Impossible Differential Attack on Midori128 Using Rebound-like Technique

Wenquan Bi[1], Zheng Li[1], Xiaoyang Dong[1] and Xiaoyun Wang[1,2]

[1] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education,Shandong University,Jinan,250100,China, biwenquan@mail.sdu.edu.cn

[2] Institute of Advanced Study, Tsinghua University, Beijing, 100084, China

Abstract. Midori is a family of lightweight block cipher proposed by Banik *et al.* in ASIACRYPT 2015 and it is optimized with respect to the energy consumed by the circuit per bit in encryption or decryption operation. Midori is based on the Substitution-Permutation Network, which has two variants according to the state sizes, i.e. Midori64 and Midori128. It attracted a lot of attention of cryptanalyst since its release. For Midori64, the first meet-in-the-middle attack was proposed by Lin and Wu, which was published on the ToSC 2017 recently. The first impossible differential attack of Midori64 was presented by Chen *et al.* and Dong gave the first related-key differential attack. Guo *et al.* introduced an invariant space attack against full-round Midori64 in weak key setting, which was published in ToSC 2017 recently. However, for Midori128, there are only one impossible differential cryptanalysis result proposed by Chen *et al.* against 10-round reduced Midori128 and one related-key result by Gérault *et al.* in INDOCRYPT 2016. In this paper, we present a new impossible differential attack on Midori128 by using a new impossible differential proposed by Sasaki *et al.*, we achieve 10-round impossible differential attack with the time complexity 2^{111} and 11-round impossible differential attack with the time complexity $2^{126.94}$ finally. This is the best single-key cryptanalytic result of Midori128 as far as we know. We should point out the our attacks do not threaten the security of full-round Midori128.

Keywords: cryptanalysis, lightweight block cipher, impossible differential, Midori128, single-key attack

1 Introduction

Block cipher plays an important role in the security of communication. As many devices are confined in size, light weight block ciphers are needed urgently. Nowadays quantities of light weight block ciphers are designed for different applications, like HIGHT [14], CLEFIA [21], PRESENT [5], KATAN and KATANTAN [8], Piccolo [20], LED [13], KLEIN [11], SIMON and SPECK [2].

At ASIACRYPT 2015, a new lightweight block cipher Midori [1] was presented by Banik *et al.* Considering the encryption and decryption operation,

they optimized Midori in aspect of its energy consumed by the circuit. As both Substitution-Permutation Network (SPN) and Feistel architectures have advantages in different aspects. The designers of Midori select SPN architecture over Feistel to get a secure cipher with the minimized number of rounds.

Impossible differential cryptanalysis was first proposed by Biham [3, 4] and Knudsen [16] independently at the end of the last century. As explored by many cryptanalysts in the following years, it is still a method with great vitality. Opposite to differential cryptanalysis, which is to find the differentials with high probability, impossible differential cryptanalysis is to find the differentials with zero probability. Therefore, the pairs of $(plaintext, cipertext)$ with right key will absolutely not obey any of impossible differentials. Once a pair obeys the impossible differential, the corresponding key used to encrypt is certainly a wrong key. As quantities of impossible differentials applied, wrong keys are eliminated, and the right key is supposed to be only one left. Many automatic approaches of searching impossible differentials emerge, such as matrix method [15], automatic search for word-oriented block ciphers [23] and so on.

Table 1. Summary of the attacks on Midori

Version	Method	Rounds	Time	Data	Reference
Midori64	Impossible differential	10	$2^{80.81}$	$2^{62.4}$	[6]
Midori64	Meet-in-the-middle	10	$2^{99.5}$	$2^{59.5}$	[17]
Midori64	Meet-in-the-middle	11	2^{122}	2^{53}	[17]
Midori64	Meet-in-the-middle	12	$2^{125.5}$	$2^{55.5}$	[17]
Midori64	Invariant subspace attack$(2^{32})^{\S}$	full	2^{16}	2	[12]
Midori64	Nonlinear invariant attack$(2^{64})^{\S}$	full	2^{16}	2	[22]
Midori64	Related key attack†	14	2^{116}	2^{59}	[9]
Midori64	Related key attack	full	$2^{35.8}$	$2^{23.75}$	[10]
Midori128	Impossible differential	10	2^{119}	$2^{118.63}$	[7]
Midori128	Impossible differential	10	$2^{116.71}$	$2^{116.17}$	[7]
Midori128	Impossible differential	10	2^{111}	$2^{109.94}$	Sect. 6
Midori128	Impossible differential	11	$2^{126.94}$	$2^{126.94}$	Sect. 7
Midori128	Related key attack	full	$2^{43.7}$	$2^{43.7}$	[10]

§:Weak key space is 2^{32} and 2^{64} respectively

†:The designers of Midori state no security claim under related key setting

In this paper, we apply the impossible differential method to the cryptanalysis of Midori128 and achieve 11-round attack which is one more round than the result ever, as the designers state no security claim under related-key setting, our result is the best single-key cryptanalytic result of Midori128 as far as we know.

