Cryptanalysis of reduced-round MIBS Block Cipher

Aslı Bay, Jorge Nakahara Jr*, and Serge Vaudenay

EPFL, Switzerland
{asli.bay, jorge.nakahara, serge.vaudenay}@epfl.ch

Abstract. This paper presents the first independent and systematic linear, differential and impossible-differential (ID) cryptanalyses of MIBS, a lightweight block cipher aimed at constrained devices such as RFID tags and sensor networks. Our contributions include linear attacks on up to 18-round MIBS, and the first ciphertext-only attacks on 13-round MIBS. Our differential analysis reaches 14 rounds, and our impossible-differential attack reaches 12 rounds. These attacks do not threaten the full 32-round MIBS, but significantly reduce its margin of security by more than 50%. One fact that attracted our attention is the striking similarity of the round function of MIBS with that of the Camellia block cipher. We actually used this fact in our ID attacks. We hope further similarities will help build better attacks for Camellia as well.

Keywords: cryptanalysis, lightweight block ciphers, RFID tags, sensor networks

1 Introduction

This paper describes the first independent and systematic linear, differential and impossible-differential cryptanalyses on reduced-round variants of the MIBS block cipher. MIBS is a lightweight cipher, with a Feistel structure, aimed at ubiquitous but constrained environments, such as RFID tags and sensor networks [6]. MIBS operates on 64-bit blocks, uses keys of 64 or 80 bits and iterates 32 rounds. There is a striking similarity between the round functions of MIBS and Camellia ciphers [1]. This feature was actually exploited in our impossible-differential analysis of MIBS in Sect.5. Our results are summarized in Table 6.

Previous cryptanalytic results on MIBS, presented by its designers, concerned differential and linear relations on up to 4-round MIBS. Nonetheless, no full attacks were ever detailed. We provide better distinguishers and attacks on up to 18 rounds, effectively reducing the margin of security of MIBS by more than 50% as originally predicted by its designers.

* This work was supported by the National Competence Center in Research on Mobile Information and Communication Systems (NCCR-MICS), a center of the Swiss National Science Foundation under grant number 5005-67322.

This paper is organized as follows: Sect. 2 describes the main components of MIBS relevant for the attacks in this paper; Sect. 3 details linear relations and attacks on reduced-round versions of MIBS; Sect. 4 presents differential characteristics and attacks; Sect. 5 presents impossible-differential distinguishers and attacks; Sect. 6 concludes this paper.

2 A Brief Description of MIBS

MIBS is a block cipher following a Feistel Network design [6]. MIBS operates on 64-bit blocks, uses keys of 64 or 80 bits, and iterates 32 rounds for both key sizes. All internal operations in MIBS are nibble-wise, that is, on 4-bit words. The round function F of MIBS has an SPN structure composed of an xor layer with a round subkey, an S layer of 4×4-bit S-boxes, and a linear transformation layer (with branch number 5), in this order.

For our attack purposes, the linear transformation (P layer) is most relevant. Let $(y_1, y_2, y_3, y_4, y_5, y_6, y_7, y_8)$ denote the input to this layer. Its output, (y'_1, y'_2, y'_3, y'_4, y'_5, y'_6, y'_7, y'_8), can be described as

$$\begin{aligned} y'_1 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8; & y'_2 &= y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7; \\ y'_3 &= y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8; & y'_4 &= y_2 \oplus y_3 \oplus y_4 \oplus y_7 \oplus y_8; \\ y'_5 &= y_1 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_8; & y'_6 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6; \\ y'_7 &= y_1 \oplus y_1 \oplus y_3 \oplus y_6 \oplus y_7; & y'_8 &= y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8, \end{aligned} \qquad (1)$$

where $\oplus$ denotes exclusive or.

The input text block to the i-th round is denoted (L_{i-1}, R_{i-1}), with $L_i, R_i \in \{0,1\}^{32}$, and $(R_{i-1} \oplus F(K_i, L_{i-1}), L_{i-1})$ denotes the round output. (L_0, R_0) denotes a plaintext block.

The key schedule of MIBS is adapted from the key schedule of PRESENT [4]. There are two versions of key schedule of MIBS, both generating 32-bit round subkeys K_i for $1 \leq i \leq 32$, from 64-bit and 80-bit user keys, respectively. Let $state^i$ denote the ith round key state; $state^0$ denote the user key. The 80-bit version of key schedule of MIBS, with bit numbering in right-to-left order from 1 to 80, is as follows:

```
for $i = 1$ to $i = 32$,
    $state^i = state^{i-1} \ggg 19$,
    $state^i = S[state^i[80 \sim 77]] \| S[state^i[76 \sim 73]] \| state^i[72 \sim 1]$,
    $state^i = state^i[80 \sim 20] \| state^i[19 \sim 15] \oplus$ Counter $\| state^i[14 \sim 1]$,
    $K_i = state^i[80 \sim 49]$.
```

where '$\ggg$' means bitwise right-rotation, '$\|$' means string concatenation, and '$\sim$' indicates a sequence of bit positions. We refer to [6] for further details about MIBS components.

3 Linear Cryptanalysis

In [6], the designers claimed security of MIBS against linear cryptanalysis by providing a 4-round linear relation with 7 active S-boxes, and overall bias 2^{-8}.

They assumed that this relation was iterative (although it was not) and claimed resistance of the full 32-round MIBS to linear attacks.

Firstly, we derived the linear approximation table (LAT) for[1] the 4×4 S-box of MIBS. See Table 7 in the appendix. We note that this S-box is linearly 4-uniform[2] (an analogous concept to that used in DC, Sect. 4). Thus, the highest bias is 2^{-2}. We have found a better 4-round linear relation, described in Table 1, with only six active S-boxes and bias 2^{-7}. The last pair of bit masks in Table 1 stand for the output masks after the swapping of half blocks in a round.

We denote the input mask to the i-th round as $(\Gamma L_{i-1}, \Gamma R_{i-1})$. The $(i+1)$-th round input mask is the i-th round output mask. Values subscripted by 'x' are in hexadecimal base.

Table 1. A 4-round linear relation for MIBS.

Round i	ΓL_{i-1}	ΓR_{i-1}	Number of active S-boxes	Bias
1	00600600$_x$	02202220$_x$	1	2^{-2}
2	02202220$_x$	00660600$_x$	2	2^{-3}
3	00660600$_x$	00202200$_x$	2	2^{-3}
4	00202200$_x$	60666600$_x$	1	2^{-2}
5	60666600$_x$	00002200$_x$	-	-

3.1 Searching for Linear Relations for MIBS

For a systematic linear analysis of MIBS, we automated the search procedure by creating a program to look for linear relations of MIBS according to the following criteria:

- focus on iterative linear relations, preferably;
- maximize the overall bias by minimizing the number of active S-boxes;
- use the fact that the S-box is linearly 4-uniform (Table 7);
- use the fact that the branch number of the P permutation in the F function of MIBS is 5 (which is claimed to be optimal)

Taking into account these criteria, the best result of our search is the 16-round linear relation with 30 active S-boxes and bias 2^{-31} in Table 2. From the LAT of MIBS, Table 7, there are six possible instantiations of this linear relation, that is, $(w, z) \in \{(2_x, 6_x), (6_x, 2_x), (4_x, e_x), (e_x, 4_x), (8_x, d_x), (d_x, 8_x)\}$, where we exploited the symmetry $w \overset{S-box}{\rightarrow} z$ and $z \overset{S-box}{\rightarrow} w$ (both with the same bias 2^{-2}). The last line of Table 2 accounts for the swapping between half blocks. The first 15 rounds of this distinguisher corresponds to the best 15-round linear relation (with 28 active S-boxes, and bias 2^{-29}) that will be used in a key-recovery attack in Sect. 3.2.

