Impossible differential cryptanalysis of Midori

Z. Chen
Center for Cryptology Study, Department of Computer Science and Technology,
Tsinghua University, Beijing, 100084, China
[†]E-mail: z-chen14@mails.tsinghua.edu.cn

X. Y. Wang
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, 250100, China
School of Mathematics, Shandong University, Jinan, 250100, China
Institute of Advanced Study, Tsinghua University, Beijing, 100084, China
E-mail: xiaoyunwang@mail.tsinghua.edu.cn

Midori is a light weight block cipher recently presented by Banik et al in ASIACRYPT 2015. There are two versions of Midori with state sizes of 64-bit and 128-bit respectively. The round function is based on Substitution-Permutation Network(SPN). In this paper, we give impossible differential cryptanalysis of Midori64. We studied the non-linear layer of the cipher and give two useful properties. We also find the first 6-round impossible differential paths with two non-zero and equal input cells and one non-zero output cell, and then mount 10-round attack. This is the first impossible differential attack on Midori.

Keywords: Midori; Light Weight Block Cipher; Impossible Differential Cryptanalysis.

1. Introduction

In recent years, the trend of linking everything into internet has aroused a great attention on light weight block ciphers. Low resource devices such as RFID tags and sensor nodes with their restricted hardware area and demand of low latency, made light weight block cipher a popular discipline. It has to be fast, efficient, as well as secure. Several light weight block ciphers emerged these years such as HIGHT[1], CLEFIA[2], KATAN[3], KLEIN[4], LED[5], PRESENT[6], Piccolo[7], and SIMON/SPECK[8].

Midori[9] is presented by Banik et al in ASIACRYPT 2015 to be a most energy-efficient architecture. Energy consumption is a measure of the total work done by voltage source during the execution of an operation. The security of light weight block cipher is vital as it is the key to keep you safe from hackers.

Impossible differential attack is a powerful tool to analyze the security of a cipher, and has been successfully applied to many block ciphers such as AES[10,11], CLEFIA[12]. It was independently introduced by Knudsen, to analyze AES candidate DEAL[13], and Biham et al.to attack Skipjack[14] and IDEA[15]. The aim of impossible differential cryptanalysis is to connect two differential paths with a contradiction, thus this differential will never occur. Any key that leads to such a differential is definitely a wrong key. When we eliminate all wrong key candidates, we are left with the right key.

This paper is organized as follows, in section 2, we give a brief description of Midori and some notations that will be used in this paper. In section 3 we first give some properties of Midori and impossible differential paths that we find, and then we describe our attack. Section 4 concludes the paper.

2. A Brief Description of Midori

There are two variants of Midori, Midori64 and Midori128 with block sizes equal to 64 and 128 bits respectively. Both have key size 128-bit. Midori uses Substitution-Permutation Network (SPN) structure, the block of the cipher is arranged in a 4 × 4 matrix called a State as follows:

$$S = \begin{pmatrix} s_0 & s_4 & s_8 & s_{12} \\ s_1 & s_5 & s_9 & s_{13} \\ s_2 & s_6 & s_{10} & s_{14} \\ s_3 & s_7 & s_{11} & s_{15} \end{pmatrix}.$$

For Midori64, each cell (s_i) is 4 bits, and for Midori128, the cell size m = 8 bits. Some parameters of Midori are shown in table 1.

Table 1. The two variants of Midori

	Block size(n)	Key size	Cell size(m)	Number of Rounds
Midori64	64	128	4	16
Midori128	128	128	4	20

2.1. *Key schedule.*

For Midori64, the 128-bit master key is denoted as concatenation of two 64-bit keys K_0 and K_1. The whitening key $WK = K_0 \oplus K_1$. Each round key $k_i = K_{(i+1)\%2} \oplus \alpha_i$, where $i = 1, \dots, 15$, and α_is are constants. $k_{16} = WK$.

2.2. *Round function specifications.*

Each round consists of three parts, substitution layer, permutation layer and *KeyAdd* layer. The plaintext is loaded to the state S. Encryption begins with a whitening key *XOR*ed to the state. Permutation layer is omitted in the last round.

The substitution layer of Midori is a S-box layer. Each cell is substituted individually by its output of a S-box. For Midori64, the 4-bit S-box is given in hexadecimal form in table 2:

Table 2. The S-box used in Midori64

s:	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
SB(*s*):	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

The permutation layer is composed of *ShuffleCell* and *MixColumn*. *ShuffleCell* is a cell re-permutation of the state. $(s_0, \dots, s_{15})$ is replaced by $(s_0, s_{10}, s_5, s_{15}, s_{14}, s_4, s_{11}, s_1, s_9, s_3, s_{12}, s_6, s_7, s_{13}, s_2, s_8)$. *MixColumn* is to multiply the state by matrix *M*, where

$$M = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}.$$

KeyAdd is to *XOR* *n*-bit round key k_i to the state *S*.