The rest of this paper is organized as follows: in Sect. 2 we give a brief description of Midori block cipher and some notations that we use in the attack. Some related works are introduced in Sect. 3. Filtering round keys using rebound-like technique is introduced in Sect. 4. We introduce the new impossible differential path in Sect. 5 and give a new 10-round impossible differential attack on Midori128 in Sect. 6. Our 11-round impossible differential attack is presented in Sect. 7. Section 8 concludes the paper.

2 Brief Description of Midori128

We use the following notations in this paper.

- P, C, K: the plaintext, ciphertext and master key of Midori128
- WK: the whitening key, which is equal to the master key in Midori128
- X_i: the input of the i-th round, P is plaintext, $X_0 = P \oplus K$
- Y_i: the state after SubCell(SC) operation of the i-th round
- Z_i: the state after ShuffleCell(ShC) operation of the i-th round
- W_i: the state after MixColumn(MC) 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, $i = 0 \cdots, 19$
- u_i: the equivalent subkey after MC^{-1} operation of k_i,$i = 0 \cdots, 19$
- $\triangle X$: the difference of two states X and X'

2.1 Round Function Specifications

Midori [1] is a lightweight block cipher designed by Banik *et al.* at AISACRYPT 2015. It adopts the Substitution-Permutation Network(SPN). There are two versions of Midori with state sizes of 64-bit and 128-bit, denoted as Midori64 and Midori128, respectively. They are designed to reduce energy consumption when implemented in hardware. Midori128 has 128-bit state size and its key size is 128-bit. It uses the following 4×4 array as a data expression:

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

where the size of each cell is 8-bit.

The round function F of Midori128 is composed of the following 4 operations:

- **SubCell(SC):** Apply the non-linear 8×8 S-box in parallel on each 8-bit cell of the state. Midori128 utilizes four different 8-bit S-boxes SSb_0, SSb_1, SSb_2 and SSb_3, where SSb_0, SSb_1, SSb_2, $SSb_3 : \{0,1\}^8 \rightarrow \{0,1\}^8$. The details of S-box can refer to [1].
- **ShuffleCell(ShC):** The 8-bit cells of the state are performed as follows:
  $(s_0, s_1, \ldots, s_{15}) \leftarrow$
  $(s_0, s_{10}, s_5, s_4, s_{11}, s_1, s_9, s_3, s_{12}, s_6, s_7, s_{13}, s_2, s_8)$.

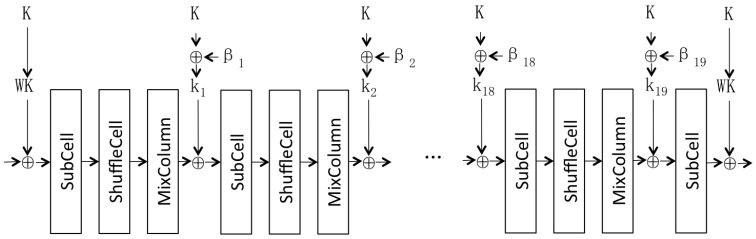

Fig. 1. The encryption algorithm of Midori128

– **MixColumn(MC):** Midori128 utilizes an almost MDS matrix $\mathbf{M}$ defined as follows:

$$\mathbf{M} = \begin{pmatrix} 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \\ 1\,1\,1\,0 \end{pmatrix}$$

$\mathbf{M}$ is applied to every column of the state S, i.e. ${}^t(s_i, s_{i+1}, s_{i+2}, s_{i+3}) \leftarrow \mathbf{M} \cdot {}^t(s_i, s_{i+1}, s_{i+2}, s_{i+3})$ and $i = 0, 4, 8, 12$.
– **KeyAdd(AK):** The i^{th} 128-bit round key rk_i is XORed to the state S.

Before the first round, an additional **AK** operation is applied, and in the last round, the ShuffleCell and MixColumn operations are omitted. The total round number of Midori128 is 20. The encryption algorithm of Midori128 is depicted in Fig. 1, more details can be referred to [**?**].

2.2 Key Schedule

The key-schedule of Midori128 is quite simple. A 128-bit mater key K is used to generate the round key with the simple linear equations. The whitening key is the same as the master key, and the sub-key for round i is $k_i = rk_i = K \oplus \beta_i$, where $0 \leq i \leq 18$ and β_i is constant.

3 Related works

Many works emerge as for the cryptanalysis of Midori. We briefly describe some of their approaches and results here. Firstly, we list the works in single-key model.