[1] The LAT of an S-box stands for a table containing an exhaustive enumeration of all linear approximations of the given S-box.

[2] It means that the largest entry in the LAT has value 4.

Table 2. A 16-round linear relation for MIBS.

Round i	ΓL_{i-1}	ΓR_{i-1}	Number of active S-boxes	Bias
1	$\mathtt{w000w0w0}_\mathtt{x}$	$\mathtt{00000000}_\mathtt{x}$	0	2^{-1}
2	$\mathtt{00000000}_\mathtt{x}$	$\mathtt{w000w0w0}_\mathtt{x}$	2	2^{-3}
3	$\mathtt{w000w0w0}_\mathtt{x}$	$\mathtt{z0000z00}_\mathtt{x}$	3	2^{-4}
4	$\mathtt{z0000z00}_\mathtt{x}$	$\mathtt{w000ww0w}_\mathtt{x}$	2	2^{-3}
5	$\mathtt{w000ww0w}_\mathtt{x}$	$\mathtt{z000zz0z}_\mathtt{x}$	2	2^{-3}
6	$\mathtt{z000zz0z}_\mathtt{x}$	$\mathtt{w0000w00}_\mathtt{x}$	3	2^{-4}
7	$\mathtt{w0000w00}_\mathtt{x}$	$\mathtt{z000z0z0}_\mathtt{x}$	2	2^{-3}
8	$\mathtt{z000z0z0}_\mathtt{x}$	$\mathtt{00000000}_\mathtt{x}$	0	2^{-1}
9	$\mathtt{00000000}_\mathtt{x}$	$\mathtt{z000z0z0}_\mathtt{x}$	2	2^{-3}
10	$\mathtt{z000z0z0}_\mathtt{x}$	$\mathtt{w0000w00}_\mathtt{x}$	3	2^{-4}
11	$\mathtt{w0000w00}_\mathtt{x}$	$\mathtt{z000zz0z}_\mathtt{x}$	2	2^{-3}
12	$\mathtt{z000zz0z}_\mathtt{x}$	$\mathtt{w000ww0w}_\mathtt{x}$	2	2^{-3}
13	$\mathtt{w000ww0w}_\mathtt{x}$	$\mathtt{z0000z00}_\mathtt{x}$	3	2^{-4}
14	$\mathtt{z0000z00}_\mathtt{x}$	$\mathtt{w000w0w0}_\mathtt{x}$	2	2^{-3}
15	$\mathtt{w000w0w0}_\mathtt{x}$	$\mathtt{00000000}_\mathtt{x}$	0	2^{-1}
16	$\mathtt{00000000}_\mathtt{x}$	$\mathtt{w000w0w0}_\mathtt{x}$	2	2^{-3}
17	$\mathtt{w000w0w0}_\mathtt{x}$	$\mathtt{z0000z00}_\mathtt{x}$	-	-

3.2 17-round Multiple Linear Attack

We proposed a key-recovery attack on 17-round MIBS by considering the first fifteen rounds of the linear distinguisher in Table 2, placed between rounds 2 and 16. We recover subkey bits from the first and last rounds.

The main relation for this 17-round attack is

$$(R_0 \oplus F(K_1, L_0)) \cdot \mathtt{w000w0w0_x} \oplus (L_{17} \oplus F(K_{17}, R_{17})) \cdot \mathtt{w000w0w0_x} = 0, \qquad (2)$$

where w is one of the values indicated in Sect. 3.1. Due to the low branch number of the P layer (see Sect. 2), only two subkey nibbles need to be guessed in both $F(K_1, L_0)$ and $F(K_{17}, R_0)$. See Fig. 1. Following [3], we use four variations of (2) for four values of w that lead to linearly independent relations: $w \in \{2_x, 4_x, 8_x, d_x\}$. According to [3], the combined bias of these multiple linear relations is $\sqrt{4 \cdot (2^{-29})^2} = 2^{-28}$. The data complexity is $4/(2^{-28})^2 = 2^{58}$ KP.

The attack procedure follows [7]:

- Take 2^{58} known plaintexts and request the corresponding ciphertexts encrypted under the unknown secret key K.
- for $w \in \{2_x, 4_x, 8_x, d_x\}$ keep independent counters for each possible value of subkey bits which correspond to active S-boxes: S_1 and S_6 in both rounds 1 and 17.
- For each possible key, check that $(R_0 \oplus F(K_1, L_0)) \cdot \mathtt{w000w0w0_x} \oplus (L_{17} \oplus F(K_{17}, R_{17})) \cdot \mathtt{w000w0w0_x} = 0$ holds, where, for instance, $w = 6$:
  For each key candidate K_i, let T_i^w be the number of plaintexts such that $(R_0 \oplus F(K_{1,1} \| K_{1,6}, L_0)) \cdot \mathtt{w000w0w0_x} \oplus (L_{17} \oplus F(K_{17,1} \| K_{17,6}, R_{17}) \oplus \mathtt{w000w0w0_x} = 0$ for each w. Let $T_{\max}^w$ be the maximal value and $T_{\min}^w$ be the minimal value of all T_i^w's, then
  - If $|T_{\max}^w - N/2| > |T_{\min}^w - N/2|$ then adopt the key candidate corresponding to $T_{\max}^w$

  - If $|T^w_{\min} - N/2| > |T^w_{\max} - N/2|$ then adopt the key candidate corresponding to $T^w_{\min}$, where $N = 2^{58}$ in this attack.
- the correct subkey is simultaneously suggested by the counters $T^w_{\max}$ or $T^w_{\min}$ corresponding to all four values of w.

According to the key schedule of MIBS, there is no overlapping between the subkeys $K_{1,1}$, $K_{1,6}$, $K_{17,1}$, $K_{17,6}$. Thus, the time complexity becomes $\frac{2^{16}}{2 \cdot 17} \cdot 2^{58} \approx 2^{69}$ 17-round MIBS encryptions because partial decryption of two nibbles in the first round and two other nibbles in the 17th round costs about half a round. The memory complexity is the 2^{58} blocks. The remaining 64 key bits can be recovered by exhaustive search without affecting the overall attack complexity. Following [9], the success probability of this attack, p_S, is computed assuming $N \cdot |p - 1/2|^2 = 4$, and $a = 8$

$$p_S = \Phi(2 \cdot \sqrt{N} \cdot |p - 1/2| - \Phi^{-1}(1 - 2^{-a-1})) \approx 0.9794$$

where Φ is the cumulative distribution function of the standard normal distribution.

3.3 Ciphertext-Only Attack

Assuming the input plaintext is coded as ASCII text, we can perform a ciphertext-only attack. In this setting though, the codebook size is reduced to $2^{64-8} = 2^{56}$, since the most significant bit of every byte is zero. We use the first 13 rounds of (Table 2), which imply the following linear relation: $L_0 \cdot \texttt{80008080}_\texttt{x} \oplus L_{17} \cdot \texttt{e0000e00}_\texttt{x} \oplus R_{17} \cdot \texttt{80008080}_\texttt{x} = 0$, with bias 2^{-27}. We perform a distinguish-from-random attack, using $2 \cdot (2^{-27})^{-2} = 2^{55}$ CO, and equivalent number of encryptions. The memory complexity is negligible. According to [7], assuming Matsui's algorithm 1, the success probability of this distinguishing attack is about 97.7%.