2.3. *Some notations.*

We use the following notations in this paper.

- X_{i-1}: the input of the *i*-th round, X_0 is plaintext
- X_{i-1}^{SB}: the state after S-box operation of the *i*-th round
- X_{i-1}^{SC}: the state after *ShuffleCell* operation of the *i*-th round
- X_{i-1}^{MC}: the state after *MixColumn* operation of the *i*-th round
- $X_i[j]$: the *j*-th cell of X_i
- k_i: the subkey of the *i*-th round, $i = 1, \dots, 16$
- ΔX: the difference of two states X and X'

3. Impossible Differential Attacks of Midori64

3.1. *Two properties of S-box.*

Property 1: Consider three cells of the state, for example, position$(0,5,15)$, with any input differences, but we want the output differences to be the same and non-zero. We traverse all possible inputs and find 61400 such inputs. The total number of inputs are $(2^4)^6 = 2^{24}$. So the probability that S-box outputs three cells with the same non-zero difference is $2^{-8.09}$. If the input differences are non-zero, the total number of inputs are $(2^4-1)^3 \times (2^4)^3$, so the probability that S-box outputs three cells with the same non-zero difference is $2^{-7.81}$.

Property 2: Consider two cells of the state, for example, position $(1,11)$, with any input differences, but we want the output differences to be the same and non- zero. We traverse all possible inputs and find 3840 such inputs. The total number of inputs are $(2^4)^4 = 2^{16}$. So the probability that S-box outputs two cells with the same non-zero difference is $2^{-4.09}$.

3.2. *Impossible differential paths of Midori64.*

We find in total 208 six-round impossible differential(ID) paths of Midori64 with the following form: two cells of the input of the ID path have non-zero and equal difference, others have zero difference. The output of the ID path have one non-zero cell.

We use the path (0, a, 0, 0, 0, 0, 0, 0, 0, 0, 0, a, 0, 0, 0, 0) → (0, 0, 0, 0, 0, *, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0) in our attack, the 6-round impossible differential is shown in figure 1, where a blank cell denotes zero difference, a and * denote non-zero difference, and ? denotes an uncertain difference.

3.3. *Procedures of the attack.*

We add one round on top and three rounds at the bottom of the impossible differential path and mount attack on 10-round Midori64. Note there is no permutation layer in the last round. The states are shown in figure 2.

3.3.1. *Data-collecting phase*

Choose a structure of 2^{24} plaintexts which have certain fixed values in 10 cells and the other six positions $(0,3,5,9,12,15)$ take all possible values. We call this a structure. Each structure can form approximately $2^{24} \times 2^{24} \times \frac{1}{2} \approx 2^{47}$ pairs. We take 2^n structures so as to obtain 2^{n+24} plaintexts and 2^{n+47} pairs. Encrypt by S-box layer, and choose only the pairs that have the same non-zero difference in position (0,5,15) and in position (3,9,12) respectively. By property 1, there remains approximately $2^{n+47-8.09\times 2} = 2^{n+30.82}$ pairs.

