SAT-Aided Differential Cryptanalysis of Lightweight Block Ciphers Midori, MANTIS and QARMA

Yaxin Cui, Hong Xu(✉), Lin Tan, and Wenfeng Qi

Information Engineering University, Zhengzhou, China
xuhong0504@163.com

Abstract. Lightweight primitives have already received a lot of attention with the growth of resource-constrained devices, and many lightweight block ciphers such as Midori, MANTIS and QARMA have been proposed in recent years. In this paper, we present a SAT-aided search of the optimal (related-tweak) differential characteristics for such block ciphers combined with the Matsui's bounding conditions and the technique of dichotomy. Using this method, we find the optimal differential characteristics for Midori-128 up to 10 rounds, and the optimal related-tweak differential characteristics for QARMA-64 and MANTIS up to 11 rounds and 10 rounds respectively. To obtain better attacks, we add some constraints into the search model to restrict the number of active S-boxes for input and output differences. As a result, we give a differential attack on 12-round Midori-128 based on the found 10-round differential characteristic with probability 2^{-115}. Moreover, we present a related-tweak differential attack on 11-round QARMA-64 based on the optimal 9-round differential characteristic with probability 2^{-52}, which improves the previous attacks as far as we know.

Keywords: Differential attack · Lightweight block cipher · Matsui's bounding conditions · The technique of dichotomy

1 Introduction

In the last decades, more and more lightweight primitives have been widely used in resource-constrained devices or environments such as RFID tags and sensor networks. The strong demand from industry has led to the design of a large number of lightweight block ciphers including PRESENT [6], PRINCE [7], Midori [2], GIFT [3], SKINNY and MANTIS [4], and QARMA [1], where the last two block ciphers are also tweakable block ciphers.

Midori is a low-energy lightweight block cipher with SPN structure proposed by Banik *et al.* at AISACRYPT 2015, which has two versions with different block size, *i.e.*, Midori-64 and Midori-128. Banik *et al.* [2] estimated the number of differentially active S-boxes for Midori-128, and evaluated that there were no 13-round differential characteristics with probability higher than 2^{-128}. Then,

D. Wang et al. (Eds.): ICICS 2023, LNCS 14252, pp. 3–18, 2023.
https://doi.org/10.1007/978-981-99-7356-9_1

Chen *et al.* [9] utilized a 6-round impossible differential characteristic to present an impossible differential attack on 10-round Midori-128. In 2019, Zhang *et al.* [20] found a 7-round integral distinguisher for Midori-128. Using Midori's round function and PRINCE's refection structure, Beierle *et al.* presented a low-latency tweakable block cipher MANTIS, which has a 64-bit block length, and works with a 128-bit key and 64-bit tweak. Some related-tweak differential characteristics were found by hand or MILP method [8,11,12]. With the MILP method, Chen *et al.* [8] found a 10-round multiple differential characteristic with probability $2^{-55.98}$, and derived a related-tweak differential attack on 12-round MANTIS. QARMA is a new family of lightweight tweakable block ciphers with reflection feature presented by Avanzi *et al.* at FSE 2017, which targets some special uses such as memory encryption and short tags for software security. There are two variants of QARMA that support block sizes of 64 and 128 bits, denoted by QARMA-64 and QARMA-128. Subsequently, many various attacks on QARMA-64 have been proposed [13,14,21,22]. In 2020, Liu *et al.* [15] proposed an 11-round related-tweak impossible differential attack with $2^{58.38}$ chosen plaintexts and $2^{64.92}$ encryptions to recover 64 key bits, which didn't include the outer whitening keys.

Recently, automatic searching techniques have been used in finding differential and linear characteristics, such as Mixed-Integer Linear Programming (MILP) method and Boolean Satisfiability (SAT) method/Satisfiability Modulo Theories (SMT) method [10]. With SAT method, Sun *et al.* [17] converted the Matsui's bounding conditions [16] into Boolean formulas, and evaluated the accelerating effect under different sets of bounding conditions. In this way, they achieved to accelerate the search of differential and linear characteristics for PRESENT, GIFT, RECTANGLE, LBlock and TWINE [17–19].

Our Contributions. We combine the Matsui's bounding conditions and the technique of dichotomy to accelerate the search of differential characteristics for lightweight block cipher with SAT method in this paper. As a result, we obtain the optimal differential characteristics for 10-round Midori-128, and the optimal related-tweak differential characteristics for 11-round QARMA-64 and 10-round MANTIS respectively. To obtain better attacks on Midori-128, we add some constraints into the search model to restrict the number of active S-boxes of input and output differences. Specifically, we find a 10-round differential characteristic with probability 2^{-115}, which has 20 active S-boxes of input and output differences, and present a differential attack on 12-round Midori-128. For QARMA-64, we add one round at the beginning and the ending of the optimal 9-round related-tweak differential characteristic with probability 2^{-52}, and present an 11-round differential attack to recover all the master keys. Compared with previous attacks, our attack has improved the known related-tweak attack on QARMA-64 with outer whitening keys by one round. The summary of known attacks is shown in Table 1.

Organization. The rest of the paper is organized as follows. In Sect. 2, we present a brief review of Midori-128 and QARMA-64. In Sect. 3, we show how to accelerate the search of optimal differential characteristics with SAT method.

Then, we give the optimal (related-tweak) differential characteristics for Midori-128, QARMA-64 and MANTIS. In Sect. 4, we present a differential attack on 12-round Midori-128 based on a 10-round differential characteristic with probability 2^{-115}. In Sect. 5, we show a related-tweak differential attack on 11-round QARMA-64 based on the optimal 9-round related-tweak differential characteristic with probability 2^{-52}. Finally, we present a short conclusion in Sect. 6.