3.4 18-round Linear Attack

We can use the full 16-round relation in Table 2 with bias 2^{-31} for a key-recovery attack on 18-round MIBS. The attack procedure is similar to the one in Sect. 3.2, but this time we recover $K_{1,1}$, $K_{1,6}$, $K_{18,6}$, $K_{18,7}$, $K_{18,8}$. We found no overlapping in these subkeys, so we recover 20 subkey bits in total. The linear relations for this attack is

$$(R_0 \oplus R_{18} \oplus F(K_1, L_0)) \cdot \texttt{w000w0w0}_\texttt{x} \oplus (L_{18} \oplus F(K_{18}, R_{18})) \cdot \texttt{z0000z00}_\texttt{x} = 0, \quad (3)$$

For each pair (w, z) in Sect. 3.1 we have an independent linear relation. Following [3], the combined bias of these multiple linear relations is $\sqrt{6 \cdot (2^{-31})^2} = 2^{-29.7}$. The data complexity is $3/(2^{-29.7})^2 = 2^{60.98}$ KP.

The time complexity is $2^{20} \cdot 2^{60.98} \cdot 5/8 \cdot 1/18 \approx 2^{76.13}$ 18-round computations, since partial decryption of two nibble in the first round, and three nibbles in the 18th round costs less than one-round computation. Memory complexity is the same as data complexity. According to [9], the success probability of this attack is 72.14%.

4 Differential Cryptanalysis

Differential cryptanalysis (DC) was originally proposed by Biham and Shamir in [2]. In [6], the designers claim security of MIBS against DC by providing a 4-round characteristic with six active S-boxes, and probability 2^{-15}. They assumed that this characteristic was iterative (although it is not) and claimed resistance of the full 32-round MIBS to DC.

4.1 Searching for Differential Characteristics of MIBS

We have computed the difference distribution table (DDT) for[3] the 4×4 S-box of MIBS. See Table 8 in the appendix. We note that this S-box is differentially 4-uniform[4]. So, the highest probability for any difference propagation across this S-box is 2^{-2}.

For a systematic differential analysis of MIBS, we automated the search for differential characteristics by creating a program to look for differential characteristics for MIBS according to the following criteria:

(a) focus on iterative characteristics, preferably;
(b) maximize the overall probability by minimizing the number of active S-boxes;
(c) use the fact that the S-box is differentially 4-uniform (Table 8) [8];
(d) use the fact that the branch number of the P permutation in the F function of MIBS is 5

Using these criteria, we have found two 12-round differential characteristics, both with probability 2^{-56}. These characteristics have 28 active S-boxes in total, and for each S-box we chose the largest entries in the DDT. One characteristic is detailed in Table 3. The other characteristic is obtained from Table 3 by turning it upside-down (due to the symmetry of the Feistel Network scheme).

4.2 13-round Differential Attack

We perform a key-recovery attack on 13-round MIBS by placing the 12-round characteristic in Table 3 in rounds 1 up to 12. We recover 24 subkey bits from the 13th round. The attack procedure is as follows:

(a) take $c \cdot 2^{56}$ pairs of plaintext blocks P_i and P_j which satisfy $P_i \oplus P_j =$ ($\texttt{EEE0E0EE}_\texttt{x}$, $\texttt{50500550}_\texttt{x}$) and obtain their corresponding ciphertexts $C_i = (L^i_{13}, R^i_{13})$ and $C_j = (L^j_{13}, R^j_{13})$;
(b) keep counters for each possible value of six subkey nibbles of K_{13} corresponding to the six E_x nibble differences in the right half of the ciphertext, namely $K_{13,1}$, $K_{13,2}$, $K_{13,3}$, $K_{13,5}$, $K_{13,7}$ and $K_{13,8}$;
(c) keep only those text pairs for which the right half of the ciphertext difference equals $\texttt{EEE0E0EE}_\texttt{x}$;

[3] The DDT of an S-box stands for a table containing an exhaustive enumeration of all pairs of input/output differences for the given S-box.

[4] It means that the largest entry in the DDT has value 4.

Table 3. A 12-round differential characteristic for MIBS.

Round i	ΔL_{i-1}	ΔR_{i-1}	Number of active S-boxes	Probability
1	EEE0E0EE$_x$	50500550$_x$	6	2^{-12}
2	00000050$_x$	EEE0E0EE$_x$	1	2^{-2}
3	00EEE000$_x$	00000050$_x$	3	2^{-6}
4	05005000$_x$	00EEE000$_x$	2	2^{-4}
5	00E000E0$_x$	05005000$_x$	2	2^{-4}
6	55500000$_x$	00E000E0$_x$	3	2^{-6}
7	00000000$_x$	55500000$_x$	0	1
8	55500000$_x$	00000000$_x$	3	2^{-6}
9	00E000E0$_x$	55500000$_x$	2	2^{-4}
10	05005000$_x$	00E000E0$_x$	2	2^{-4}
11	00EEE000$_x$	05005000$_x$	3	2^{-6}
12	00000050$_x$	00EEE000$_x$	1	2^{-2}
13	EEE0E0EE$_x$	00000050$_x$	-	-

(d) for each plaintext pair with indices i, j, compute $P^{-1}(L^i_{13} \oplus L^j_{13} \oplus \texttt{00000050}_{\texttt{x}})$, and compare with the output difference of the S-box layer inside $F(K_{13}, R^i_{13})$ $\oplus$ $F(K_{13}, R^j_{13})$; discard the pairs that do not match one of the seven possible output differences of the S-box, according to the DDT (Table 8) with input difference E_x; from the input difference to the 13th round, increment counters corresponding to each suggested 24 subkey bits by the input difference $\texttt{EEE0E0EE}_{\texttt{x}}$, and $P^{-1}(L^i_{13} \oplus L^j_{13} \oplus \texttt{00000050}_{\texttt{x}})$;

Following [2], we estimate the signal-to-noise ratio (SNR), as $2^{24} \cdot 2^{-56}/(1 \cdot 2^{-32} \cdot (7/15)^6 \cdot (2^{-4})^2) = 2^{14}$, since $p = 2^{-56}$, $k = 24$, $\alpha = 1$ (we expect one subkey on average to be suggested in step (d)), $\beta = 2^{-32} \cdot (7/15)^6 \cdot (2^{-4})^2$, since $\Delta R_{13} = \texttt{EEE0E0EE}_{\texttt{x}}$ gives a 32-bit condition, every output difference to an S-box whose input difference is E_x can have only seven possible nonzero output differences, and the two S-boxes with input difference 0 can only have 0 output difference. We estimate about $c = 32$ right pairs to uniquely determine the correct subkey values. This means 2^{61} CP. Step (c) imposes a 32-bit condition on the pairs. So, about $2^{61}/2^{32} = 2^{29}$ pairs survive. In step (d), the complexity corresponds to $2 \cdot 2^{29}$ one-round computations. This corresponds to about $2^{30}/13 \approx 2^{26.3}$ 13-round computations. The memory complexity corresponds to 2^{24} counters. If the user key has 64 bits, the remaining 40 key bits requires 2^{40} 13-round computations; if the key is 80-bit long, then the remaining 56 key bits requires 2^{56} 13-round computations.