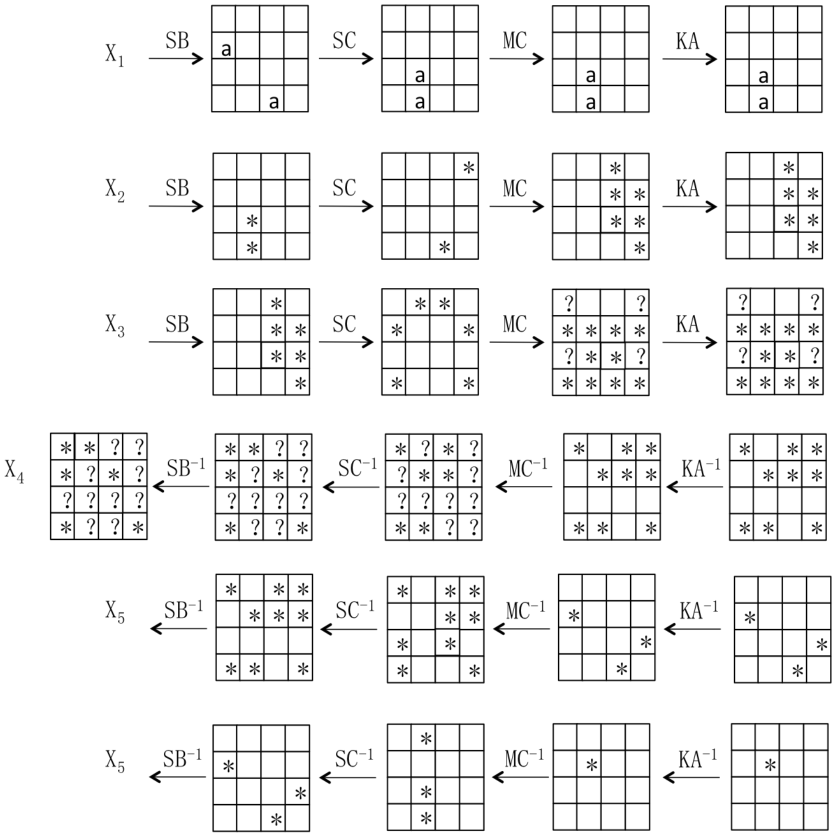

Fig. 1. 6-round impossible differential path of Midori64.

3.3.2. *Key recovery phase*

Encrypt the plaintext through *ShuffleCell* and *MixColumn*, guess $k_1[1,11]$ and compute X_1^{SB}. Keep only the pairs such that $X_1^{SB}[1]$ and $X_1^{SB}[11]$ have the same difference. By property 2, there are $2^{n+30.82-4.09} = 2^{n+26.73}$ pairs left.

Encrypt the remaining pairs through 9 rounds and get X_{10}. Keep only the pairs such that ΔX_{10} have zero difference in position (0, 7, 9, 12, 13, 14, 15). There left $2^{n+26.73-28} = 2^{n-1.27}$ pairs.

Guess $k_{10}[1,2,3,4,5,6,8,10,11]$ and compute ΔX_9 . We want only the pairs that have the same difference in each column of the state. By property 1, the number of pairs that satisfy this condition is $2^{n-1.27-7.81\times 3} = 2^{n-24.7}$.

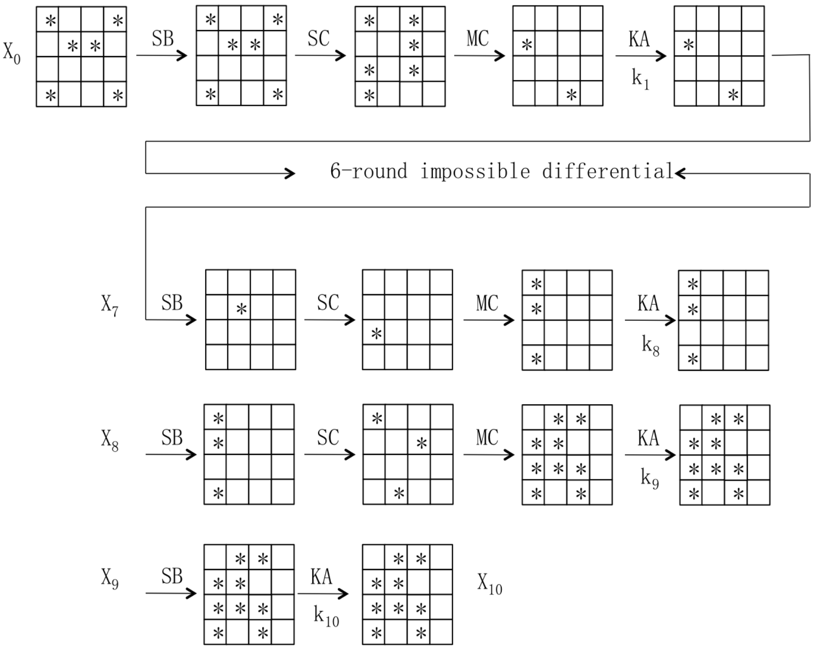

Fig. 2. 6-round impossible differential path of Midori64.

For every remaining pair, Guess $k_9[2,3,4,5,6,8,10]$ (note $k_9[1] = k_1[1]\oplus\alpha_1\oplus\alpha_2$ and $k_9[11] = k_1[11]\oplus\alpha_1\oplus\alpha_2$ are already guessed) and compute ΔX_8. By property 1, the probability that the pairs have the same difference in the first column of the state is $2^{-7.81}$. Such a difference is impossible and every k_9 that propose such a difference is definitely a wrong key.

So if there exists a pair satisfying the condition, the guessed k_9 are definitely wrong keys. Unless the initial assumption on $k_1[1,11]$ and $k_{10}[1,2,3,4,5,6,8,10,11]$ is correct, it is expected that we can get rid of all wrong values of k_9 for each guessed 8-bit k_1 and 36-bit k_{10} since the wrong value (k_1, k_9, k_{10}) remains with a very small probability by choosing a proper n. Hence if there remains a value of k_9 after the filtering, we can assume the guessed key value above is the right key.