Lin and Wu [17] proposed a 12-round meet-in-the-middle attack on Midori64. Using both differential enumeration technique and key-dependent sieve technique, they obtained a 7-round meet-in-the-middle distinguisher. Then they added 1 round and 4 rounds at the beginning and the end of the distinguisher, respectively.

Chen *et al.* presented a 10-round impossible differential attack on both Midori64 [6] and Midori128 [7]. They found a 6-round impossible differential, which

has two nonzero but equal cells in the input and one nonzero output cell in the output. Together with exploiting the properties of S-boxes, they reduced time complexity by the hash table constructed in the pre-computation phase.

Furthermore, the weak-key attack also attracted the cryptanalysts. Some novel ideas are proposed and achieved efficient results.

The invariant subspace attack against Midori64 was presented by Guo *et al.* [12] As a weak-key attack, the weak key space is of size 2^{32}. Actually, just one chosen plaintext query can make it able to distinguish Midori64 from a random permutation. Thus, the attack cost negligible computation and memory. This work illustrated that the selection of key used should be careful.

At ASIACRYPT 2016, Todo *et al.* [22] proposed the nonlinear invariant attack and applied it to Midori64. It succeed to distinguish full-round Midori64 in a weak-key set in size of 2^{64}. They also consider the modes of operation as Midori64 consumes low energy. In the well-known modes of operation like CBC, CFB, OFB and CTR, the attack achieved to recover 32-bit plaintext among the 64-bit block. Their attacks are all practical.

Additionally, cryptanalysis in the related-key model is performed on Midori. Some representative works are listed here.

Dong and Shen [9] propose a 14-round related-key differential attack on Midori64. They explored the Mixcolumn and obtained branching properties. According to that, they found many 4-round truncated differentials for Midori64. It is proved that no truncated differentials with more rounds exist by exhaustive search. The above conclusion is also right for Midori128 because Midori64 and Midori128 applies the same Mixcolumn matrix in the round function.

At INDOCRYPT 2016, full-round related-key key recovery attacks on both Midori64 and Midori128 are proposed by Gérault and Lafourcade [10]. As to obtain optimal related-key differentials with high probability, they constructed automatic search with the help of a constraint programming model.

4 Filtering Round Keys using Rebound-like Technique

The original rebound attack is a hash function analyzing technique which was first proposed by Mendel *et al.* [18] in FSE 2009. It uses the following property of S-box.

Property 1 (Property of S-box). Given $\triangle X$ and $\triangle Y$ two non-zero differences, the equation of s-box $S(x) \oplus S(x \oplus \triangle X) = \triangle Y$ has one solution on average.

As shown in Fig. 2, the rebound attack works in two phases: inbound phase and outbound phase. In the inbound phase the low-weight input and output differences are propagated to forward and backward which connect usually in the most expensive part. Then generate all possible actual value pairs that satisfy the difference and construct solutions though the connected part such as S-box layer using Property 1. Then in the outbound phase, these solutions are propagated through the other rounds in both directions.

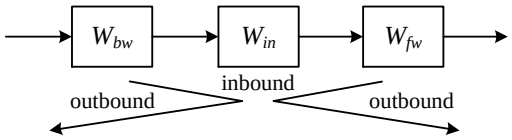

Fig. 2. The Rebound Attack

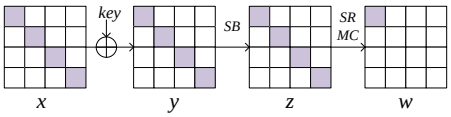

Fig. 3. Guess and Determine Technique

In differential attack and impossible differential attack, one find pairs that meet the given differential under guessed keys, denoted as (x, x', key). In differential attack, we maintain a counter of such pairs with the key, store it a list indexed by the key, the right key is marked by the largest counters in the list. In impossible differential attack, one filter guessed keys if there is at least one pair meet the given differential under these keys. So the important step in these two attack models is to find pairs efficiently to meet a given differential under guessed key. In these section, we apply the *rebound-like technique* to accelerate this step.

As an example shown in Fig. 3, if we use the classic guess-and-determine method to find pairs that meet the differential, for one given (x, x'), we need guess 2^{24} key bytes in diagonal to find one (x, x', key) that meets the truncated differential. The time complexity is 2^{24}. However, using a rebound-like technique, as shown in Fig. 4, there are only 2^8 possible differences in z, for a given pair (x, x'), using Property 1, we can get the value in y for a Δz and then the key

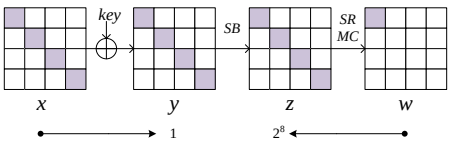

Fig. 4. Rebound-like Technique

bytes in diagonal are computed. So using the rebound-like technique, the time complexity to a pair (x, x', key) that meets the truncated differential is 1.

