Impossible Differential Attack on the QARMA Family of Block Ciphers

Dong Yang, Wenfeng Qi*, Huajin Chen

National Digital Switching System Engineering & Technological Research Center, P. O. Box 407, 62 Kexue Road, Zhengzhou, 450001, China.

Abstract

QARMA is a family of lightweight tweakable block ciphers, which is used to support a software protection feature in the ARMv8 architecture. In this paper, we study the security of QARMA family against the impossible differential attack. First, we generalize the concept of truncated difference. Then, based on the generalized truncated difference, we construct the first 6-round impossible differential dinstinguisher of QARMA. Using the 6-round distinguisher and the time-and-memory trade-off technique, we present 10-round impossible differential attack on QARMA. This attack requires $2^{119.3}$ (resp. $2^{237.3}$) encryption units, 2^{61} (resp. 2^{122}) chosen plaintext and 2^{72} 72-bit (resp. 2^{144} 144-bit) space for QARMA-64 (resp. QARMA-128). Further, if allowed with higher memory complexity (about 2^{116} 120-bit and 2^{232} 240-bit space for QARMA-64 and QARMA-128, respectively), our attack can break up 11 rounds of QARMA. To the best of our knowledge, these results are currently the best results with respect to attacked rounds.

Key words: impossible differential attack, truncated differential, QARMA
2000 MSC: 11B50, 94A55, 94A60

1. Introduction

As the number of low-end devices grows, the security of these devices becomes increasing important. The lightweight block cipher, which is target to provide security solutions to low-end devices, has attracted much attention. Many lightweight primitives, such as PRESENT [1], LBlock [2], SIMON/SPECK [3] and Midori [4] *et al*, have been proposed. Since the widely use of lightweight block ciphers, one problem when using a block cipher should come into notice. That is when the same message is encrypted by the same key in different cases, one will get the same ciphertext. It means that the same ciphertext indicates the same message in different cases. Thus, once the message is obtained by the attacker, it can be detected in other cases. Fortunately, Moses Liskov, Ronald L. Rivest and David Wagner introduced the concept of tweakable block cipher [5], which can provide a solution to the above problem. Unlike the usual block ciphers with only the plaintext and key as inputs, the tweakable block cipher accept a third input called the *tweak*. Together with the key, the tweak can select round functions of a block cipher.

QARMA [6] is a family of lightweight tweakable block ciphers, which is designed for very specific uses, such as memory encryption, generation of very short tags by truncation. The QARMA family adopts the similar structure of PRINCE [7] and contains two versions of block ciphers: 64-bit block version (QARMA-64) and 128-bit block version (QARMA-128). It aims to provide a proposal with conservative security margins while still achieving best-in-class latency. In 2016, QARMA is chosen by ARMv8-A architecture to provide a software protection [8]. The designer analyzed the security of QARMA against differential/linear

☆This work is supported by NSF of China under Grant Nos. (61272042, 61402524, 61602510), and the National 863 Program of China under Grant No. 2015AA01A708

*Corresponding author.
Email addresses: yangdong_sky@126.com (Dong Yang), wenfeng.qi@263.net (Wenfeng Qi), huajin_chen@126.com (Huajin Chen)

[9, 10], impossible differential (ID) [11, 12] and zero-correlation linear attacks [13] *et al.* Based on mixed integer linear programming, they counted the number of active S-boxes of QARMA, and claimed that QARMA is powerful to resist differential/linear attack. With the characteristic matrix technique [14], the designer showed that three rounds of QARMA achieve a full diffusion. Thus, they claimed that 8-round QARMA is sufficient to resist impossible differential and zero-correlation linear attacks. In [15], Zong and Dong presented a 10-round meet-in-the-middle (MITM) attack on QARMA based on the differential enumeration [16] and key-dependent sieve [17] techniques. It is the first attack on QARMA and analyzes the security of QARMA against MITM attack.