Table 1. Summary of known attacks on QARMA-64

Rounds	Method	Setting	Outer whitening	Time	Data	Memory	Ref
9	MITM	SK	Yes	2^{89}	2^{16}	2^{89}	[14]
10	MITM	SK	No	2^{116}	2^{53}	2^{116}	[21]
10	Impossible differential	RK	No	$2^{63.8}$	2^{62}	2^{37}	[22]
10	Statistical saturation	RK	Yes	2^{59}	2^{59}	$2^{29.6}$	[13]
11	Impossible differential	RK	No	$2^{64.92}$	$2^{58.38}$	$2^{63.38}$	[15]
11	Differential	RK	Yes	$2^{65.35}$	2^{54}	2^{64}	Sect. 5

2 Preliminaries

2.1 The Lightweight Block Cipher Midori-128

Midori is a family of lightweight block ciphers which is composed of two variants: Midori-64 and Midori-128. The round function consists of four operations SubCell, PermuteCells, MixColumns and AddRoundTweakey, which is shown in Fig. 1. The internal state is divided into sixteen cells

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

For Midori-128, the 8 bits $(127, 126, 125, 124, 123, 122, 121, 120)$ are contained in the 0th cell, and the 8 bits $(7, 6, 5, 4, 3, 2, 1, 0)$ in the 15th cell.

SubCell(S)**.** Midori-128 utilizes four different 8-bit S-boxes SSb_0, SSb_1, SSb_2 and SSb_3. The S-box SSb_i is applied to the i-th row of the internal state where $0 \leq i \leq 3$, which consists of the input bit permutation S_p^i, the output bit permutation $S_{p^{-1}}^i$ and two 4-bit S-boxes Sb_i. More details can be referred to [2].

PermuteCells(P)**.** $(P(IS))_i = s_{P(i)}$ for $0 \leq i \leq 15$, where P is the cell permutation of Midori represented as

$$P = [0, 10, 5, 15, 11, 1, 14, 4, 6, 12, 3, 9, 13, 7, 8, 2].$$

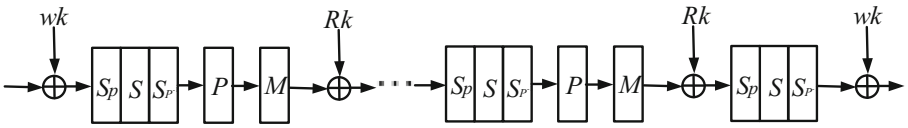

Fig. 1. The lightweight block cipher Midori

Table 2. The S-boxes of Midori-128 and QARMA-64

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S_{\text{Midori}}(x)$	1	0	5	3	E	2	F	7	d	a	9	B	C	8	4	6
$S_{\text{QARMA}}(x)$	A	D	E	6	F	7	3	5	9	8	0	C	B	1	2	4

MixColumns(M)**.** Midori utilizes an involutive binary matrix M defined as follows

$$M = circ(0, 1, 1, 1) = \begin{pmatrix} 0\,1\,1\,1 \\ 1\,0\,1\,1 \\ 1\,1\,0\,1 \\ 1\,1\,1\,0 \end{pmatrix},$$

and each column of the internal state is multiplied by the matrix M.

AddRoundTweakey. Midori-128 utilizes a 128-bit secret key K, and the whitening key is $wk = K$ and the round key is $Rk_i = K \oplus \beta_i$ for $0 \leq i \leq 18$ where β_i are constants. The j-th bit of Rk_i is XORed to the j-th bit of the internal state.

2.2 The Tweakable Block Cipher QARMA-64

QARMA is a family of lightweight tweakable block ciphers proposed in 2017 which has been used by the ARMv8 architecture to support a software protection feature. QARMA-64 is a three-round Even-Mansour construction shown in Fig. 2 where the first r rounds of the cipher (ignoring initial whitening) differ from the last r rounds solely by the addition of a non-zero constant α. The internal state is also divided into sixteen 4-bit cells, and the bits $(63, 62, 61, 60)$ are contained in the 0th cell.

The Forward Round Function is composed of four operations as follows.

AddRoundTweakey. The round tweakey $T = t_0 \| t_1 \cdots \| t_{15}$ is XORed to the internal state. The tweak T is updated by a permutation h and a LFSR ω. First, the cells are permuted as $h(T) = t_{h(0)} \| \cdots \| t_{h(15)}$ where $h = [6, 5, 14, 15, 0, 1, 2, 3, 7, 12, 13, 4, 8, 9, 10, 11]$. Then, a LFSR ω updates the tweak cells with indexes $0, 1, 3, 4, 8, 11, 13$. For QARMA-64, ω is a maximal period LFSR that maps the cell (b_3, b_2, b_1, b_0) to $(b_0 \oplus b_1, b_3, b_2, b_1)$.

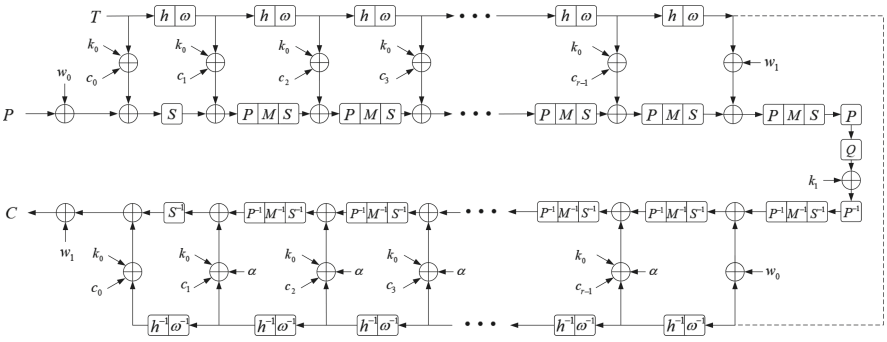

Fig. 2. The tweakable block cipher QARMA

PermuteCells(P)**.** $(P(IS))_i = s_{P(i)}$ for $0 \leq i \leq 15$, where P is the cell permutation represented as