According to [9], the success probability p_S of this attack, for SNR $= 2^{14}$, $a = 7$ (i.e. assuming we expect the correct 24-bit subkey to be ranked among the 7 highest counters), $N = 2^{61}$ CP, $p = 2^{-56}$, is

$$p_S = \Phi(\frac{\sqrt{p \cdot N \cdot SNR} - \Phi^{-1}(1 - 2^{-a})}{\sqrt{SNR + 1}}) \approx 0.9999$$

4.3 14-round Differential Attack

For 14-round MIBS, we studied a key-recovery attack by placing the 12-round characteristic in Table 3 between rounds 2 and 13. We recover subkey bits from K_1 and K_{14} at the same time. The attack procedure is as follows:

(a) consider m structures of plaintexts, such that R_0 contains all possible 32-bit values, but in the L_0, half of the text contain arbitrary 32-bit values, and half of them contain $L_0 \oplus \texttt{50500550}_\texttt{x}$. Each structure, thus, contain $2^{32} \cdot 2^{32} = 2^{64}$ pairs with which difference $(\texttt{50500550}_\texttt{x}, \Delta R_0)$, where ΔR_0 is a nonzero 32-bit difference;

(b) keep only those text pairs for which the right half of the ciphertext difference equals $\texttt{EEE0E0EE}_\texttt{x}$;

(c) prepare counters for each possible value of four subkey nibbles of K_1 corresponding to the four 5_x nibble differences in the left half of the plaintext, namely $K_{1,1}$, $K_{1,3}$, $K_{1,6}$ and $K_{1,7}$, and each of the six nibbles of K_{14} corresponding to the six E_x nibble differences in the right half of the ciphertext; this corresponds to 40 subkey bits;

(d) for each pair of plaintext with indices i, j, compute $P^{-1}(R_0^i \oplus R_0^j \oplus \texttt{EEE0E0EE}_\texttt{x})$, and compare it with the output difference of the S-box layer inside $F(K_1, L_0^i)$ $\oplus$ $F(K_1, L_0^j)$; discard the pairs that do not match one of the seven possible output differences of the S-box layer, according to the DDT (Table 8) with input difference 5_x; also, the S-boxes with input difference 0 can only have 0 output difference; from the input difference to the 1st round, increment counters corresponding to each suggested 16 subkey bits by the input difference $\texttt{50500550}_\texttt{x}$, and $P^{-1}(R_0^i \oplus R_0^j \oplus \texttt{EEE0E0EE}_\texttt{x})$;

(e) analogously, compute $P^{-1}(L_{14}^i \oplus L_{14}^j \oplus \texttt{00000050}_\texttt{x})$, and compare it with the output difference of the S-box layer inside $F(K_{14}, R_{14}^i) \oplus F(K_{14}, R_{14}^j)$; discard the pairs that do not match one of the seven possible output differences of the S-box, according to the DDT (Table 8) with input difference E_x; also, the S-boxes with input difference 0 can only have 0 output difference; from the input difference to the 14th round, increment counters corresponding to each suggested 24 subkey bits by the input difference $\texttt{EEE0E0EE}_\texttt{x}$, and $P^{-1}(L_{14}^i \oplus L_{14}^j \oplus \texttt{00000050}_\texttt{x})$;

Following [2], we estimate the signal-to-noise ratio (SNR), as $2^{40} \cdot 2^{-56}/(1 \cdot 2^{-32} \cdot (7/15)^4 \cdot (2^{-4})^4 \cdot (7/15)^6 \cdot (2^{-4})^2) = 2^{50}$, since $p = 2^{-56}$, $k = 40$, $\alpha = 1$ (we expect one subkey on average to be suggested in steps (d) and (e)), $\beta = 2^{-32} \cdot (7/15)^4 \cdot (2^{-4})^4 \cdot (7/15)^6 \cdot (2^{-4})^2$, since $\Delta R_{14} = \texttt{EEE0E0EE}_\texttt{x}$ gives a 32-bit condition, every output difference to an S-box whose input difference is 5_x or E_x can have only seven possible nonzero output differences, and the S-boxes with input difference 0 can only have 0 output difference. We estimate about $m = 128$ structures to determine the correct subkey values. This means $2^{7+33} = 2^{40}$ CP. Step (c) imposes a 32-bit condition on the pairs. So, about $2^{7+64}/2^{32} = 2^{39}$ pairs survive. In step (d), the complexity corresponds to $2 \cdot 2^{39}$ one-round computations. The same holds in step (e). This corresponds to about $2^{41}/14 \approx 2^{37.2}$ 14-round computations. The memory complexity corresponds to 2^{40} counters. If the user key has 64 bits, the remaining 24 key bits requires 2^{24} 14-round computations; if the key is 80-bit long, then the remaining 40 key bits requires 2^{40} 14-round computations.

According to [9], the success probability p_S of this attack, for SNR = 2^{50}, $a = 8$ (i.e. assuming we expect the correct 40-bit subkey to be ranked among the 8 highest counters), $N = 2^{40}$ CP, $p = 2^{-56}$, is

$$p_S = \Phi(\frac{\sqrt{p \cdot N \cdot SNR} - \Phi^{-1}(1-2^{-a})}{\sqrt{SNR+1}}) \approx 0.5015$$

5 Impossible-Differential Cryptanalysis

There is a striking similarity between the round functions of MIBS and Camellia [1] block ciphers. Therefore, inspired by the impossible differential attack on Camellia, proposed by Wu *et al.* in [11], we have constructed a similar 8-round impossible differential for MIBS, as the one built for Camellia proposed in [10]. Then, we use this 8-round impossible differential to attack 12-round MIBS.

We have found the following 8-round impossible differential for MIBS:

$$(\mathtt{00000000_x}, \mathtt{000000s0_x}) \overset{8r}{\not\rightarrow} (\mathtt{0000h000_x}, \mathtt{00000000_x}). \qquad (4)$$

where u and v are nonzero nibble differences, and the broken arrow indicates that the difference in the left hand side does not cause the difference in the right hand side.

We have also found another 8-round impossible differential distinguisher for MIBS: $(\mathtt{00000000_x}, \mathtt{00s00000_x}) \overset{8r}{\not\rightarrow} (\mathtt{0000000h_x}, \mathtt{00000000_x})$.

5.1 Some Properties of MIBS for 80-bit user key

We have exploited two properties of MIBS to use in the attack:

Property 1. *Let $K_i = (K_{i,1}, K_{i,2}, \ldots, K_{i,8})$ denote the i-th round subkey, where $K_{i,1}$ is the most significant nibble. Then, K_1 and K_2 share 13 bits in common: $K_1[1 \sim 13] = K_2[20 \sim 32]$ or $K_{1,1}\|K_{1,2}\|K_{1,3}\|K_{1,4}[1] = K_{2,5}[4]\|K_{2,6}\|K_{2,7}\|K_{2,8}$ where values inside square brackets index bit positions.*

Property 2. *(similar to [5]) For any 32-bit strings X, X^*, if there exists a nonzero nibble difference s such that $P^{-1}(X \oplus X^* \oplus \mathtt{000000s0_x})$ is of the form $\mathtt{??0?00??_x}$, then s is unique (? denotes any nibble value). The same holds for a nonzero nibble difference h.*

Proof. Suppose there are two nibble differences s and w that satisfy this property. Then, P is a linear transformation relative to xor, $P^{-1}(X \oplus X^* \oplus \mathtt{000000s0_x})$ $\oplus$ $P^{-1}(X \oplus X^* \oplus \mathtt{000000w0_x}) = P^{-1}(\mathtt{000000s0_x}) \oplus P^{-1}(\mathtt{000000w0_x})$ and has the form $\mathtt{??0?00??_x}$. But, $P^{-1}(\mathtt{000000s0_x}) \oplus P^{-1}(\mathtt{000000w0_x}) = \mathtt{ss0ss0ss_x} \oplus \mathtt{ww0ww0ww_x}$. From the fifth nibble position, it follows that $s \oplus w = 0$, which is a contradiction.