5 The new impossible differential path by Sasaki *et al.*

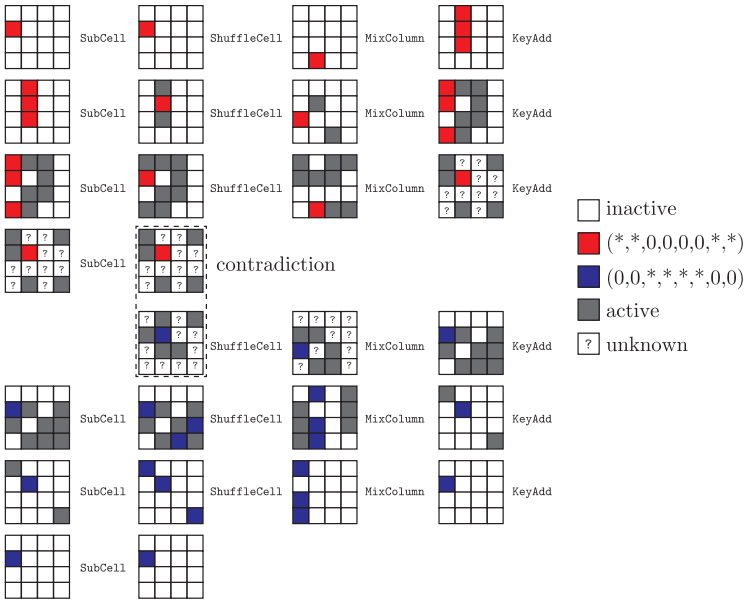

Fig. 5. 7-round impossible differential of Midori128

The impossible differential used in our attack was proposed by Sasaki *et al.* [19] to be presented at EUROCRYPT 2017. They provided a new tool searching for impossible differentials which can additionally consider the property of S-box with small size. As depicted in Fig. 5, $(0\alpha00, 0000, 0000, 0000)$ and $(0\beta00, 0000, 0000, 0000)$ will not be the input diffecrence and output difference of 7-round Midori128 at the same time, where $\alpha = (*, *, 0, 0, 0, 0, *, *), \beta = (0, 0, *, *, *, *, 0, 0)$. Based on the work by Sasaki *et al.*, we truncate their impossible differential of Midori128, change two cells of it and get a new 6-round impossible differential as shown in Fig. 6.

we use the 6-round impossible differential as shown in Fig. 6 to implement a new 10-round impossible differential attack on 10-round Midori128 and use the 7-round impossible differential by Sasaki *et al.* to achieve 11-round attack.

6 A New Impossible Differential Attack on 10-Round Midori128

In this section, we present a new impossible differential attack on 10-round Midori128 with the new impossible differential characteristic shown in Fig. 6 which was presented in [19]. In our attack, we use the rebound-like technique to filter the round keys which follow the impossible differential and need to be discard. In that way, we don't guess the round keys but the difference and reduce the time complexity.

We start Midori128 at round 0, and place this impossible differential path at round 2 to 8, then add two rounds before the 6-round impossible differential and two rounds after it. We illustrate the states of each round in Fig. 7.

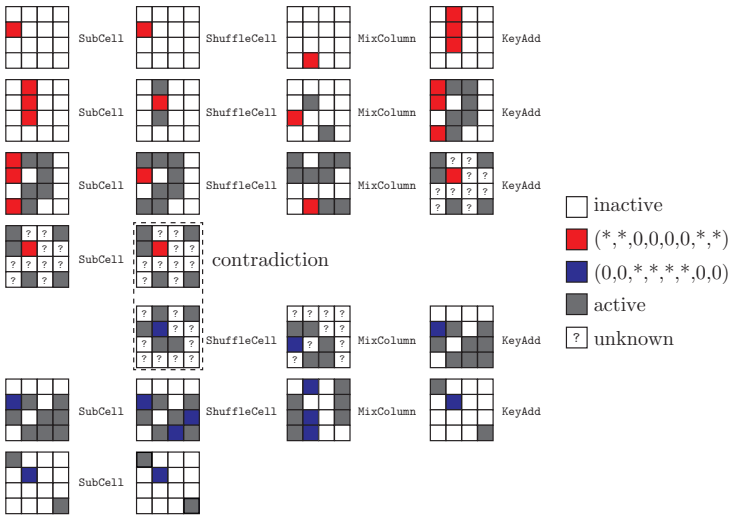

Fig. 6. 6-round impossible differential of Midori128

6.1 Data Collecting Phase

We take all possible values in the nine cells at position $[1, 2, 5, 7, 10, 11, 13, 14, 15]$ of plaintext P and remain other cells constants. Then we take the $2^{8\times 9} = 2^{72}$ plaintexts as a structure, encrypt it through 10-round Midori128 and get the ciphertexts. Insert the corresponding ciphertexts into a hash table indexed by cell positions $[4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]$. For each row we expect to have $2^{72} \times 2^{-8\times 12} = 2^{-24}$ ciphertexts. Select all possible pairs in each row with more than one ciphertexts, we expect to have $2^{(-24)\times 2-1} \times 2^{8\times 12} = 2^{47}$ pairs. We take 2^n structures and get 2^{n+47} pairs with zero difference in cell $[4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15]$.