$$P = [0, 11, 6, 13, 10, 1, 12, 7, 5, 14, 3, 8, 15, 4, 9, 2].$$

MixColumns(M)**.** Each column of the internal state is multiplied by the matrix M. The matrix M is defined as follows:

$$M = circ(0, \rho^a, \rho^b, \rho^c) = \begin{pmatrix} 0 & \rho^a & \rho^b & \rho^c \\ \rho^c & 0 & \rho^a & \rho^b \\ \rho^b & \rho^c & 0 & \rho^a \\ \rho^a & \rho^b & \rho^c & 0 \end{pmatrix},$$

where ρ^i is just a simple left circular rotation of the element by i bits. For QARMA-64, $a = c = 1$ and $b = 2$, and the matrix is involutory.

SubCell(S)**.** The 4-bit S-box is applied to each cell of the internal state, and the details are shown in Table 2.

The 128-bit key K is partitioned as $w_0 \| k_0$, where w_0 is 64-bit whitening key and k_0 is 64-bit core key. For encryption, put $w_1 = (w_0 \ggg 1) \oplus (w_0 \gg 63)$ and $k_1 = k_0$. For decryption, $k_0 \oplus \alpha$ is used as the core key, and the whitening keys w_0 and w_1 are swapped.

3 Searching the Optimal Differential Characteristics with SAT Method

In this section, we achieve to accelerate the search of differential characteristics for lightweight block ciphers with SAT method, and present some searching results for Midori-128, QARMA-64 and MANTIS.

To build a SAT model for a block cipher, we first need to convert differential propagations of the round function into Boolean formulas. QARMA-64 and MANTIS adopt 4-bit S-boxes, and Midori-128 utilizes 8-bit S-boxes. For

Midori-128, we divide the 8-bit S-box operation into the 4-bit S-box operation and the linear permutation operation. Therefore, we only introduce the differential propagations of the 4-bit S-box operation and the XOR operation in the following.

XOR Operation. For an n-bit XOR operation, $\alpha = (\alpha_{n-1}, \cdots, \alpha_1, \alpha_0)$ and $\beta = (\beta_{n-1}, \cdots, \beta_1, \beta_0)$ are two input differences, and the output difference is $\gamma = (\gamma_{n-1}, \cdots, \gamma_1, \gamma_0)$. The differential holds if and only if the values of α, β and γ validate all the assertions in the following.

$$\begin{cases} \overline{\alpha_i} \vee \beta_i \vee \gamma_i = 1 \\ \alpha_i \vee \overline{\beta_i} \vee \gamma_i = 1 \\ \alpha_i \vee \beta_i \vee \overline{\gamma_i} = 1 \\ \overline{\alpha_i} \vee \overline{\beta_i} \vee \overline{\gamma_i} = 1 \end{cases},$$

where $0 \leq i \leq n-1$.

The 4-Bit S-Box Operation. For a 4-bit S-box S, denote $\alpha = (\alpha_3, \alpha_2, \alpha_1, \alpha_0) \in \mathbb{F}_2^4$ and $\beta = (\beta_3, \beta_2, \beta_1, \beta_0) \in \mathbb{F}_2^4$ as the input and output differences respectively. The differential distribution tables (DDT) of the S-boxes for Midori-128, QARMA-64 and MANTIS have five possible values which are 0, 2, 4, 8 and 16, and the corresponding probabilities are 0, 2^{-3}, 2^{-2}, 2^{-1} and 1 respectively. For each S-box, three additional variables p_0, p_1 and p_2 are used to encode the non-zero differential probability p, and the encoding rules are as follows.

$$p_0 \parallel p_1 \parallel p_2 = \begin{cases} 001 & \text{if } p = 2^{-1} \\ 011 & \text{if } p = 2^{-2} \\ 111 & \text{if } p = 2^{-3} \\ 000 & \text{if } p = 1 \end{cases}.$$

In this way, we have the opposite number of the binary logarithm of p equals $p_0+p_1+p_2$. Then, we define a function f over the 11-bit vector $(\alpha_3, \cdots, \alpha_0, \beta_3, \cdots, \beta_0, p_0, p_1, p_2)$ as

$$f(\alpha, \beta, p) = \begin{cases} 1 & \text{if } \alpha \to \beta \text{ is a difference progratation with } -\log_2 p = p_0 + p_1 + p_2 \\ 0 & \text{if } \alpha \to \beta \text{ doesn't exist} \end{cases}.$$

Utilizing Logic Friday, we can derive Boolean formulas of the function $f(\alpha, \beta, p_0, p_1, p_2)$.

Setting the Object Function. Based on the above work, we can convert differential propagations of the round function into Boolean formulas to build a SAT model. Assume that N S-boxes are involved in a differential characteristic, the object function is $\sum_{j=1}^{N}(p_0^{(j)} + p_1^{(j)} + p_2^{(j)}) \leq k$ in the SAT model where 2^{-k} is an initial estimation probability. Then, we can utilize the sequential encoding method [5] to convert this constraint into CNF formulas.

Once we set the opposite number of the binary logarithm of an estimation probability as the target value, the SAT model discusses whether the variables

involved in given Boolean formulas can be consistently replaced by the value True or False so that the formulas are evaluated to be True. If this is the case, the formulas are called satisfiable. When the SAT model is satisfiable, we can obtain a solution that indicates there exists a differential characteristic with probability higher than or equal to the current probability. In the previous work, the target value of the object function usually increases by 1 at a time from the initial value until the SAT model is satisfiable. In order to further accelerate the search process, we consider using the technique of dichotomy to set the target value.

