1)} \oplus Y_1^{(2)} \oplus Z_1^{(2)} \oplus Y_4^{(2)} \oplus Z_4^{(2)}) = \mathrm{lsb}_1(r_1 \oplus s_1)\,. \tag{41}$$

  The right-hand side of (41) can be represented as (36) or (37). Expressions (41) and (36) provide a one-bit condition to recover 97 key bits of information: $Z_1^{(1)}$, $Z_2^{(1)}$, $Z_3^{(1)}$, $Z_4^{(1)}$, $Z_5^{(1)}$, $Z_6^{(1)}$, and $\mathrm{lsb}_1(Z_1^{(2)} \oplus Z_4^{(2)})$. The attack

requirements are about 97 known plaintexts, and $\frac{30}{34} \cdot 2^{97} \approx 2^{97}$ 1.5-round MESH-64 computations.
Expressions (41) and (37) provide a one-bit condition to recover 128 key bits of information: $Z_1^{(1)}$, $Z_4^{(1)}$, $Z_5^{(1)}$, $Z_6^{(1)}$, $Z_1^{(2)}$, $Z_2^{(2)}$, $Z_3^{(2)}$, $Z_4^{(2)}$. The attack requirements are about 128 known plaintexts, and $\frac{30}{34} \cdot 2^{128} \approx 2^{128}$ 1.5-round MESH-64 computations.

To attack 2-round MESH-64, there are two possibilities in the graph of Fig. 2:

- Consider the trail involving the two middle words in a block:

$$\text{lsb}_1((P_2 \boxplus Z_2^{(1)} \oplus r_1) \odot Z_3^{(2)} \oplus s_2) = \text{lsb}_1(X_2^{(3)})\,, \tag{42}$$

$$\text{lsb}_1((P_3 \boxplus Z_3^{(1)} \oplus s_1) \odot Z_2^{(2)} \oplus r_2) = \text{lsb}_1(X_3^{(3)})\,. \tag{43}$$

  Combining (42) and (43) results in:

$$\text{lsb}_1((P_2 \boxplus Z_2^{(1)} \oplus r_1) \odot Z_3^2 \oplus (P_3 \boxplus Z_3^{(1)} \oplus s_1) \odot Z_2^{(2)} \oplus X_2^{(3)} \oplus X_3^{(3)}) = \text{lsb}_1(r_2 \oplus s_2)\,. \tag{44}$$

  The right-hand side of (44) can be represented as:

$$\text{lsb}_1(r_2 \oplus s_2) = \text{lsb}_1(((X_1^{(3)} \oplus X_2^{(3)}) \odot Z_5^{(2)} \boxplus (X_3^{(3)} \oplus X_4^{(3)})) \odot Z_6^{(2)})\,. \tag{45}$$

  For (44), the individual values of r_1 and s_1 are needed:

$$r_1 = (n_1 \odot Z_5^{(1)} \boxplus (n_1 \odot Z_5^{(1)} \boxplus q_1) \odot Z_6^{(1)}) \odot Z_7^{(1)}\,, \tag{46}$$

$$s_1 = r_1 \boxplus (n_1 \odot Z_5^{(1)} \boxplus q_1) \odot Z_6^{(1)}\,. \tag{47}$$

  Combining (44), (45), (46) and (47) contains 10 $\odot$, 7 $\oplus$ and 7 $\boxplus$. This combination results in a one-bit condition to recover $Z_1^{(1)}$, $Z_2^{(1)}$, $Z_3^{(1)}$, $Z_4^{(1)}$, $Z_5^{(1)}$, $Z_6^{(1)}$, $Z_7^{(1)}$, $Z_2^{(2)}$, $Z_3^{(2)}$, $Z_5^{(2)}$, $Z_6^{(2)}$, which according to the key schedule of MESH-64, correspond to the full 128-bit user key. The effort is therefore, not less than an exhausive key search.
- Consider the trails involving the first and 4th words in a block:

$$\text{lsb}_1(P_1 \odot Z_1^{(1)} \oplus s_1 \oplus Z_1^{(2)} \oplus s_2) = \text{lsb}_1(X_1^{(3)})\,, \tag{48}$$

$$\text{lsb}_1(P_4 \odot Z_4^{(1)} \oplus r_1 \oplus Z_4^{(2)} \oplus r_2) = \text{lsb}_1(X_4^{(3)})\,. \tag{49}$$