6.2 Key Recovering Phase

In this phase, we eliminate wrong values of the 11-byte key $K[0, 1, 2, 3, 5, 7, 10, 11, 13, 14, 15]$ by showing that the impossible differential path holds if these keys were used.

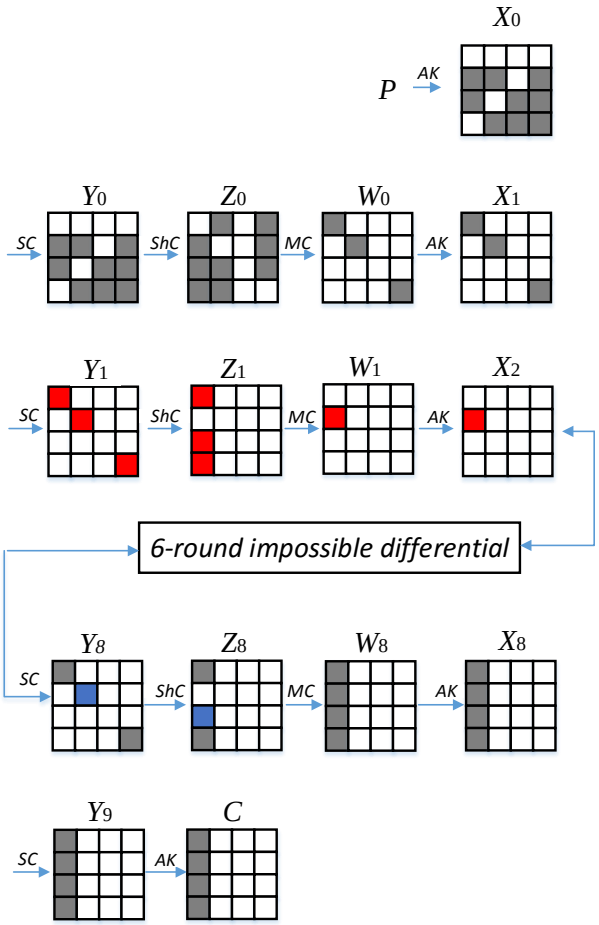

Fig. 7. A new 10-round impossible differential attack on Midori128

Step 1 For each of the 2^{n+39} pairs, guess the 24-bits difference values $\triangle X_1[0, 5, 15]$, then deduce $\triangle Y_0[1, 2, 5, 7, 10, 11, 13, 14, 15]$, $X_0[1, 2, 5, 7, 10, 11, 13, 14, 15]$ and $Y_0[1, 2, 5, 7, 10, 11, 13, 14, 15]$ can be got from $\triangle Y_0$ and $\triangle X_0 = \triangle P$ according to the property 1. Then compute the master $K[1, 2, 5, 7, 10, 11, 13, 14, 15]$ from the P and X_0. In this step, we get 2^{24} values of $K[1, 2, 5, 7, 10, 11, 13, 14, 15]$.

Step 2 For each pair in step 1, guess the 4-bit difference values of $\triangle X_2[1]$ (the differences with the pattern $(**0000**)$), then deduce $\triangle Y_1[0,5,15]$. According to the property 1, $X_1[0,5,15]$ and $Y_1[0,5,15]$ can be got from $\triangle Y_1[0,5,15]$ and $\triangle X_1[0,5,15]$ which was guessed in step 1. As the values of $Y_0[1,2,5,7,10,11,13,14,15]$ are known in step 1, $W_1[0,5,15]$ can be got and we can compute the subkey $K_0[0,5,15]$. In this step, we get 2^4 values of $K_0[0,5,15]$. As the $K_0 = K \oplus \beta_0$, we have two 8-bit linear equation in position $(5,15)$ and there is a key independent sieve for the key we deduced. So we expect $2^{24} \times 2^4 \times 2^{-8\times 2} = 2^{12}$ different master key $K[0,1,2,5,7,10,11,13,14,15]$ left after this step.