Algorithm 1. Searching Method with Dichotomy

Input: the lower bound LB, the upper bound UB
Set $AV \leftarrow \frac{(LB+UB)}{2}$
while (true) **do**
  Build the SAT model M_{AV} when the target value is set to AV
  if M_{AV} is satisfiable **then**
    if $AV == LB + 1$ **then**
      Set $OP \leftarrow AV$
      Break
    end if
    Set $UB \leftarrow AV$
  else
    if $AV == UB - 1$ **then**
      Set $OP \leftarrow UB$
      Break
    end if
    Set $LB \leftarrow AV$
  end if
  Set $AV \leftarrow \frac{(LB+UB)}{2}$
end while
return OP

When searching the optimal r-round differential characteristics, a lower bound LB and an upper bound UB should be given corresponding to the probability values 2^{-LB} and 2^{-UB} respectively. In our experiments, we usually take $LB = OP_{r-1}$ and $UB = n \times OP_{r-1}$, where the optimal probability of $(r-1)$-round characteristic is $2^{-OP_{r-1}}$, and the parameter n should ensure that the SAT model with probability 2^{-UB} is satisfiable. We compute the average value AV of UB and LB, and decide to update the lower bound LB or the upper bound UB to AV by solving the SAT model. When the SAT model M_{AV} is satisfiable and $AV = LB + 1$, we know that the optimal probability of r-round differential characteristic is 2^{-AV} since M_{LB} is unsatisfiable. Similarly, when the SAT model M_{AV} is unsatisfiable and $AV = UB - 1$, the optimal probability should be 2^{-UB}. The details are shown in Algorithm 1.

Setting the Bounding Conditions. To accelerate the search of differential characteristics effectively, we consider adding the Matsui's bounding conditions into the SAT model to avoid the search of unnecessary branches.

For Midori-128, each round has the same function $\mathcal{R}$. We consider that to start the search from the first round, and then extend backwards with the bounding conditions. Let $\Pr_{\mathcal{R}}(i)$ be the optimal probability of the i-round differential characteristics. When we search the optimal r-round differential characteristic, we set $\Pr_{est}(r)$ as an initial estimation probability in our model. An i-round differential characteristic with probability $\Pr(i)$ is a child node located at the i-th level of the searching tree, where $0 < i < r$. The subtree originating from this node will not be explored if the following bounding condition is violated

$$\Pr(i) \cdot \Pr_{\mathcal{R}}(r-i) \geq \Pr_{est}(r).$$

Table 3. The optimal (related-tweak) differential probability

Round	single-key	related-tweak	
	Midori-128	QARMA-64	MANTIS
1	2^{-2}	–	–
2	2^{-8}	1	2^{-4}
3	2^{-14}	2^{-2}	2^{-8}
4	2^{-32}	2^{-4}	2^{-12}
5	2^{-49}	2^{-8}	2^{-20}
6	2^{-67}	2^{-12}	2^{-24}
7	2^{-79}	2^{-26}	2^{-32}
8	2^{-90}	2^{-36}	2^{-40}
9	2^{-96}	2^{-52}	2^{-56}
10	2^{-114}	2^{-60}	2^{-68}
11	–	2^{-80}	–

Table 4. The optimal 10-round differential characteristic of probability 2^{-114} for Midori-128

Round	Input difference
1st	0000 2000 0000 0080 0000 0000 0041 0000
2nd	0000 0000 0000 0000 0000 0001 0000 0000
3rd	0000 0000 0080 0000 0080 0000 0080 0000
4th	0100 0400 0100 0404 0000 0404 0100 0004
5th	0080 2000 0000 2404 8000 0400 0080 0404
6th	0000 0000 8080 0400 0080 0405 8000 0401
7th	0100 0000 0080 0000 0000 0400 0000 0000
8th	0000 0000 0000 0000 0000 0000 8000 0000
9th	0000 0400 0000 0000 0000 0400 0000 0400
10th	8002 0020 0002 0020 8000 0020 8002 0000
output	0110 0511 8528 0105 8438 0414 8538 0515

Table 5. The optimal 9-round related-tweak differential characteristic of probability 2^{-52} for QARMA-64

Round	Input difference	Tweak difference
1st	2042 0108 e103 169a	3000 0000 0003 0098
2nd	0014 1000 0000 0003	0094 1000 0000 0003
3rd	0008 0004 0008 0000	0001 0094 0008 0000
4th	0010 0000 0080 0000	c000 0001 2000 0008
5th	0004 6000 8000 2000	0004 6000 8000 2000
central structure	0000 0000 0000 0000	–
6th	0000 0000 0000 0000	0004 6000 8000 2000
7th	0004 6000 8000 2000	c000 0001 2000 0008
8th	0010 0000 0080 0000	0001 0094 0008 0000
9th	0008 0004 0008 0000	0094 1000 0000 0003
output	0014 1000 0000 0003	

Table 6. The optimal 10-round related-tweak differential characteristic of probability 2^{-68} for MANTIS

Round	Input difference	Tweak difference
1st	0a00 00a0 0000 00a0	0000 f000 f000 0f00
2nd	0f0f 00f0 00ff 00f0	0000 0000 00ff f000
3rd	0000 0a00 0a00 00f0	0000 0000 0f00 00ff
4th	0000 0000 f000 f000	00ff 0000 0000 0f00
5th	0000 00ff 00f0 0000	0000 00ff 00f0 0000
central structure	0000 0000 0000 0000	–
6th	0000 0000 0000 0000	0000 00ff 00f0 0000
7th	0000 00ff 00f0 0000	00ff 0000 0000 0f00
8th	0000 0000 f000 f000	0000 0000 0f00 00ff
9th	0000 0a00 0a00 00f0	0000 0000 00ff f000
10th	0f0f 00a0 00af 00a0	0000 f000 f000 0f00
output	0a00 00a0 0000 00a0	

For a $2r$-round reflection block cipher such as QARMA and MANTIS, suppose that E_1 and E_2 are the r-round sub-ciphers with round function $\mathcal{R}$ and $\mathcal{R}^{-1}$ respectively. Since different round functions are used in a reflection block cipher, our idea is to start the search from the middle function, and then extend forwards and backwards with the Matsui's bounding conditions.