  Combining (48) and (49) results in:

$$\begin{aligned} \text{lsb}_1(P_1 \odot Z_1^{(1)} \oplus Z_1^{(2)} \oplus X_1^{(3)} \oplus P_4 \odot Z_4^{(1)} \oplus Z_4^{(2)} \oplus X_4^{(3)}) = \\ \text{lsb}_1(r_1 \oplus s_1) \oplus \text{lsb}_1(r_2 \oplus s_2) = \\ \text{lsb}_1(((P_1 \odot Z_1^{(1)} \oplus (P_3 \boxplus Z_3^{(1)}) \odot Z_5^{(1)} \boxplus ((P_2 \boxplus Z_2^{(1)}) \oplus (P_4 \odot \\ Z_4^{(1)}))) \odot Z_6^{(1)}) \oplus \text{lsb}_1(((X_1^{(3)} \oplus X_2^{(3)}) \odot Z_5^2 \boxplus (X_3^{(3)} \oplus X_4^{(3)})) \odot Z_6^{(2)})\,. \end{aligned} \tag{50}$$

  Expression (50) contains 6 $\odot$, 4 $\boxplus$ and 5 $\oplus$, which is equivalent to 27 $\oplus$. This expression is a one-bit condition that allows to recover 128 key bits of information: $Z_1^{(1)}$, $Z_2^{(1)}$, $Z_3^{(1)}$, $Z_4^{(1)}$, $Z_5^{(1)}$, $Z_6^{(1)}$, $Z_5^{(2)}$, $Z_6^{(2)}$, with about 128 known plaintexts and $\frac{27}{52} \cdot 2^{128} \approx 2^{127}$ 2-round MESH-64 computations.

2.2 The Biryukov-Demirci Attack on MESH-96

Similar attacks to the previous section can be applied on at most 2 rounds of MESH-96 [4], with an effort less than that of exhaustive key search.

To attack 1.5-round MESH-96, consider the trails involving $(P_2, Y_4^{(2)})$,and $(P_6, Y_6^{(2)})$ in the graph of Fig. 3.

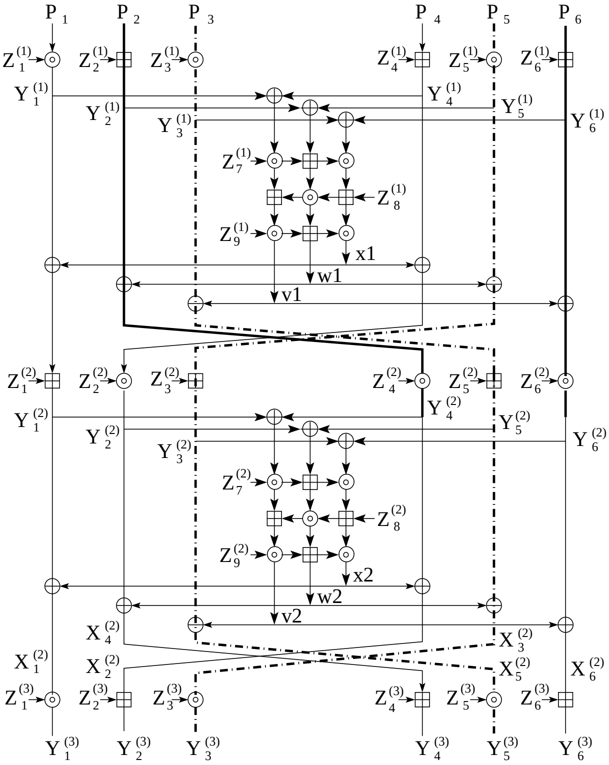


Fig. 3. The first 2.5 rounds of MESH-96.