Step 3 For each pair in step 2, guess the $2^{8\times 2+4}$ values of $\triangle Y_8[0,5,15]$ where byte 0 and 15 take all possible values and byte 5 is with the bit pattern $(00****00)$, then deduce 2^{20} $\triangle X_9[0,1,2,3]$, as the difference $\triangle Y_9 = \triangle C$, $X_9[0,1,2,3]$ and $Y_9[0,1,2,3]$ can be got according to the property 1. Then the master key $K[0,1,2,3]$ can be computed by $Y_9[0,1,2,3]$ and C. Notice that there are three bytes key $K[0,1,2]$ repeated with the key deduced in step 1 and 2. Compare the 24-bit value, if they are unequal, discard this value. We expect $2^{20} \times 2^{12} \times 2^{-8\times 3} = 2^8$ value left after this step.

Step 4 After guess and eliminate for 2^{n+47} pairs, if there are keys left of the 88-bit master key, exhaustive search the other 40-bit master key to get and examine the right key.

Note that for each pair, we could eliminate 2^8 value of the 11-byte key $K[0,1,2,3,5,7,10,11,13,14,15]$. We want to eliminate all the values in the subkey list unless the value of subkey is correct. The probability of a wrong value in list is 2^{-88}, we expect the number of wrong keys left is $N = 2^{88} \times (1 - \frac{2^8}{2^{88}})^{2^{n+47}} = 2^{88} \times (1 - 2^{-80})^{2^{80} \times 2^{n-33}} \approx 2^{88} \times 2^{-1.44 \times 2^{n-33}} < 1$, then we have $n = 38.94$.

6.3 Complexity Analysis

The data complexity is $2^{n+72} = 2^{110.94}$ chosen plaintexts.

The time complexity of data collecting phase is $2^{110.94}$ 10-round encryptions.

Step 1 requires $2 \times 2^{n+39} \times 2^{24} = 2^{102.94}$ one-round encryptions.

Step 2 requires $2 \times 2^{n+39} \times 2^{24} \times 2^4 = 2^{106.94}$ one-round encryptions.

Step 3 requires $2 \times 2^{n+39} \times 2^{12} \times 2^{20} = 2^{110.94}$ one-round encryptions.

Step 4 requires 2^{40} 10-round encryptions.

$2^{110.94} + 2^{102.94}/10 + 2^{106.94}/10 + 2^{110.94}/10 + 2^{40} \approx 2^{111}$ 10-round encryptions.

7 Impossible Differential Attack on 11-Round Midori128

In this section, we present a new impossible differential attack on Midori128 with the new impossible differential characteristic $(**0000**) \rightarrow (00****00)$ shown in [19]. We launch our attack like the way in Sect. 6. We start Midori128 at round 0, and place this impossible differential path at round 2 to 8, then add two rounds before the 7-round impossible differential and three rounds after it. We illustrate the states of each round in Fig. 8.

7.1 Data Collecting Phase

We take all possible values in the nine cells at position $[1, 2, 5, 7, 10, 11, 13, 14, 15]$ of plaintext P and remain other cells constants. Then we take the $2^{8\times 9} = 2^{72}$ plaintexts as a structure, encrypt it through 11-round Midori128 and get the ciphertexts. Insert the corresponding ciphertexts into a hash table indexed by cell positions $[0, 1, 2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15]$. For each row we expect to have $2^{72} \times 2^{-8\times 13} = 2^{-32}$ ciphertexts. Select all possible pairs in each row with more than one ciphertexts, we expect to have $2^{(-32)\times 2-1} \times 2^{8\times 13} = 2^{39}$ pairs. We take 2^n structures and get 2^{n+39} pairs with zero difference in cell $[0, 1, 2, 3, 7, 8, 9, 10, 11, 12, 13, 14, 15]$.