When we try to search the optimal (n_1+n_2)-round differential characteristic, we need to precompute the optimal probabilities $\mathrm{Pr}_{\mathcal{R}}(i)$ and $\mathrm{Pr}_{\mathcal{R}^{-1}}(i)$ of the i-round differential characteristic for E_1 and E_2 respectively where $1 \leq i \leq r$.

Due to reflection feature, we have $\Pr_{\mathcal{R}}(i) = \Pr_{\mathcal{R}^{-1}}(i)$ to reduce the amount of precomputation by half. Let $\Pr_{est}(n_1 + n_2)$ be an initial estimation probability of a $(n_1 + n_2)$-round differential characteristic. A $(t_1 + t_2)$-round differential characteristic with probability $\Pr(t_1 + t_2)$ is a child node located at the $(t_1 + t_2)$-th level of the searching tree, where $t_1 \leq n_1$ and $t_2 \leq n_2$. The subtree originating from this node will not be explored if the following bounding condition is violated

$$\Pr(t_1 + t_2) \cdot \Pr_{\mathcal{R}}(n_1 - t_1) \cdot \Pr_{\mathcal{R}^{-1}}(n_2 - t_2) \geq \Pr_{est}(n_1 + n_2).$$

With the encoding method introduced in [17], the above bounding conditions could be converted into Boolean formulas to accelerate the search.

Based on our SAT model, we obtain the optimal (related-tweak) differential probability for Midori-128, QARMA-64 and MANTIS, which are shown in Table 3. It is worth noting that we only concern about the optimal related-tweak differential probability for $(n_1 + n_2)$-round QARMA-64 and MANTIS where $0 \leq |n_1 - n_2| \leq 1$. For Midori-128, we find the optimal 10-round differential characteristic with probability 2^{-114} shown in Table 4. For QARMA-64, the optimal 9-round related-tweak differential characteristic with probability 2^{-52} is shown in Table 5. For MANTIS, the optimal 10-round related-tweak differential characteristic with probability 2^{-68} is shown in Table 6.

4 Differential Attack on 12-Round Midori-128

From Table 4, we know that the number of active nibbles for output differences is too large. To present better attacks on Midori-128, we put additional constraints on the number of active nibbles for input and output differences into the SAT model, and find a 10-round differential characteristic with probability 2^{-115} shown in Table 7, where input and output differences have totally 20 active nibbles. Based on this 10-round differential characteristic, we add one round at the beginning and the ending to present a differential attack on 12-round Midori-128. The key-recovery process is shown in Fig. 3, where the symbol "$*$" represents an active nibble with unknown difference, and the symbol "?" represents an unknown difference bit. In addition, the 0th cell contains the 0th and 1st nibbles, the 1st cell contains the 2nd and 3rd nibbles, and so on.

We choose plaintexts P where all possible values of 92 active bits are traversed, and the other bits are set to constants, and then get $2^{92+92-1}$ plaintext pairs $(P, \overline{P})$ satisfying the input difference. If we construct N structures by choosing different constants, $N_R = N \cdot 2^{183} \cdot 2^{-92} \cdot 2^{-115}$ right pairs will be identified on average. We want to obtain one right pair, and construct $N = 2^{24}$ structures to have $2^{24} \cdot 2^{183-84} = 2^{123}$ plaintext-ciphertext pairs satisfying the output difference.

Table 7. The 10-round differential characteristic of probability 2^{-115} for Midori-128

Round	Input difference
1st	0084 0484 0100 0110 3001 0001 0000 0000
2nd	0000 0020 0000 8000 0080 0000 0000 0000
3rd	0000 0000 0000 0100 0000 0000 0000 0000
4th	0000 0000 0000 8000 0000 8000 0000 8000
5th	0402 0000 0002 0100 0400 0100 0402 0100
6th	0001 8004 0041 8000 0040 0004 0101 0000
7th	0280 0020 0280 0800 0000 0000 0200 0920
8th	0001 0000 4000 0000 0000 0000 0000 0400
9th	0080 0000 0000 0000 0000 0000 0000 0000
10th	0080 0000 0000 0000 0080 0000 0080 0000
output	00a0 0100 0000 0104 00a0 0104 00a0 0004