5.2 Construction of 8-round Impossible Differential Distinguisher

This 8-round impossible differential characteristic (4) is constructed by concatenating two 3-round differentials, and putting two connection rounds in between the two differentials. See Fig. 4. The first 3-round differential, depicted in Table 4, is built as follows: let the input difference to the first round be $(\Delta L_0, \Delta R_0) = (\texttt{00000000}_\texttt{x}, \texttt{000000s0}_\texttt{x})$ where s is a non-zero nibble difference and after the first round, the input difference to the second round will be $(\Delta L_1, \Delta R_1) = (\texttt{000000s0}_\texttt{x},\ \texttt{00000000}_\texttt{x})$. Then in the second round, the input difference $\texttt{000000s0}_\texttt{x}$ to the S layer leads to the output difference $\texttt{000000t0}_\texttt{x}$, where t is a nonzero nibble difference. After applying the P layer, the output difference of the F-function will be $\texttt{tt0t00tt}_\texttt{x}$. The input difference to the third round is $(\Delta L_2, \Delta R_2) = (\texttt{tt0t00tt}_\texttt{x},\ \texttt{000000s0}_\texttt{x})$. Afterwards, the difference $\Delta L_2 = \texttt{tt0t00tt}_\texttt{x}$ becomes $t_1t_20t_400t_7t_8$ after the S layer where t_1, t_2, t_4, t_7 and t_8 are non-zero nibble differences. Then, it evolves to $(c_1c_2c_3c_4c_5c_6c_7c_8)$, c_i are nonzero nibble differences, after the application of the P layer, and the output difference of the third round turns out to be $(\Delta L_3, \Delta R_3) = (c_1c_2c_3c_4c_5c_6c_7c_8 \oplus \texttt{000000s0}_\texttt{x}, \texttt{tt0t00tt}_\texttt{x})$. This completes the first differential.

Table 4. The first 3-round truncated differential for MIBS (in encryption direction).

Round i	ΔL_{i-1}	ΔR_{i-1}
1	$\texttt{00000000}_\texttt{x}$	$\texttt{000000s0}_\texttt{x}$
2	$\texttt{000000s0}_\texttt{x}$	$\texttt{00000000}_\texttt{x}$
3	$\texttt{tt0t00tt}_\texttt{x}$	$\texttt{000000s0}_\texttt{x}$
4	$c_1c_2c_3c_4c_5c_6c_7c_8 \oplus \texttt{000000s0}_\texttt{x}$	$\texttt{tt0t00tt}_\texttt{x}$

The second 3-round differential in Table 5 is constructed as follows: let the output difference of round 8 be $(\Delta L_8, \Delta R_8) = (\texttt{0000h000}_\texttt{x}, \texttt{00000000}_\texttt{x})$ and if this difference is rolled back through round 8, then the output difference of round 7 becomes $(\Delta L_7, \Delta R_7) = (\texttt{00000000}_\texttt{x}, \texttt{0000h000}_\texttt{x})$. The difference $\Delta L_7 = \texttt{0000h000}_\texttt{x}$ will be $\texttt{0000w000}_\texttt{x}$ after the application of the S layer in round 7 and the difference evolves to $\texttt{www0ww00}_\texttt{x}$ after the P layer where w denotes a nonzero nibble. Then, the output difference of round six becomes $(\Delta L_6, \Delta R_6) = (\texttt{www0ww00}_\texttt{x},\ \texttt{0000h000}_\texttt{x})$ becomes $w_1w_2w_30w_5w_600$, where w_i are *nonzero nibble differences*, after the S layer and we get the input difference of round six as $(\Delta L_5, \Delta R_5) = (e_1e_2e_3e_4e_5e_6e_7e_8 \oplus \texttt{0000h000}_\texttt{x}, \texttt{www0ww00}_\texttt{x})$. This completes the second 3-round differential.

Concatenating these two 3-round differentials, we obtain an 8-round impossible differential distinguisher. One can see in Fig. 4, the input and output differences of the F-function in round 5 are $(e_1e_2e_3e_4e_5e_6e_7e_8) \oplus \texttt{0000h000}_\texttt{x}$ and $(c_1c_2c_3c_4c_5c_6c_7c_8) \oplus \texttt{000000s0}_\texttt{x} \oplus \texttt{www0ww00}_\texttt{x} = (c_1 \oplus w, c_2 \oplus w, c_3 \oplus w, c_4, c_5 \oplus w, c_6 \oplus w, c_7 \oplus s, c_8)$, respectively. Since the output difference of the S layer has to be equal to input difference of the P layer, that is, $S[(e_1e_2e_3e_4e_5e_6e_7e_8) \oplus$

Table 5. The second 3-round truncated differential for MIBS (in decryption direction).

Round i	ΔL_{i-1}	ΔR_{i-1}
8	$\mathtt{0000h000_x}$	$\mathtt{00000000_x}$
7	$\mathtt{00000000_x}$	$\mathtt{0000h000_x}$
6	$\mathtt{0000h000_x}$	$\mathtt{www0ww00_x}$
5	$\mathtt{www0ww00_x}$	$e_1e_2e_3e_4e_5e_6e_7e_8 \oplus \mathtt{0000h000_x}$

$\mathtt{0000h000_x}] = P^{-1}(c_1 \oplus w, c_2 \oplus w, c_3 \oplus w, c_4, c_5 \oplus w, c_6 \oplus w, c_7 \oplus s, c_8)$, we have: $P^{-1}(c_1 \oplus w, c_2 \oplus w, c_3 \oplus w, c_4, c_5 \oplus w, c_6 \oplus w, c_7 \oplus s, c_8)= P^{-1}(c_1c_2c_3c_4c_5c_6c_7c_8) \oplus P^{-1}(\mathtt{000000s0_x}) \oplus P^{-1}(\mathtt{www0ww00_x})= (t_1t_20t_400t_7t_8) \oplus \mathtt{ss0ss0ss_x} \oplus \mathtt{0000w000_x} = (t_1 \oplus s, t_2 \oplus s, 0, t_4 \oplus s, s \oplus w, 0, t_7 \oplus s, t_8 \oplus s)$.

We can see that the output difference of the third and sixth S-boxes are zero in round five, which implies the input differences of these S-boxes are zero, too since they are bijective. Therefore, $e_3 = e_6 = 0$ where $e_3 = w_1 \oplus w_2 \oplus w_3 \oplus w_5 \oplus w_6$, $e_6 = w_1 \oplus w_2 \oplus w_5 \oplus w_6$. But, if $e_3 = w_1 \oplus w_2 \oplus w_3 \oplus w_5 \oplus w_6 = 0$ and $e_6 = w_1 \oplus w_2 \oplus w_5 \oplus w_6 = 0$, then this leads to $w_3 = 0$ which contradicts the assumption that w_3 is nonzero.

5.3 12-round Impossible Differential Attack on MIBS with 80-bit user key

Fig. 3 depicts our 12-round impossible differential attack. We start in round 1 and end in round 12. But it can be constructed anywhere between rounds 1 and 32 due to the key schedule of MIBS for 80-bit user keys. From Fig. 3, the required plaintexts for the attack have the form $(\Delta L_0, \Delta R_0) =(\mathtt{uu0u00uu_x}, P(\mathtt{??0?00??_x}) \oplus \mathtt{000000?0_x})$ where 'u' and '?' are nonzero nibble differences.

This attack is different from the conventional impossible differential attack in a way that we exploit the equality of some subkey bits to eliminate wrong key guesses by using the impossible differential. Instead of eliminating pairs round by round, we can make a different analysis to reduced the time complexity of the attack: the ciphertext pairs which satisfy the impossible differential should have the output difference of round 10: $\Delta L_{10} = (\mathtt{0000h000_x}, \mathtt{00000000_x})$, where h is a nonzero nibble. When the S-box of MIBS is analyzed, one can see that the number of nonzero entries of each row of the DDT is at most 2^3, that is each nonzero input difference to the S-box causes at most 2^3 nonzero output differences. Therefore, the nonzero nibble h can take $2^4 - 1 = 15$ different values and in round 11, the output differences of the S-box, which corresponds to h, has at most $15 \cdot 2^3$ possible nonzero output differences. Then in Round 12, five nonzero nibbles at positions $(1, 2, 3, 5, 6)$ have at most $(2^3)^5$ nonzero output differences which result in at most $15 \cdot 2^3 \cdot (2^3)^5 \approx 2^{22}$ possible output differences after the S layer.