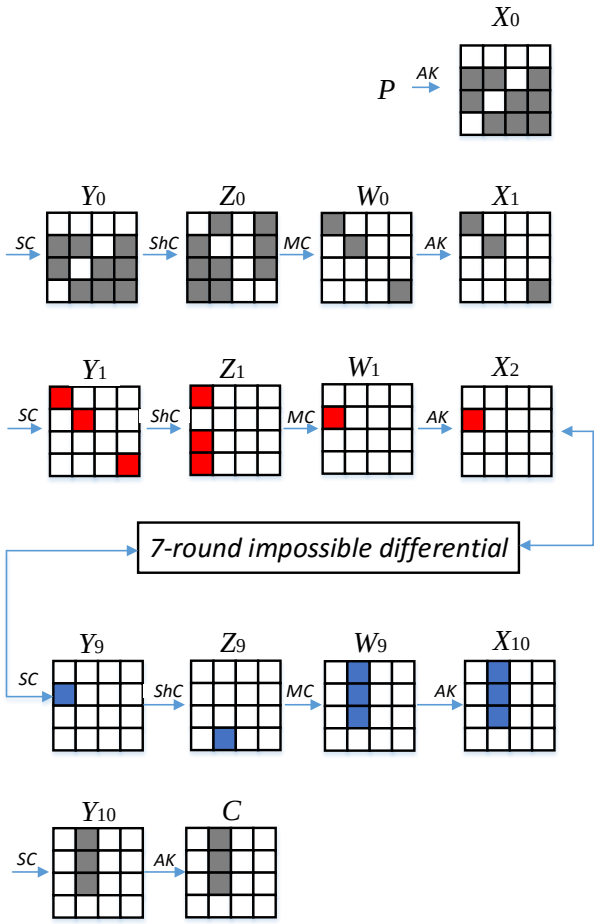

Fig. 8. 11-round impossible differential attack on Midori128

7.2 Key Recovering Phase

In this phase, we eliminate wrong values of the 11-byte key $K[0,1,2,4,5,6,7,10,11,13,14,15]$ by showing that the impossible differential path holds if these keys were used.

Step 1 For each of the 2^{n+39} pairs, guess the 24-bits difference values $\triangle X_1[0,5,15]$, then deduce $\triangle Y_0[1,2,5,7,10,11,13,14,15]$, $X_0[1,2,5,7,10,11,13,14,15]$ and $Y_0[1,2,5,7,10,11,13,14,15]$ can be got from $\triangle Y_0$ and $\triangle X_0 = \triangle P$ according to the property 1. Then compute the master $K[1,2,5,7,10,11,13,14,15]$ from the P and X_0. In this step, we get 2^{24} values of $K[1,2,5,7,10,11,13,14,15]$.

Step 2 For each pair in step 1, guess the 4-bit difference values of $\triangle X_2[1]$ (the differences with the pattern $(**0000**)$), then deduce $\triangle Y_1[0,5,15]$. According to the property 1, $X_1[0,5,15]$ and $Y_1[0,5,15]$ can be got from $\triangle Y_1[0,5,15]$ and $\triangle X_1[0,5,15]$ which was guessed in step 1. As the values of $Y_0[1,2,5,7,10,11,13,14,15]$ are known in step 1, $W_1[0,5,15]$ can be got and we can compute the subkey $K_0[0,5,15]$. In this step, we get 2^4 values of $K_0[0,5,15]$. As the $K_0 = K \oplus \beta_0$, we have two 8-bit linear equation in position $(5,15)$ and there is a key independent sieve for the key we deduced. So we expect $2^{24} \times 2^4 \times 2^{-8\times 2} = 2^{12}$ different master key $K[0,1,2,5,7,10,11,13,14,15]$ left after this step.

Step 3 For each pair in step 2, guess the 4-bits values of $\triangle Y_9[1]$ with the bit pattern $(00****00)$, then deduce 2^4 $\triangle X_{10}[4,5,6]$, as the difference $\triangle Y_{10} = \triangle C$, $X_{10}[4,5,6]$ and $Y_{10}[4,5,6]$ can be got according to the property 1. Then the master key $K[4,5,6]$ can be computed by $Y_{10}[4,5,6]$ and C. Notice that there are two bytes key $K[5,6]$ repeated with the key deduced in step 1 and 2. Compare the 16-bit value, if they are unequal, discard this value. We expect $2^4 \times 2^{12} \times 2^{-8\times 2} = 1$ value left after this step.

Step 4 After guess and eliminate for 2^{n+39} pairs, if there are keys left of the 88-bit master key, exhaustive search the other 40-bit master key to get and examine the right key.

Note that for each pair, we could get 1 value of the 11-byte key $K[0,1,2,4,5,6,7,10,11,13,14,15]$. We want to eliminate all the values in the subkey list unless the value of subkey is correct. The probability of a wrong value in list is 2^{-88},we expect the number of wrong keys left is $N = 2^{88} \times (1 - \frac{2^1}{2^{88}})^{2^{n+39}} = 2^{88} \times (1 - 2^{-88})^{2^{88}\times 2^{n-49}} \approx 2^{88} \times 2^{-1.44\times 2^{n-49}} < 1$, then we have $n = 54.94$.

7.3 Complexity Analysis

The data complexity is $2^{n+72} = 2^{126.94}$ chosen plaintexts.

The time complexity of data collecting phase is $2^{126.94}$ 11-round encryptions.

Step 1 requires $2 \times 2^{n+39} \times 2^{24} = 2^{118.94}$ one-round encryptions.

Step 2 requires $2 \times 2^{n+39} \times 2^{24} \times 2^4 = 2^{122.94}$ one-round encryptions.

Step 3 requires $2 \times 2^{n+39} \times 2^{12} \times 2^4 = 2^{110.94}$ one-round encryptions.

Step 4 requires 2^{40} 11-round encryptions.

$2^{126.94} + 2^{118.94}/11 + 2^{122.94}/11 + 2^{110.94}/11 + 2^{40} \approx 2^{126.94}$ 11-round encryptions.