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus w_1) = \mathrm{lsb}_1(Y_4^{(2)} \odot (Z_4^{(2)})^{-1})\,, \tag{51}$$

$$\mathrm{lsb}_1(P_6 \oplus Z_6^{(1)} \oplus v_1) = \mathrm{lsb}_1(Y_6^{(2)} \odot (Z_6^{(2)})^{-1})\,. \tag{52}$$

Combining (51) and (52) results in:

$$\mathrm{lsb}_1(P_2 \oplus Z_2^{(1)} \oplus P_6 \oplus Z_6^{(1)} \oplus Y_4^{(2)} \odot (Z_4^{(2)})^{-1} \oplus Y_6^{(2)} \odot (Z_6^{(2)})^{-1}) = \mathrm{lsb}_1(v_1 \oplus w_1)\,. \tag{53}$$

The right-hand side of (53) can be represented as:

$$\mathrm{lsb}_1(v_1 \oplus w_1) = \mathrm{lsb}_1(((Y_1^{(2)} \oplus Y_2^{(2)}) \odot Z_7^{(1)} \boxplus (Y_3^{(2)} \oplus Y_4^{(2)})) \odot \\ (Z_8^{(1)} \boxplus ((Y_1^{(2)} \oplus Y_2^{(2)}) \odot Z_7^{(1)} \boxplus (Y_3^{(2)} \oplus Y_4^{(2)})) \odot (Y_5^{(2)} \oplus Y_6^{(2)}))) \,. \qquad (54)$$

Expressions (53) and (54) contain 6 $\odot$, 3 $\boxplus$ and 10 $\oplus$, which is equivalent to 31 $\oplus$. These expressions provide a one-bit condition to recover 65 key bits of information: $Z_7^{(1)}$, $Z_8^{(1)}$, $Z_4^{(2)}$, $Z_6^{(2)}$, $\mathrm{lsb}_1(Z_2^{(1)} \oplus Z_6^{(1)})$. The attack requirements are about 65 known plaintexts and $\frac{31}{52} \cdot 2^{65} \approx 2^{64.3}$ 1.5-round MESH-96 computations.

To attack 2-round MESH-96, consider the trails involving $(P_3, X_3^{(2)})$,and $(P_5, X_5^{(2)})$ in the graph of Fig. 3.

$$\mathrm{lsb}_1(P_3 \odot Z_3^{(1)} \oplus v_1 \oplus Z_5^{(2)} \oplus w_2) = \mathrm{lsb}_1(X_3^{(2)}) \,, \qquad (55)$$

$$\mathrm{lsb}_1(P_5 \odot Z_5^{(1)} \oplus w_1 \oplus Z_3^{(2)} \oplus v_2) = \mathrm{lsb}_1(X_5^{(2)}) \,. \qquad (56)$$

Combining (55) and (56) results in:

$$\mathrm{lsb}_1((P_3 \odot Z_3^{(1)} \oplus Z_5^{(2)} \oplus X_3^{(2)} \oplus P_5 \odot Z_5^{(1)} \oplus Z_3^{(2)} \oplus X_5^{(2)}) = \mathrm{lsb}_1(v_1 \oplus w_1) \oplus \mathrm{lsb}_1(v_2 \oplus w_2) \,. \qquad (57)$$

The components in the right-hand side of (57) can be represented as:

$$\mathrm{lsb}_1(v_1 \oplus w_1) = \mathrm{lsb}_1(((Y_1^{(1)} \oplus Y_4^{(1)}) \odot Z_7^{(1)} \boxplus (Y_2^{(1)} \oplus Y_5^{(1)})) \odot \\ (Z_8^{(1)} \boxplus ((Y_1^{(1)} \oplus Y_4^{(1)}) \odot Z_7^{(1)} \boxplus (Y_2^{(1)} \oplus Y_5^{(1)})) \odot (Y_3^{(1)} \oplus Y_6^{(1)}))) \,. \qquad (58)$$

$$\mathrm{lsb}_1(v_2 \oplus w_2) = \mathrm{lsb}_1(((X_1^{(2)} \oplus X_2^{(2)}) \odot Z_7^{(2)} \boxplus (X_4^{(2)} \oplus X_3^{(2)})) \odot \\ (Z_8^{(2)} \boxplus ((X_1^{(2)} \oplus X_2^{(2)}) \odot Z_7^{(2)} \boxplus (X_4^{(2)} \oplus X_3^{(2)})) \odot (X_5^{(2)} \oplus Y_6^{(2)}))) \,. \qquad (59)$$