3.4. *Complexity analysis.*

In step 5, we analyze the $2^{n-24.7}$ pairs, the expected remaining number of remaining 72-bit wrong keys is $N = 2^{36+28+8}\times(1-2^{-7.81})^{2^{n-24.7}}$. In order to have $N \ll 1$, we set n = 38.4. Then the date complexity is $2^{38.4+24} = 2^{62.4}$ chosen plaintexts. The time complexity of each step is shown in table 4. So the total time complexity is $2^{80.81}$ 10-round encryption, memory complexity is $2^{65.13}$ 64-bit blocks.

Table 3. Complexity of the attack on Midori64

Step	Time complexity	Memory complexity
DCF[a]	$2^{n+24}\times\frac{1}{4}/10\text{E} \approx 2^{57.08}\text{E}$	-
1	$\leq (2^{n+24}\times\frac{2}{4} + 2^{n+24}\times\frac{2}{4}\times2^{8}\times\frac{2}{16})/10\text{ E} \approx 2^{63.08}\text{ E}$	$2\times2^{n+26.73}$ 64-bit block
2	$\leq 2^{n+24}\times2^{8}\times(\frac{3}{4}+8)/10\text{ E} \approx 2^{70.21}\text{ E}$	$2\times2^{n-1.27}$ 64-bit block
3	$2\times2^{n-1.27}\times2^{8}\times2^{36}\times\frac{2}{4}/10\text{ E} \approx 2^{77.81}\text{ E}$	$2\times2^{n-24.7}$ 64-bit blocks
4	$2\times2^{8+36+28}\times(1+(1-2^{-7.81})+\cdots+(1-2^{-7.81})^{2^{n-24.7}})/10\text{E} \approx 2^{80.81}\text{ E}$	-

Note: [a]data collecting phase.

4. Conclusion

In this paper, we find 6-round impossible differential paths of Midori64, and then mount attack up to 10-round. This is the first impossible differential attack on Midori.

References

1. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer (2006)
2. T. Shirai, K. Shibutani, T. Akishita, S. Moriai, T. Iwata. The 128-bit Block-cipher CLEFIA (Extended Abstract). In FSE 2007, LNCS, vol. 4593, pp. 181-195.
3. De Canniere C, Dunkelman O, Knežević M. KATAN and KTANTAN—a family of small and efficient hardware-oriented block ciphers[M] // Cryptographic Hardware and Embedded Systems-CHES 2009. Springer Berlin Heidelberg, 2009: 272-288.
4. Z. Gong, S. Nikova, Y.W. Law. KLEIN: a new family of lightweight block ciphers. In RFIDSec 2011, LNCS, vol. 7055, pp. 1-18.

5. J. Guo, T. Peyrin, A. Poschmann, M. J. B. Robshaw. The LED Block Cipher. In CHES 2011, LNCS, vol. 6917, pp. 326-341.
6. A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In CHES 2007, LNCS, vol. 4727, pp. 450-466.
7. K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, T. Shirai. Piccolo: An Ultra-Lightweight Blockcipher. In CHES 2011, LNCS, vol. 6917, pp. 342-357.
8. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers. The SIMON and SPECK Families of Lightweight Block Ciphers. In IACR eprint archive. Available at https://eprint.iacr.org/2013/404.pdf.
9. Banik S, Bogdanov A, Isobe T, et al. Midori: A Block Cipher for Low Energy[M]//Advances in Cryptology–ASIACRYPT 2015. Springer Berlin Heidelberg, 2014: 411-436.
10. Phan R C W. Impossible differential cryptanalysis of 7-round advanced encryption standard (AES)[J]. Information processing letters, 2004, 91(1): 33-38.
11. Lu J, Dunkelman O, Keller N, et al. New impossible differential attacks on AES[M]//Progress in Cryptology-INDOCRYPT 2008. Springer Berlin Heidelberg, 2008: 279-293.
12. Boura C, Naya-Plasencia M, Suder V. Scrutinizing and improving impossible differential attacks: Applications to clefia, camellia, lblock and simon[M]//Advances in Cryptology–ASIACRYPT 2014. Springer Berlin Heidelberg, 2014: 179-199.
13. Knudsen, L.: DEAL - A 128-bit Block Cipher. In: NIST AES Proposal (1998)
14. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Stern, J. (ed.) Advances in Cryptology - EUROCRYPT ’99. LNCS, vol. 1592, pp. 12–23. Springer (1999)
15. Biham E, Biryukov A, Shamir A. Miss in the Middle Attacks on IDEA and Khufu[C]//Fast Software Encryption. Springer Berlin Heidelberg, 1999: 124-138.