The attack procedure is as follows:
Data Collection

Choose 2^m structures of plaintexts of each structure is of the form:

$$\begin{aligned} \Delta L_0 &= (uua_3ua_5a_6uu) \\ \Delta R_0 &= P(x_1x_2b_3x_4b_5b_6x_7x_8) \oplus (c_1c_2c_3c_4c_5c_6yc_8) \end{aligned}$$

where (a_i, b_j, c_j) are constants and (u, x_i, y) takes all possible nonzero values. So, each structure has $(2^4)^7 = 2^{28}$ plaintexts which constitute $\frac{1}{2} \cdot 2^{28} \cdot 2^{28} = 2^{55}$ plaintext pairs. Since we take 2^m structures, there are 2^{55+m} plaintexts pairs in total.

Data Filtering and Key Elimination

- The analysis that we made above shows that the probability of a random pair passes the test is $2^{-42} = 2^{22} \cdot 2^{-64}$, therefore after this filtering step $2^{55+m} \cdot 2^{22} \cdot 2^{-64} = 2^{13+m}$ pairs remain.
- For each remaining pair $((L_0, R_0), (L_{12}, R_{12}))$ and $((L_0^*, R_0^*), (L_{12}^*, R_{12}^*))$, do the following steps:
  1. By Property 2, there is only one nibble u which satisfies $P^{-1}(L_0 \oplus L_0^* \oplus \texttt{000000u0}_{\texttt{x}})$, and it has the form $\texttt{??0?00??}_{\texttt{x}}$. Therefore, for each pair of plaintexts compute $P^{-1}(L_0 \oplus L_0^* \oplus \texttt{000000u0}_{\texttt{x}})$ to find the unique value of u by trying all possible values of u. It is analogous to find the unique value of h.
  2. Afterwards, in rounds 1 and 12, since the input and output differences of the S-boxes are known, the subkey nibbles ($K_{1,1}$, $K_{1,2}$, $K_{1,4}$, $K_{1,7}$, $K_{1,8}$) and ($K_{12,1}$, $K_{12,2}$, $K_{12,3}$, $K_{12,5}$, $K_{12,6}$) are suggested with the help of the DDT.
  3. Guess further 24 subkey bits (6 nibbles) of rounds 1 and 12, namely, ($K_{1,3}$, $K_{1,5}$, $K_{1,6}$, $K_{12,4}$, $K_{12,7}$, $K_{12,8}$), then do the followings:
     (a) For every remaining pair, encrypt plaintexts through the first round, and decrypt their corresponding ciphertexts through the last round to obtain intermediate values (L_1, L_1^*) and (R_{11}, R_{11}^*), respectively.
     (b) Compute the suggested bits of the subkey nibbles $K_{2,7}$ and $K_{11,5}$ using the values L_1, L_1^*, u and $P^{-1}(L_0 \oplus L_0^*)$ for round 2 and R_{11}, R_{11}^*, h and $P^{-1}(R_{12} \oplus R_{12}^*)$ for round 12.
     (c) By Property 1, check the subkey nibbles satisfying the following relation $K_{2,7} = K_{1,2}[2 \sim 4] || K_{1,3}[1]$. This equality implies a 4-bit condition on pairs and any pair which satisfies the equality eliminates one wrong 68-bit subkey value: ($K_{1,1}$, $K_{1,2}$, $K_{1,4}$, $K_{1,7}$, $K_{1,8}$, $K_{12,1}$, $K_{12,2}$, $K_{12,3}$, $K_{12,5}$, $K_{12,6}$, $K_{1,3}$, $K_{1,5}$, $K_{1,6}$, $K_{12,4}$, $K_{12,7}$, $K_{12,8}$, $K_{11,5}$). Each pair eliminates 2^{-4} of all subkey guesses, so after the first pair the number of remaining keys is $2^{68}(1-2^{-4})$. Since we have 2^{13+m} pairs, there are $2^{68}(1-2^{-4})^{2^{13+m}}$ wrong subkeys. For $m = 0$, no wrong subkeys survive.

5.4 Complexity Analysis

Data Complexity: We set $m = 0$, because it is enough to take just one structure of plaintexts. So, the data complexity the attack is 2^{28} chosen plaintexts (CP).

Memory Access: In data filtering step, we have to have access to all 2^{22} output differences $(\Delta L_{12}, \mathtt{ggg0gg00_x})$ stored in a hash table to identify the useful pairs. Therefore, this step needs $2^{22} \cdot 2^{28} = 2^{50}$ memory access (MA). We approximate the cost of one round MIBS encryption to be equivalent to one memory access. Thus, 2^{50} memory accesses cost about $2^{46.42}$ 12-round MIBS encryptions.

Time complexity:

- Step 1 needs at most two one-round MIBS encryption per remaining pair. Therefore, the time complexity of this step is at most $2^{13} \cdot \dfrac{2}{12} \approx 2^{10.41}$ 12-round MIBS encryptions. We do not need to try all possible 15 values of a and h, since the computation is less than two round encryptions.
- The time complexity of Step 2 is less than $2^{13} \cdot \dfrac{2}{12} \approx 2^{10.41}$ 12-round MIBS encryptions. Because, for five active S-boxes, we use the DDT to find the suggested keys, which costs less than one round encryption.
- In Step 3(a), since we guess 24 bits of subkeys; the time complexity of this step is at most $2 \cdot 2^{13} \cdot 2^{24} \cdot \dfrac{2}{12} \approx 2^{35.42}$ 12-round MIBS encryptions. In Step 3(b), the time complexity is less than $2^{13} \cdot \dfrac{2}{12} \approx 2^{10.41}$ 12-round MIBS encryptions. Note that the complexity of checking 4-bit equality in subkeys is negligible.

Memory Complexity: The storage of all chosen plaintexts and their corresponding ciphertexts is $2^{28} \cdot 2 = 2^{29}$ blocks. In step 1, we have to store 2^{22} possible output differences which need 2^{22} blocks of memory. In the key elimination step, since we have 2^{68} bits subkey guess, we need $2^{68} \cdot 2^{-6} = 2^{62}$ blocks of memory.

To conclude, the time complexity of the attack is dominated by the data filtering step, which is $2^{46.42}$ 12-round MIBS encryptions. The memory and the data complexities are 2^{62} blocks and 2^{28} CP, respectively. The attack recovers 68 bits of the 80-bit secret key; the remaining 12-bit of the secret key can be found by exhaustive search.

6 Conclusions

This paper described the first independent and systematic linear, differential and impossible-differential analyses of reduced-round versions of the MIBS block cipher [6]. Actually, we presented the best known-plaintext attack so far on up to 18-round MIBS, and the first ciphertext-only attack on 13-round MIBS. These attacks do not threaten the full 32-round MIBS, but reduce by more than 50% its margin of security.

Table 6 summarizes the complexities of all attacks on reduced-round MIBS described in this paper.

Table 6. Attack complexities on reduced-round MIBS block cipher.