Though the security of QARMA against impossible differential attack has been analyzed by the designer, it is not very specific. To more specificly identify the security of QARMA against impossible differential attack, we continue studying the impossible differential attack on QARMA in this paper. First, we generalize the concept of truncated difference inspired by the generalized δ-set [18]. Then, based on the generalized truncated difference, the first 6-round impossible differential distinguisher is constructed. By the 6-round distinguisher and the time-and-memory trade-off technique, we present 10-round impossible differential attack on QARMA. Our attack requires $2^{119.3}$ (resp. $2^{237.3}$) encryption units, 2^{61} (resp. 2^{122}) chosen plaintext and 2^{72} 72-bit (resp. 2^{144} 144-bit) space for QARMA-64 (resp. QARMA-128). Further, if allowed with higher memory complexity (about 2^{116} 120-bit and 2^{232} 240-bit space for QARMA-64 and QARMA-128, respectively), our attack can break up 11 rounds of QARMA. To the best of our knowledge, these results are currently the best results with respect to attacked rounds. Summaries of our attacks and other attacks on QARMA are listed in Table 1.

The paper is organized as follows. Section 2 introduces some necessary preliminaries. Section 3 and 4 present 10-round and 11-round impossible differential attacks on QARMA, respectively. Finally, conclusions are drawn in Section 5.

Table 1: The attacks on QARMA.

Version	Attack	Round	Data	Time	Memory	Ref.
QARMA-64	MITM	10	2^{53}	$2^{70.1}$	2^{116}	[15]
	ID	10	2^{61}	$2^{119.3}$	2^{72}	Section 3
	ID	11	2^{61}	$2^{120.4}$	2^{116}	Section 4
QARMA-128	MITM	10	2^{105}	$2^{141.7}$	2^{232}	[15]
	ID	10	2^{122}	$2^{237.3}$	2^{144}	Section 3
	ID	11	2^{122}	$2^{241.8}$	2^{232}	Section 4

2. Preliminaries

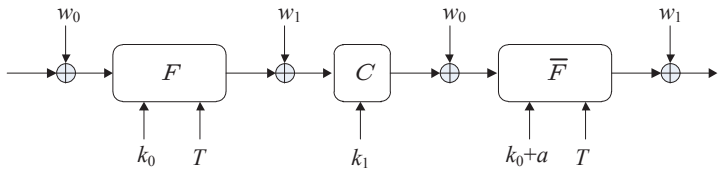
In this section, we briefly introduce the family of QARMA block ciphers, and define some notations.

2.1. A Brief Description of QARMA Family

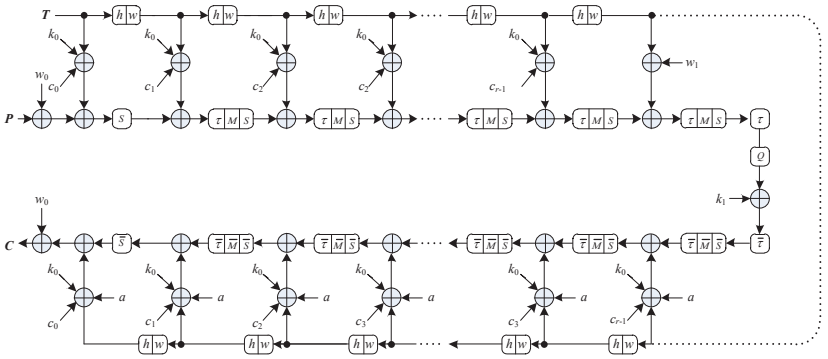
QARMA is a lightweight tweable block cipher proposed by Roberto Avanzi in 2016. The over scheme of QARMA adopts the three-round Even-Mansour construction (Figure 1.*a*) where the permutations are parameterized by a core key, and all the subkeys are deduced from a whitening key. In Figure 1, permutations F and $\overline{F}$ are functionally the inverse of each other, which are parameterized by a tweak. There, throughout this paper, a bar over a function denotes its inverse.

The details of QARMA are shown in Figure 1.*b*. It can be seen that QARMA is a bricklayer SPN. The internal state of QARMA is divided into 16 m-bit nibbles that are represented by a 4×4 array matrix as follows

$$IS = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 \\ 12 & 13 & 14 & 15 \end{bmatrix},$$



a. The Overall Scheme



b. The Structure of QARMA

Figure 1: Details of QARMA.

where $m = 4$ for QARMA-64 and $m = 8$ for QARMA-128. The encryption procedure iteratives 16 rounds for QARMA-64, and 24 rounds for QARMA-128. Next, we introduce operations used in each round.