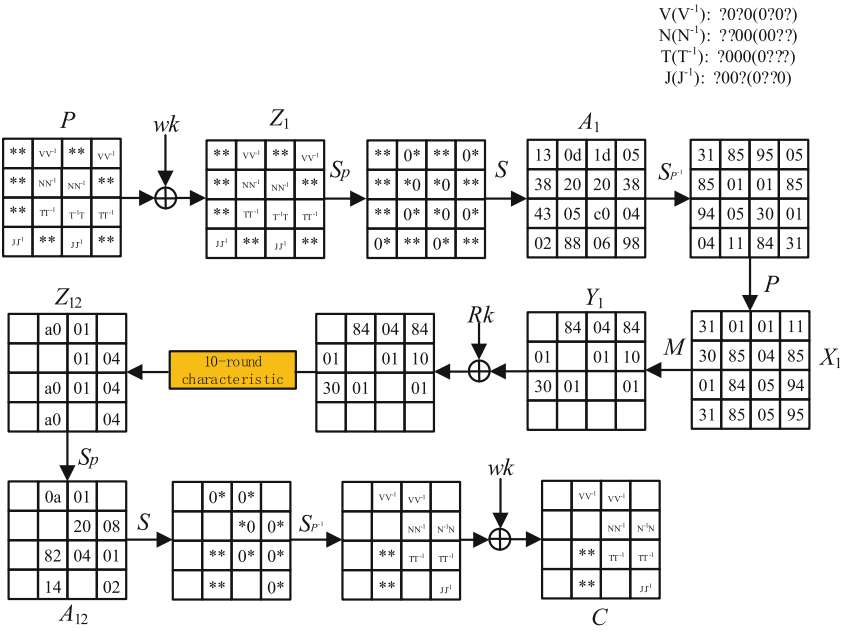

Fig. 3. Differential key-recovery attack on 12-round Midori128

Step 1: recovering the same key bits used in the first and the last round. For 2^{123} chosen plaintext-ciphertext pairs, we first guess 4 key bits $wk[17, 18, 20, 23]$, and encrypt the corresponding values of plaintexts to get the differences ΔA_1^{27}. Then, we can decrypt the corresponding values of ciphertexts by the same key

bits to get the differences ΔA_{12}^{27}. The time complexity is $2 \times 2^{123} \times 2^4 \times \frac{1}{32} = 2^{123}$ one-round encryptions.

Then, we guess 4 key bits $wk[16, 19, 21, 22]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select 2^{120} right pairs that satisfy $\Delta A_1^{26} = 8$ and $\Delta A_{12}^{26} = 1$. The time complexity is $2 \times 2^{123} \times 2^8 \times \frac{1}{32} = 2^{127}$ one-round encryptions.

We guess 4 key bits $wk[1, 2, 4, 7]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select $2^{120-2\times4}$ right pairs that satisfy $\Delta A_1^{31} = 8$ and $\Delta A_{12}^{31} = 2$. The time complexity is about $(2^{120} \times 2^{12} + 2^{116} \times 2^{12}) \times \frac{1}{32} \approx 2^{127.09}$ one-round encryptions.

We guess 4 key bits $wk[32, 33, 34, 39]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select $2^{112-2\times4}$ right pairs that satisfy $\Delta A_1^{23} = 4$ and $\Delta A_{12}^{23} = 1$. The time complexity is about $(2^{112} \times 2^{16} + 2^{108} \times 2^{16}) \times \frac{1}{32} \approx 2^{123.09}$ one-round encryptions.

We guess 4 key bits $wk[48, 49, 50, 55]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select $2^{104-2\times4}$ right pairs that satisfy $\Delta A_1^{19} = 5$ and $\Delta A_{12}^{19} = 2$. The time complexity is about $(2^{104} \times 2^{20} + 2^{100} \times 2^{20}) \times \frac{1}{32} \approx 2^{119.09}$ one-round encryptions.

We guess 4 key bits $wk[66, 67, 68, 69]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select $2^{96-2\times4}$ right pairs that satisfy $\Delta A_1^{15} = \Delta A_{12}^{15} = 8$. The time complexity is about $(2^{96} \times 2^{24} + 2^{92} \times 2^{24}) \times \frac{1}{32} \approx 2^{115.09}$ one-round encryptions.

We guess 4 key bits $wk[72, 73, 78, 79]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select $2^{88-2\times4}$ right pairs that satisfy $\Delta A_1^{12} = \Delta A_{12}^{12} = 2$. The time complexity is about $(2^{88} \times 2^{28} + 2^{84} \times 2^{28}) \times \frac{1}{32} \approx 2^{111.09}$ one-round encryptions.

We guess 4 key bits $wk[104, 106, 109, 111]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select $2^{80-2\times4}$ right pairs that satisfy $\Delta A_1^5 = d$ and $\Delta A_{12}^5 = 1$. The time complexity is about $(2^{80} \times 2^{32} + 2^{76} \times 2^{32}) \times \frac{1}{32} \approx 2^{107.09}$ one-round encryptions.

We guess 4 key bits $wk[112, 114, 117, 119]$ to encrypt the corresponding values of plaintexts and decrypt the corresponding values of ciphertexts, and select $2^{72-2\times4}$ right pairs that satisfy $\Delta A_1^3 = d$ and $\Delta A_{12}^3 = a$. The time complexity is about $(2^{72} \times 2^{36} + 2^{68} \times 2^{36}) \times \frac{1}{32} \approx 2^{103.09}$ one-round encryptions.

Step 2: recovering partial key bits in the first round. We guess every four bits of the 56 key bits, and successively encrypt the plaintexts to select $2^{64-14\times4}$ right pairs that satisfy $\Delta A_1^{0,1,4,7,8,9,10,14,16,17,20,25,29,30}$. The time complexity is about $(2^{64} \times 2^{40} + 2^{60} \times 2^{44} + \cdots + 2^{12} \times 2^{92}) \times \frac{1}{32} = 2^{104} \times 14 \times \frac{1}{32} \approx 2^{102.8}$ one-round encryptions.

Step 3: recovering partial key bits in the last round. We guess 4 key bits $wk[40, 41, 42, 47]$ to decrypt the corresponding values of ciphertexts, and select 2^{8-4} right pairs that satisfy $\Delta A_{12}^{21} = 4$. The time complexity is $2^8 \times 2^{96} \times \frac{1}{32} = 2^{99}$ one-round encryptions. Then, we guess 4 key bits $wk[51, 52, 53, 54]$ to decrypt the corresponding values of ciphertexts, and select 2^{4-4} right pair that satisfies $\Delta A_{12}^{18} = 8$. The time complexity is $2^4 \times 2^{100} \times \frac{1}{32} = 2^{99}$ one-round encryptions.