#Rnds	Time	Data	Memory	Key Size	Source	Comments	Success
				(bits)			Prob.
12	$2^{46.42}$	2^{28} CP	2^{62}	80	Sect. 5	ID, key-recovery	—
13	2^{40}	2^{61} CP	2^{24}	64	Sect. 4.2	DC, key-recovery	99.9%
13	2^{55}	2^{55} CO	—	64 or 80	Sect. 3.3	LC,distinguishing	97.7%
13	2^{56}	2^{61} CP	2^{24}	80	Sect. 4.2	DC, key-recovery	99.9%
14	$2^{37.2}$	2^{40} CP	2^{40}	64	Sect. 4.3	DC, key-recovery	50.15%
14	2^{40}	2^{40} CP	2^{40}	80	Sect. 4.3	DC, key-recovery	50.15%
17	2^{69}	2^{58} KP	2^{58}	80	Sect. 3.2	LC, key-recovery	97.94%
18	$2^{76.13}$	$2^{60.98}$ KP	$2^{60.98}$	80	Sect. 3.4	LC, key-recovery	72.14%

time complexity is number of reduced-round encryptions;
LC: Linear Cryptanalysis; DC: Differential Cryptanalysis; ID: Imposs. Differential
CP: Chosen Plaintext; KP: Known Plaintext; CO: Ciphertext Only

References

1. Aoki, K., Ichikawa, T., Kanda, M. Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: *Camellia: a 128-bit block cipher suitable for multiple platforms, design and analysis.* In Stinson.D.R., Tavares, S. (Eds.), SAC'00, Springer, LNCS 2012, 39–56 (2001)
2. Biham, E., Shamir, A.: *Differential Cryptanalysis of DES-like Cryptosystems.* Journal of Cryptology, 4(1), 3–72 (1991)
3. Biryukov,A., De Canniére,C., Quisquater,M: *On Multiple Linear Approximations.* CRYPTO 2004, Springer, LNCS 3152, 1–22 (2004)
4. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C. Poschman, A. Robshaw, M.J.B., Seurin, Y. Vikkelsoe, C.: *PRESENT: An ultra-lightweight block cipher.* In: Paillier, P., Verbauwhede, I. (Eds), CHESS 2007, Springer, LNCS 4727, 450–466 (2007)
5. Lu, J., Kim, J.-S., Keller, N., Dunkelman, O.: *Improving the efficiency of impossible differential cryptanalysis of reduced round camellia and MISTY1.* In Malkin, T.G. (Ed), CT-RSA 2008, Springer, LNCS 4964, 370–386 (2008)
6. Izadi, M.I., Sadeghiyan, B., Sadeghian, S.S., Khanooki, H.A.: *MIBS: a new lightweight Block Cipher.* In: Garay, J.A., Miyaji, A., Otsuka, A. (Eds.), CANS'09, Springer, LNCS 5888, 334–348 (2009)
7. Matsui, M.: *Linear Cryptanalysis Method for DES Cipher*, EUROCRYPT'93, Springer, LNCS 765, 386–397 (1994)
8. Nyberg, K.: *Differentially Uniform Mappings for Cryptography*, In: Helleseth, T. (Ed.), Eurocrypt'93, Springer, LNCS 765, 55–64 (1994)
9. Selçuk, A.A.: *On Probability of Success in Linear and Differential Cryptanalysis*, Journal of Cryptology, (21):1, 1–19 (2008)
10. Wu, W., Zhang, W., Feng, D.: *Impossible differential cryptanalysis of reduced-round ARIA and Camellia.* Journal of Computer Science and Technology, 22(3), Springer, 449–456 (2007)
11. Wu, W., Zhang, L., Zhang, W.: *Improved Impossible-Differential Cryptanalysis of Reduced-Round Camellia.* Avanzi, R., Keliher, L., Sica, F. (Eds.), SAC'08, Springer, LNCS 5381, 442–456 (2009)

A Appendix - Figures and Tables

Table 7. Linear Approximation Table (LAT) of the S-box of MIBS.

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_X	B_x	C_x	D_x	E_x	F_x
0_x	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	-2	0	2	0	-2	-4	-2	2	0	-2	0	2	0	2	-4
2_x	0	0	-2	-2	-2	2	-4	0	0	4	2	-2	-2	-2	0	0
3_x	0	2	2	0	2	0	0	2	-2	4	0	2	0	2	-2	-4
4_x	0	-2	-2	4	-2	0	0	2	0	-2	2	0	-2	0	-4	-2
5_x	0	0	-2	2	2	-2	0	0	2	2	0	4	-4	0	2	2
6_x	0	-2	4	2	0	-2	0	-2	0	2	4	-2	0	2	0	2
7_x	0	4	0	0	0	-4	0	0	-2	-2	2	-2	-2	-2	2	-2
8_x	0	2	2	4	0	2	-2	0	-2	0	0	2	2	-4	0	2
9_x	0	0	2	-2	-4	-4	-2	2	0	0	-2	2	0	0	-2	2
A_x	0	-2	0	-2	-2	0	2	-4	-2	0	2	4	0	-2	0	-2
B_x	0	0	4	0	-2	2	2	2	4	0	0	0	-2	-2	2	-2
C_x	0	0	0	0	2	-2	2	-2	2	2	-2	-2	0	-4	-4	0
D_x	0	2	0	-2	2	0	-2	0	4	-2	4	2	2	0	-2	0
E_x	0	4	-2	2	-4	0	2	-2	2	2	0	0	2	2	0	0
F_x	0	2	2	0	0	2	-2	-4	0	-2	-2	0	-4	2	-2	0

Table 8. (xor) Difference Distribution Table (DDT) of the S-box of MIBS.

	0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	0	2	0	0	2	2	2	0	4	2	0	2	0
2_x	0	2	0	2	0	0	0	4	0	0	2	2	2	0	0	2
3_x	0	0	2	0	0	2	2	2	0	0	0	2	4	2	0	0
4_x	0	0	0	2	0	2	2	2	2	4	0	0	0	0	0	2
5_x	0	0	2	2	2	0	0	2	0	0	0	0	0	2	4	2
6_x	0	0	2	0	0	2	0	0	4	0	2	0	2	0	2	2
7_x	0	2	2	2	4	2	0	0	0	2	0	0	2	0	0	0
8_x	0	0	0	0	2	0	2	0	0	2	2	0	2	2	0	4
9_x	0	4	0	0	2	2	0	0	2	0	0	2	0	2	0	2
A_x	0	2	0	4	0	0	2	0	2	0	0	0	2	2	2	0
B_x	0	0	2	2	2	0	2	0	2	0	4	2	0	0	0	0
C_x	0	2	2	0	0	0	4	0	0	2	0	2	0	0	2	2
D_x	0	2	4	0	0	0	0	2	2	2	2	0	0	2	0	0
E_x	0	2	0	0	2	4	2	2	0	0	2	0	0	0	2	0
F_x	0	0	0	2	0	2	0	0	0	2	2	2	0	4	2	0

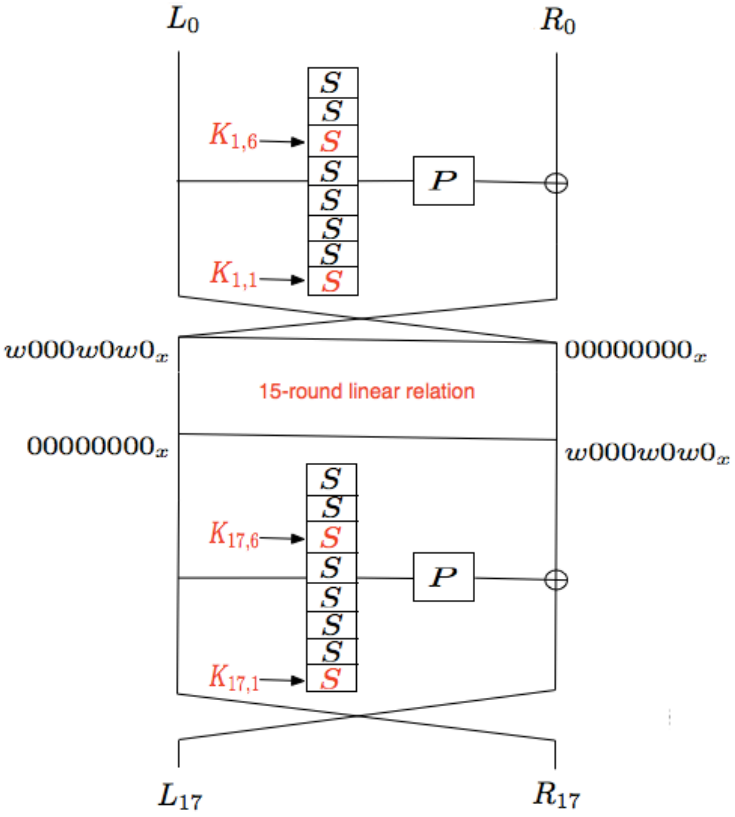

Fig. 1. Linear attack on 17-round MIBS.