Expressions (57), (58) and (59) contain 10 $\odot$, 15 $\oplus$ and 6 $\boxplus$, which is equivalent to about 51 $\oplus$. This combination results in a one-bit condition to recover 161 key bits of information: $Z_i^{(1)}$, $1 \leq i \leq 8$, $Z_7^{(2)}$, $Z_8^{(2)}$, and $\mathrm{lsb}_1(Z_5^{(2)} \oplus Z_3^{(2)})$. The attack requirements are about 161 known plaintexts, and $\frac{51}{80} \cdot 2^{161} \approx 2^{160.3}$ 2-round MESH-96 computations of (57).

To attack 2.5-round MESH-96, consider the trails involving $(P_3, Y_3^{(3)})$,and $(P_5, Y_5^{(3)})$ in the graph of Fig. 3. The procedure is similar to the attack on 2 rounds, but involves 257 key bits of information: $Z_i^{(1)}$, $1 \leq i \leq 8$, $Z_7^{(2)}$, $Z_8^{(2)}$, $Z_i^{(3)}$, $1 \leq i \leq 6$, and $\mathrm{lsb}_1(Z_5^{(2)} \oplus Z_3^{(2)})$. That is more than an exhaustive key search effort.

2.3 The Biryukov-Demirci Attack on MESH-128

Similar attacks to the previous section can be applied on at most 2 rounds of MESH-128 [4], with an effort less than that of exhaustive key search.

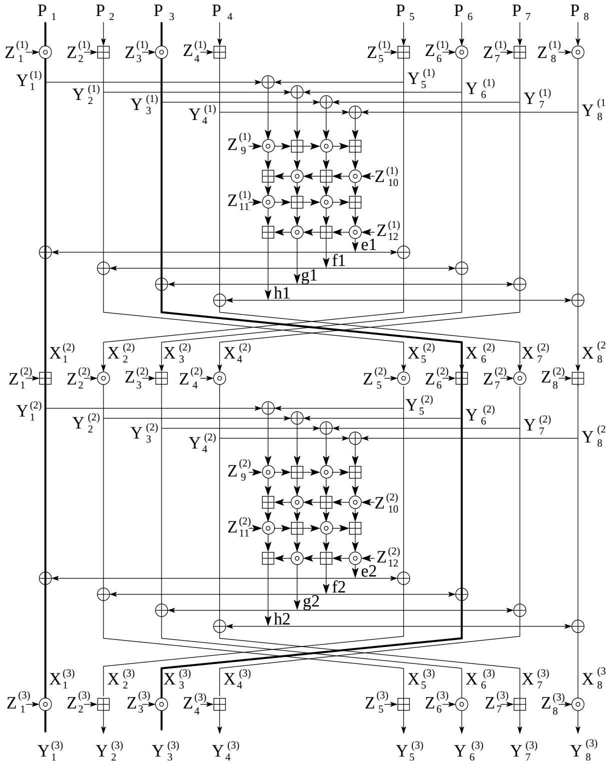


Fig. 4. The first 2.5 rounds of MESH-128.