Step 4: exhaustively searching for the remaining keys. Exhaustively search the remaining $128 - 100 = 28$ unknown key bits in the master key.

The time complexity of the key-recovery process is approximately $2 \times (2^{127} + 2^{127.09}) \times \frac{1}{12} + 2^{28} \approx 2^{125.46}$ 12-round encryptions, and the data complexity is $2^{92} \times 2^{24} = 2^{116}$ plaintexts.

5 Related-Tweak Differential Attack on 11-Round QARMA-64

In this section, we present a related-tweak differential attack on 11-round QARMA-64 by adding one round at the beginning and the ending of the optimal 9-round differential characteristic respectively. The key-recovery process is shown in Fig. 4, where green nibbles represent the unknown differences.

Choose two tweaks $(T, \overline{T})$ such that the difference of the 6th nibble is 7, the difference of the 10th nibble is 9, the difference of the 11th nibble is 8 and the difference of the 13th nibble is 3. Under the tweak T, we can choose plaintexts P where the 0th, 2nd, 3rd, 5th, 7th, 8th, 9th, 11th, 12th, 13th, 14th and 15th nibbles are traversed by all possible values, and the other nibbles are set to constants. Under the tweak $\overline{T}$, we can construct plaintexts $\overline{P}$ where the 0th, 2nd, 3rd, 5th, 7th, 8th, 9th, 11th, 12th, 13th, 14th and 15th nibbles are traversed by all possible values, $P^6 \oplus \overline{P^6} = 7$, $P^{10} \oplus \overline{P^{10}} = 9$, and other nibbles are set to the same constants as P. Therefore, we can get $2^{2\times 48-1} = 2^{95}$ plaintext pairs $(P, \overline{P})$. If we construct N structures by choosing different constants, $N_R = N \cdot 2^{95} \cdot 2^{-48} \cdot 2^{-52}$ right pairs will be identified on average. We want to obtain one right pair, and construct $N = 2^5$ structures to have $2^5 \cdot 2^{95-4\times 12} = 2^{52}$ plaintext-ciphertext pairs satisfying $C^{1,5,6,7,8,9,10,12,13} \oplus \overline{C^{1,5,6,7,8,9,10,12,13}} = 000000000$, $C^0 \oplus \overline{C^0} = 3$, $C^{11} \oplus \overline{C^{11}} = 3$ and $C^{14} \oplus \overline{C^{14}} = 9$. The key-recovery process is shown as allows.

Step 1: recovering partial key bits in the first round. For 2^{52} chosen plaintext-ciphertext pairs, we first guess 4 key bits $(k_0 \oplus w_0)[0-3]$, and partially encrypt the 15th nibble of plaintexts to get the corresponding values of A_2^{15}. The time complexity is about $2^{52} \times 2^4 \times \frac{1}{16} = 2^{52}$ one-round encryptions. Then, we guess every four bits of the 12 key bits $(k_0 \oplus w_0)[4-15]$, and successively encrypt the 14th, 13th and 12th nibble of plaintexts to get the corresponding values of $A_2^{14,13,12}$. There are 2^{48} pairs remained such that $\Delta A_2^{15} = a$, $\Delta A_2^{14} = 9$, $\Delta A_2^{13} = 6$ and $\Delta A_2^{12} = 1$, and the time complexity is about $(2^{52} \times 2^8 + 2^{52} \times 2^{12} + 2^{52} \times 2^{16}) \times \frac{1}{16} \approx 2^{64.09}$ one-round encryptions.

Similarly, we guess every four bits of the 32 key bits $(k_0 \oplus w_0)[16-19, 24-35, 40-44, 48-55, 60-63]$, and successively encrypt the values of the 11th, 9th, 8th, 7th, 5th, 3rd, 2nd, 0th nibble of plaintexts to get the corresponding values of $A_2^{11,9,8,7,5,3,2,0}$. There are $2^{48-8\times 4}$ pairs remained such that $\Delta A_2^{11} = 3$, $\Delta A_2^9 = 1$, $\Delta A_2^8 = e$, $\Delta A_2^7 = 8$, $\Delta A_2^5 = 1$, $\Delta A_2^3 = 2$, $\Delta A_2^2 = 4$ and $\Delta A_2^0 = 2$, and the time complexity is $(2^{48} \times 2^{20} + 2^{44} \times 2^{24} + 2^{40} \times 2^{28} \cdots + 2^{20} \times 2^{48}) \times \frac{1}{16} = 2^{68} \times 8 \times \frac{1}{16} = 2^{67}$ one-round encryptions.

Step 2: recovering partial key bits in the last round. Guess every 4 bits of the 16 key bits $(w_1 \oplus k_0)[0-3]$ and $(w_1 \oplus k_0)[44-55]$, and decrypt ciphertexts to obtain

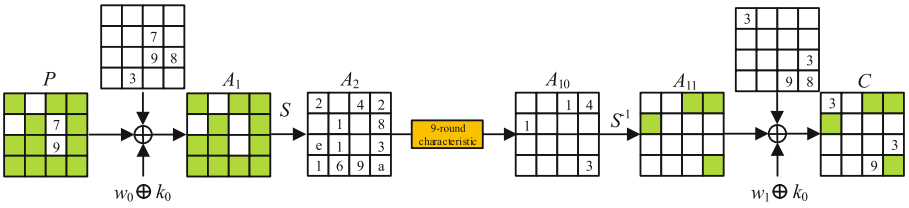

Fig. 4. Differential key-recovery attack on 11-round QARMA-64 (Color figure online)

the differences of the 15th, 4th, 3rd and 2nd nibbles of A_{10}. There is only $2^{16-4\times4}$ pair remained such that $\Delta A_{10}^2 = 1$, $\Delta A_{10}^3 = 4$, $\Delta A_{10}^4 = 1$ and $\Delta A_{10}^{15} = 3$, and time complexity is $(2^{16}\times2^{52}+2^{12}\times2^{56}+2^{8}\times2^{60}+2^{4}\times2^{64})\times\frac{1}{16} = 2^{68}\times4\times\frac{1}{16} = 2^{66}$ one-round encryptions.