8 Conclusion

In this paper, we present a new cryptanalysis of Midori128 by using the impossible differential attack. We achieve 10-round impossible differential attack on Midori128 with time complexity 2^{111} which is better than the result before by Chen *et al.*. And then we extend the attack one more round to 11 rounds. The time and data complexity are both $2^{126.94}$ for our 11-round impossible differential attack on Midori128. The attacks of all previous attacks on Midori are listed in Tab. 1. Our results are the best single-key cryptanalytic results on Midori128 as far as we know, which have no threaten the security of full-round Midori128.

Acknowledgments. We would like to extend my sincere gratitude to the anonymous reviewers for their time and advice on this paper.

References

1. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A block cipher for low energy. In: Advances in CryptologyCASIACRYPT 2015, pp. 411C436. Springer (2014)
2. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK lightweight block ciphers. In Proceedings of the 52nd Annual Design Automation Conference (p. 175). ACM (2015, June)
3. 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)
4. 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.
5. Bogdanov, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J., ... Vikkelsoe, C.: PRESENT: An ultra-lightweight block cipher (pp. 450-466). Springer Berlin Heidelberg (2007)
6. Chen, Z, Wang, X. Impossible Differential Cryptanalysis of Midori[J]. IACR Cryptology ePrint Archive, 2016, 2016: 535.
7. Chen Z, Chen H, Wang X. Cryptanalysis of Midori128 Using Impossible Differential Techniques[C]//International Conference on Information Security Practice and Experience. Springer International Publishing, 2016: 1-12.
8. De Canniere, C., Dunkelman, O., Kneževi, M.: KATAN and KTANTAN a family of small and efficient hardware-oriented block ciphers. In Cryptographic Hardware and Embedded Systems-CHES 2009 (pp. 272-288). Springer Berlin Heidelberg (2009)
9. Dong X, Shen Y. Cryptanalysis of reduced-round midori64 block cipher[R]. Cryptology ePrint Archive, Report 2016/676, 2016.
10. Gérault, D, Lafourcade, P. Related-Key Cryptanalysis of Midori[C]//Progress in CryptologyCINDOCRYPT 2016: 17th International Conference on Cryptology in India, Kolkata, India, December 11-14, 2016, Proceedings 17. Springer International Publishing, 2016: 287-304.
11. Gong, Z., Nikova, S., Law, Y. W.: KLEIN: a new family of lightweight block ciphers (pp. 1-18). Springer Berlin Heidelberg (2011)

12. Guo, J, Jean, J, Nikolic, I, et al. Invariant Subspace Attack Against Full Midori64[J]. IACR Transactions on Symmetric Cryptology, [S.l.], p. 33-56, dec. 2016. ISSN 2519-173X. http://tosc.iacr.org/index.php/ToSC/article/view/534.
13. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.: The LED block cipher. In Cryptographic Hardware and Embedded Systems CHES 2011 (pp. 326-341). Springer Berlin Heidelberg (2011)
14. 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)
15. Kim, J, Hong, S, Lim, J. Impossible differential cryptanalysis using matrix method[J]. Discrete Mathematics, 2010, 310(5): 988-1002.
16. Knudsen, L.: DEAL - A 128-bit Block Cipher. In: NIST AES Proposal (1998)
17. Lin, L, Wu, W. Meet-in-the-Middle Attacks on Reduced-Round Midori-64[J]. IACR Transactions on Symmetric Cryptology, [S.l.], p. 215-239, mar. 2017. ISSN 2519-173X. http://tosc.iacr.org/index.php/ToSC/article/view/592.
18. Mendel F., Rechberger C., Schläffer M., Thomsen S.S., The rebound attack: cryptanalysis of reduced Whirlpool and Grøstl, in: Fast Software Encryption, (pp. 260C276). Springer, (2009).
19. Sasaki, Y, Todo, Y. New Impossible Differential Search Tool from Design and Cryptanalysis Aspects[J]. Cryptology ePrint Archive, Report 2016/1181, 2016. http://eprint.iacr.org/2016/1181.
20. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: an ultra-lightweight blockcipher. In Cryptographic Hardware and Embedded Systems CHES 2011 (pp. 342-357). Springer Berlin Heidelberg (2011)
21. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA. In Fast software encryption (pp. 181-195). Springer Berlin Heidelberg (2007, March)
22. Todo, Y, Leander, G, Sasaki, Y. Nonlinear Invariant Attack: Practical Attack on Full SCREAM, i SCREAM, and Midori 64[C]//Advances in CryptologyCASIACRYPT 2016: 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II 22. Springer Berlin Heidelberg, 2016: 3-33.
23. Wu S, Wang M. Automatic search of truncated impossible differentials for word-oriented block ciphers[C]//International Conference on Cryptology in India. Springer Berlin Heidelberg, 2012: 283-302.