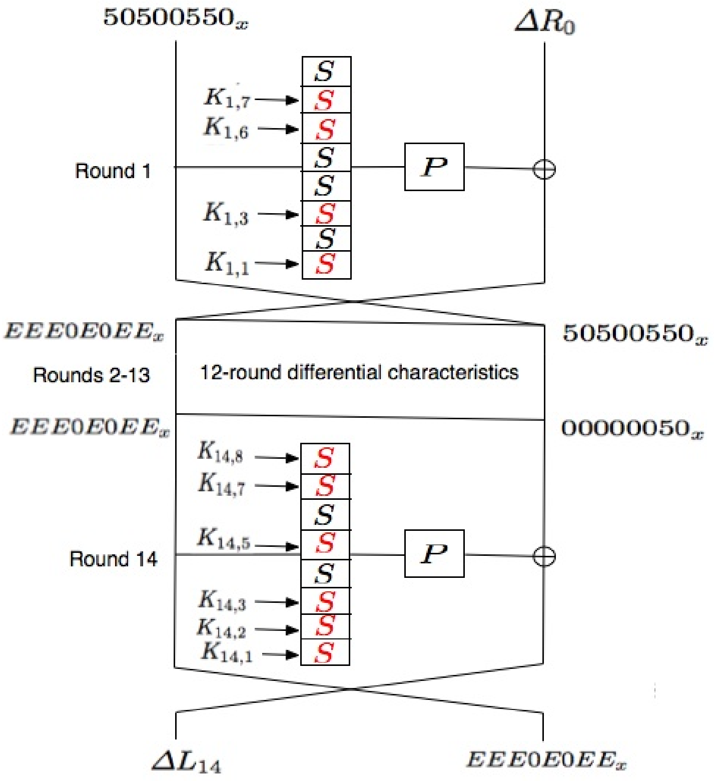

Fig. 2. Differential attack on 14-round MIBS.

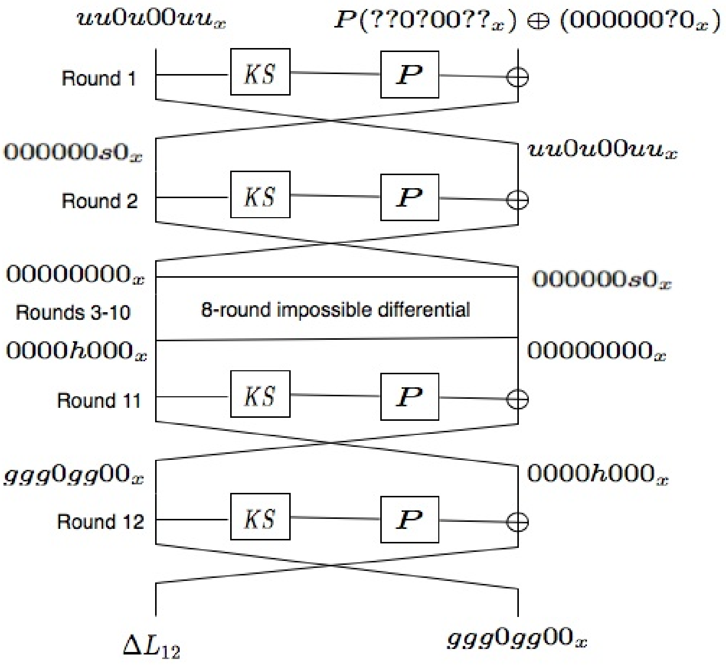

Fig. 3. Impossible differential attack on 12-round MIBS.

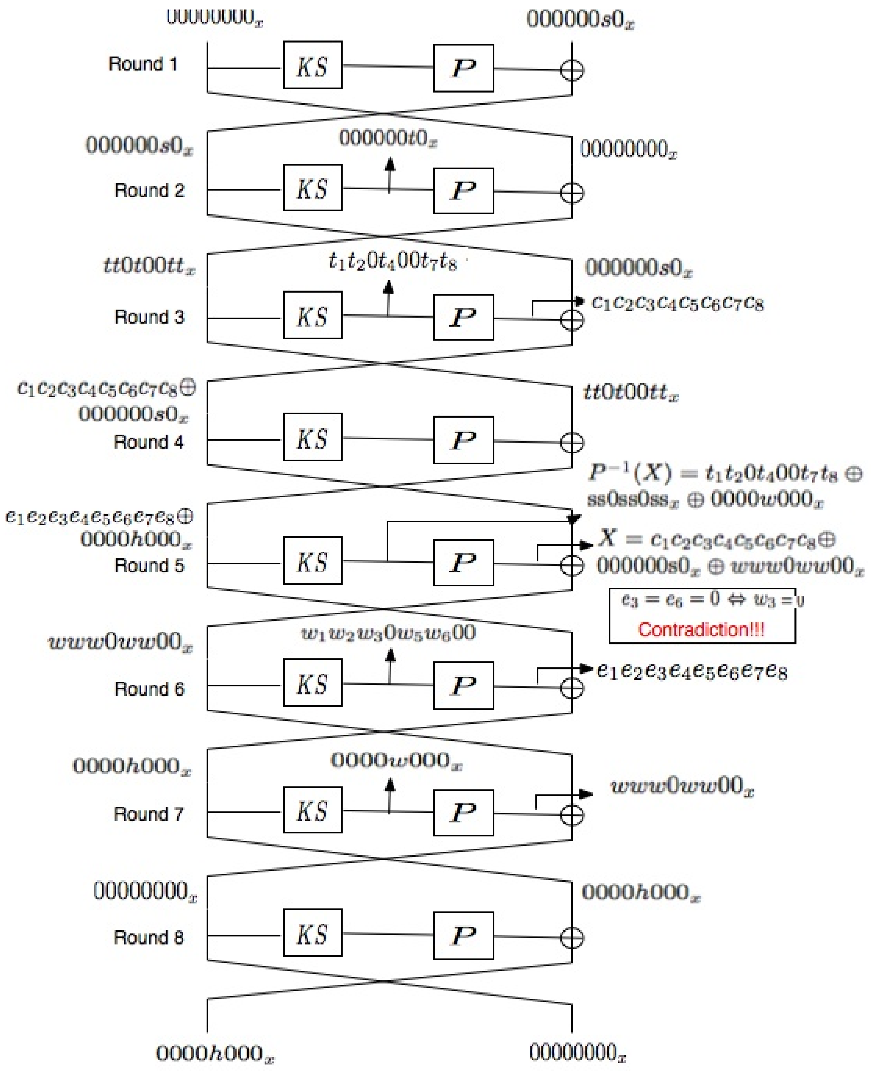

Fig. 4. 8-round impossible differential of MIBS.