To attack 1.5-round MESH-128, consider the trails involving $(P_1, Y_1^{(2)})$, $(P_3, Y_6^{(2)})$, $(P_6, Y_3^{(2)})$, and $(P_8, Y_8^{(2)})$ in the graph of Fig. 4.

$$\mathrm{lsb}_1(P_1 \odot Z_1^{(1)} \oplus e_1 \boxplus Z_1^{(2)}) = \mathrm{lsb}_1(Y_1^{(2)})\,, \tag{60}$$

$$\mathrm{lsb}_1(P_3 \odot Z_3^{(1)} \oplus g_1 \boxplus Z_6^{(2)}) = \mathrm{lsb}_1(Y_6^{(2)})\,, \tag{61}$$

$$\mathrm{lsb}_1(P_6 \odot Z_6^{(1)} \oplus f_1 \boxplus Z_3^{(2)}) = \mathrm{lsb}_1(Y_3^{(2)})\,, \tag{62}$$

$$\mathrm{lsb}_1(P_8 \odot Z_8^{(1)} \oplus h_1 \boxplus Z_8^{(2)}) = \mathrm{lsb}_1(Y_8^{(2)})\,. \tag{63}$$

Combining (60), (61), (62), and (63) results in:

$$\begin{gathered}\mathrm{lsb}_1(P_1 \odot Z_1^{(1)} \oplus P_3 \odot Z_3^{(1)} \oplus P_6 \odot Z_6^{(1)} \oplus P_8 \odot Z_8^{(1)} \oplus Z_1^{(2)} \oplus \\ Y_1^{(2)} \oplus Z_6^{(2)} \oplus Y_6^{(2)} \oplus Z_3^{(2)} \oplus Y_3^{(2)} \oplus Z_8^{(2)} \oplus Y_8^{(2)}) = \\ \mathrm{lsb}_1(h_1 \oplus g_1) \oplus \mathrm{lsb}_1(e_1 \oplus f_1)\,.\end{gathered} \tag{64}$$

The right-hand side of (64) depends on P_i, and $Z_j^{(1)}$, $1 \leq i \leq 8$, $1 \leq j \leq 11$. The combination of (60), (61), (62), (63), and (64) involves 23 $\odot$, 17 $\boxplus$

and 15 $\oplus$, which is equivalent to about 75 $\oplus$. In total, (64) provides a one-bit condition to recover 177 key bits of information: $Z_i^{(1)}$, $1 \leq i \leq 11$, and $\mathrm{lsb}_1(Z_1^{(2)} \oplus Z_3^{(2)} \oplus Z_6^{(2)} \oplus Z_8^{(2)})$. The attack requirements are about 177 known plaintexts and $\frac{91}{76} \cdot 2^{177} \approx 2^{177.3}$ 1.5-round MESH-128 computations.

To attack 2-round MESH-128, consider the extended trails used previously for 1.5 rounds (Fig.4):

$$\mathrm{lsb}_1(g_2 \oplus h_2) \oplus \mathrm{lsb}_1(f_1 \oplus h_1) = \mathrm{lsb}_1(X_6^{(3)} \oplus (Z_3^{(2)} \boxplus P_6 \odot Z_6^{(1)}) \oplus X_8^{(3)} \oplus (Z_8^{(2)} \boxplus (P_8 \odot Z_8^{(2)}))) \,, \tag{65}$$

$$\mathrm{lsb}_1(e_2 \oplus f_2) \oplus \mathrm{lsb}_1(e_1 \oplus g_1) = \mathrm{lsb}_1(X_1^{(3)} \oplus (Z_1^{(2)} \boxplus P_1 \odot Z_1^{(1)}) \oplus X_3^{(3)} \oplus (Z_6^{(2)} \boxplus (P_3 \odot Z_3^{(1)}))) \,. \tag{66}$$

The left-hand sides of (65) and (66) depend on P_i, $1 \leq i \leq 8$, $X_i^{(3)}$, $1 \leq j \leq 8$, $Z_l^{(1)}$, $1 \leq l \leq 11$ and $Z_9^{(2)}$, $Z_{10}^{(2)}$, $Z_{11}^{(2)}$, $\mathrm{lsb}_1(Z_1^{(2)} \oplus Z_3^{(2)} \oplus Z_6^{(2)} \oplus Z_8^{(2)})$. The combination of (65) and (66) contain 25 $\odot$, 26 $\boxplus$ and 30 $\oplus$, which is equivalent to about 126 $\oplus$. In total, the attack requirements are about 225 known plaintexts and $\frac{126}{120} \cdot 2^{225} \approx 2^{225}$ 2-round MESH-128 computations.