- **KeyAddition**: The i-th round key is bit-wise XORed to the internal state with the round tweak t and round constant c_i.
- **ShuffleCell** (τ): It applies a permutation P_T to the nibble positions of the internal state, where

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

- **MixColumn** (M): It multiplies each column of the internal state by a matrix Ma. The matrix Ma is defined as follows:

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

  where ρ^i is just a simple left circular rotation of the element by i bits. For QARMA-64, $a = c = 1$ and $b = 1$, and the matrix is involutory. For QARMA-128, $a = 1$, $b = 2$ and $c = 5$, and the inverse of ma is $circ(0, \rho^5, \rho^6, \rho^1)$. The Q in Figure 2 is also a MixColumn operation. It use the same matrix of M for QARMA-64, and use $circ(0, \rho^1, \rho^4, \rho^1)$ for QARMA-128.

- **SubCell** (S): It simply applies non-linear S-box to each nibble of the internal state. Details of the S-boxes please refer to [6].

The keys k_0, k_1, w_0 and w_1 in Figure 1.b are derived from the master key k as follows: $w_0||k_0 = k, w_1 = (w_0 \ggg 1) \oplus (w_0 \gg (16m - 1))$ and $k_1 = k_0$. The tweak is represented by T in Figure 1.b.

2.2. Notations

The following notations will be used throughout this paper.

- x_i : the internal state just after the S or $\overline{S}$ operation of the i-th round.
- y_i : the internal state just after the τ or $\overline{\tau}$ operation of the i-th round.
- z_i : the internal state just after the M or $\overline{M}$ operation of the i-th round.
- w_i : the internal state just after KeyAddition operation of the i-th round.
- $X[j]$: the j-th cell of X, where X is an array of 4×4 cells.
- $\Delta X[j]$: the difference of $X[j]$ and $X^{'}[j]$.
- $X[j_0, j_1, ..., j_l]$: the abbreviation of $X[j_0], X[j_1], ..., X[j_l]$.
- $X[i..j]$: the abbreviation of $X[i], X[i+1], ..., X[j]$.

3. 10-Round Impossible Differential Attack on QARMA

In this section, we first generalize the concept of truncated difference. Then, based on the generalized truncated difference, a 6-round impossible differential characteristic is constructed. Exploiting the 6-round impossible differential characteristic, 10-round impossible differential attack on QARMA is presented.

3.1. Impossible Differential Characteristic of QARMA

In [18], Derbez *et al.* introduced the generalized δ-set in the MITM attack of AES. With the generalized δ-set, the diffusion of active S-boxes can be controlled during the construction of MITM distinguisher. Inspired by this idea, we introduce the generalized truncated differential.

Generalized Truncated Differential. The traditional truncated difference usually focus on a set of differences that some bits are active and the others are constant. In the generalized truncated difference, we can focus on a set of differences that some *linear combinations* of state bits are constant.

Let Γ_0 be a set of differences such that $\Delta z_1[1..11, 13..15] = 0$ and $\Delta z_1[12] \neq 0$. And let Γ_1 be a set of differences such that $\Delta y_6[1..3, 5..15] = 0$, $\Delta z_6[1..3, 5..15] = 0$, $\Delta z_6[0] \neq 0$ and $\Delta z_6[4] \neq 0$. By the property of M operation, it can be verified that $|\Gamma_0| = 2^4 - 1$ and $|\Gamma_1| = 2^2 - 1$ for QARMA-64, $|\Gamma_0| = 2^8 - 1$ and $|\Gamma_1| = 2^2 - 1$ for QARMA-128, where $|\Gamma_0|$ and $|\Gamma_1|$ denotes the number of elements contained in Γ_0 and Γ_1, respectively. Then, we have the following proposition.

Proposition 1. *Let Γ_0 and Γ_1 be truncated differentials defined above. Then, the truncated differential characteristic $\Gamma_0 \xrightarrow{6R} \Gamma_1$ as shown in Figure 2 is an impossible differential characteristic.*

Proof 1. *Since $\Delta z_1[1..11, 13..15] = 0$ and $\Delta z_1[12] \neq 0$, it can be verified that $\Delta y_4[1, 7, 10, 12] = 0$ by going forward three rounds. From the backward, it can be verified that $\Delta y_4[7]$ and $\Delta y_4[10]$ are non-zero, which contradicts with $\Delta y_4[7, 10] = 0$. Thus, the truncated differential $\Gamma_0 \xrightarrow{6R} \Gamma_1$ is impossible.*

Next, we present the 10-round impossible differential attack on QARMA.