Step 3: exhaustively searching for the remaining keys. Exhaustively search the remaining 64 unknown key bits in the master key.

The time complexity of the key-recovery process is approximately $2\times(2^{64.09}+2^{67}+2^{66})\times\frac{1}{11}+2^{64} \approx 2^{65.35}$ 12-round encryptions, and the data complexity is $2\times2^{53} = 2^{54}$ plaintexts. The data-time product complexity is $2^{119.35}$.

6 Conclusion

In this paper, we combine the Matsui's bounding conditions and the technique of dichotomy to accelerate the search of differential characteristics with SAT method, and obtain the optimal (related-tweak) differential characteristics for Midori-128, QARMA-64 and MANTIS. To obtain better attacks on Midori-128, we add some constraints into the search model to restrict the number of active S-boxes for input and output differences. As a result, we find a 10-round differential characteristic with probability 2^{-115} to present a differential attack on 12-round Midori-128. For QARMA-64, we utilize the optimal 9-round related-tweak differential characteristic with probability 2^{-52} to present an 11-round related-tweak differential attack, which improves the previous work to our knowledge.

References

1. Avanzi, R.: The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involutory central rounds, and search heuristics for low-latency s-boxes. IACR Trans. Symmetric Cryptol. **2017**(1), 4–44 (2017)
2. Banik, S., et al.: Midori: a block cipher for low energy. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 411–436. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48800-3_17

3. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Yu., Sim, S.M., Todo, Y.: GIFT: a small present. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66787-4_16
4. Beierle, C., et al.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_5
5. Blondeau, C., Gérard, B.: Multiple differential cryptanalysis: theory and practice. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 35–54. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-21702-9_3
6. Bogdanov, A., et al.: PRESENT: an ultra-lightweight block cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74735-2_31
7. Borghoff, J., et al.: PRINCE – a low-latency block cipher for pervasive computing applications. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_14
8. Chen, S., Liu, R., Cui, T., Wang, M.: Automatic search method for multiple differentials and its application on MANTIS. Sci. China Inf. Sci. **62**(3), 32111:1–32111:15 (2019). https://doi.org/10.1007/s11432-018-9658-0
9. Chen, Z., Chen, H., Wang, X.: Cryptanalysis of Midori128 using impossible differential techniques. In: Bao, F., Chen, L., Deng, R.H., Wang, G. (eds.) ISPEC 2016. LNCS, vol. 10060, pp. 1–12. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-49151-6_1
10. Cook, S.A.: The complexity of theorem-proving procedures. In: Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, Shaker Heights, Ohio, USA, 3–5 May 1971, pp. 151–158. ACM (1971)
11. Dobraunig, C., Eichlseder, M., Kales, D., Mendel, F.: Practical key-recovery attack on MANTIS5. IACR Trans. Symmetric Cryptol. **2016**(2), 248–260 (2016)
12. Eichlseder, M., Kales, D.: Clustering related-tweak characteristics: application to MANTIS-6. IACR Trans. Symmetric Cryptol. **2018**(2), 111–132 (2018)
13. Li, M., Hu, K., Wang, M.: Related-tweak statistical saturation cryptanalysis and its application on QARMA. IACR Trans. Symmetric Cryptol. **2019**(1), 236–263 (2019)
14. Li, R., Jin, C.: Meet-in-the-middle attacks on reduced-round QARMA-64/128. Comput. J. **61**(8), 1158–1165 (2018)
15. Liu, Y., Zang, T., Gu, D., Zhao, F., Li, W., Liu, Z.: Improved cryptanalysis of reduced-version QARMA-64/128. IEEE Access **8**, 8361–8370 (2020)
16. Matsui, M.: On correlation between the order of S-boxes and the strength of DES. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 366–375. Springer, Heidelberg (1995). https://doi.org/10.1007/BFb0053451
17. Sun, L., Wang, W., Wang, M.: Accelerating the search of differential and linear characteristics with the SAT method. IACR Trans. Symmetric Cryptol. **2021**(1), 269–315 (2021)
18. Sun, L., Wang, W., Wang, M.: Improved attacks on GIFT-64. In: AlTawy, R., Hülsing, A. (eds.) SAC 2021. LNCS, vol. 13203, pp. 246–265. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-99277-4_12
19. Sun, L., Wang, W., Wang, M.: Linear cryptanalyses of three AEADs with GIFT-128 as underlying primitives. IACR Trans. Symmetric Cryptol. **2021**(2), 199–221 (2021)

20. Zhang, W., Rijmen, V.: Division cryptanalysis of block ciphers with a binary diffusion layer. IET Inf. Secur. **13**(2), 87–95 (2019). https://doi.org/10.1049/iet-ifs.2018.5151
21. Zong, R., Dong, X.: Meet-in-the-middle attack on QARMA block cipher. IACR Cryptology ePrint Archive, p. 1160 (2016)
22. Zong, R., Dong, X.: MILP-aided related-tweak/key impossible differential attack and its applications to QARMA, Joltik-BC. IEEE Access **7**, 153683–153693 (2019)