To attack 2.5-round MESH-128, consider the extended trails used previously for 2 rounds (Fig.4):

$$\mathrm{lsb}_1(g_2 \oplus h_2) \oplus \mathrm{lsb}_1(f_1 \oplus h_1) = \mathrm{lsb}_1(Y_6^{(3)} \odot (Z_6^{(3)})^{-1} \oplus (Z_3^{(2)} \boxplus P_6 \odot Z_6^{(1)}) \oplus Y_8^{(3)} \odot (Z_8^{(3)})^{-1} \oplus (Z_8^{(2)} \boxplus (P_8 \odot Z_8^{(2)}))) \,, \tag{67}$$

$$\mathrm{lsb}_1(e_2 \oplus f_2) \oplus \mathrm{lsb}_1(e_1 \oplus g_1) = \mathrm{lsb}_1(Y_1^{(3)} \odot (Z_1^{(3)})^{-1} \oplus (Z_1^{(2)} \boxplus P_1 \odot Z_1^{(1)}) \oplus Y_3^{(3)} \odot (Z_3^{(3)})^{-1} \oplus (Z_6^{(2)} \boxplus (P_3 \odot Z_3^{(1)}))) \,. \tag{68}$$

The exclusive-or combination of (67) and (68) depends on P_i, $1 \leq i \leq 8$, $Z_j^{(1)}$, $1 \leq j \leq 11$, $Z_9^{(2)}$, $Z_{10}^{(2)}$, $Z_{11}^{(2)}$, and $Z_l^{(3)}$, $1 \leq l \leq 8$ and $\mathrm{lsb}_1(Z_1^{(2)} \oplus Z_3^{(2)} \oplus Z_6^{(2)} \oplus Z_8^{(2)})$. In total, the attack requirements are about 16*22=352 known plaintexts and 2^{352} computations of the exclusive-or of (67) and (68), which is more than the effort for an exhaustive key search.

3 Conclusion

This report presented an attack on reduced-round IDEA block ciphers, based on an observation by Alex Biryukov, and an attack by Demirci [1]. Table 1 contains a summary of the attack complexities for IDEA and MESH some ciphers.

Even though the attacks on IDEA started from the first round, further analysis indicated that starting the attack at the 5th round would also require the same complexity, and both are the lowest possible values, taking into account the key overlapping property in the key schedule of IDEA.

Table 1. Attack complexitites for IDEA and some MESH ciphers.

Cipher	Block Size	Key Size	# Rounds	Data (KP)	Memory	Time
IDEA	64	128	1.5	33	33	2^{32}
			2.5	90	90	2^{89}
			3.5	112	112	2^{112}
			4	114	114	2^{114}
MESH-64	64	128	1.5	97	97	2^{97}
			2	128	128	2^{127}
MESH-96	96	192	1.5	65	65	$2^{64.3}$
			2	161	161	$2^{160.3}$
MESH-128	128	256	1.5	177	177	$2^{177.3}$
			2	225	225	2^{225}

References

1. H. Demirci. Square-like Attacks on Reduced Rounds of IDEA. In K. Nyberg and H. Heys, editors, *9th Selected Areas in Cryptography Workshop, SAC'02*, LNCS 2595, pages 147–159, Aug 2002.
2. X. Lai. *On the Design and Security of Block Ciphers*, volume 1 of *ETH Series in Information Processing.* Hartung-Gorre Verlag, Konstanz, 1995. J.L. Massey.
3. X. Lai, J.L. Massey, and S. Murphy. Markov Ciphers and Differential Cryptanalysis. In D.W. Davies, editor, *Advances in Cryptology, Eurocrypt'91*, LNCS 547, pages 17–38. Springer-Verlag, 1991.
4. J. Nakahara, Jr, V. Rijmen, B. Preneel, and J. Vandewalle. The MESH Block Ciphers. COSIC Tech Report, 2002.