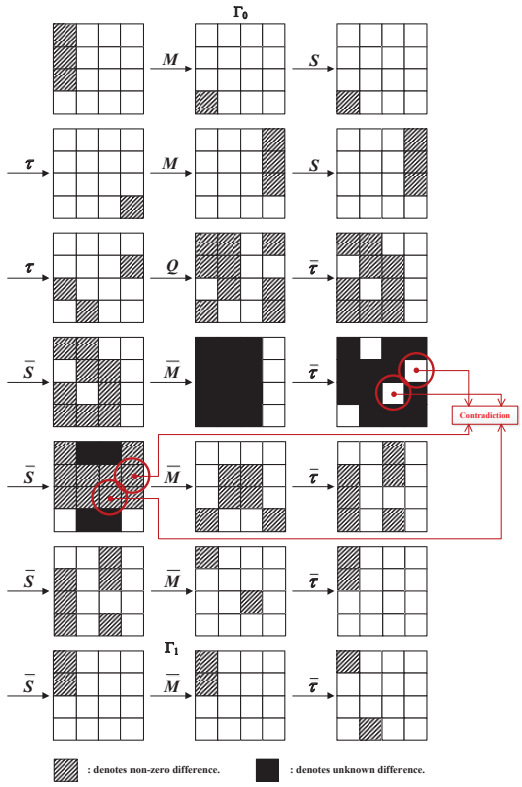


Figure 2: 6-round impossible differential characteristic of QARMA.

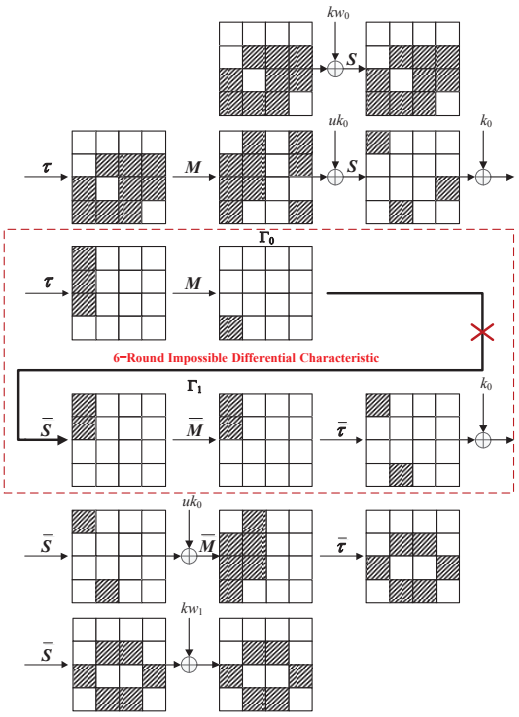


Figure 3: 10-round impossible differential attack on QARMA.

3.2. Details of the 10-Round attack

By appending two rounds on the top and bottom of the 6-round impossible differential characteristic, we get the 10-round attack on QARMA as shown in Figure 3. The uk_0 in Figure 3 is equivalent subkey computed from k_0, namely $uk_0 = M \circ \tau(k_0)$. The kw_0 and kw_1 in Figure 3 represent $k_0 \oplus w_0$ and $k_0 \oplus w_1$, respectively. The details of the 10-round attack are described as follows.

1. Take 2^n structures of plaintext with the following form:

$$P(C_0, C_1, C_2, C_3, C_4, X_0, X_1, X_2, X_3, C_5, X_4, X_5, X_6, X_7, X_8, C_6),$$

where C_i $(0 \leq i \leq 6)$ are fixed constants, and X_i $(0 \leq i \leq 8)$ take all the m-bit values. Thus, each structure contains 2^{9m} plaintexts, which can provide about $\left(\frac{2^m-1}{2^m}\right)^9 \times 2^{18m}$ plaintext pairs with the following difference form:

$$(0, 0, 0, 0, 0, *, *, *, *, 0, *, *, *, *, *, *, 0)$$

where "$*$" represents non-zero difference.

2. Obtain the corresponding ciphertext of each plaintext. Choose only the pairs by birthday paradox such that

$$\Delta x_{10} = [0, 0, 0, 0, 0, *, *, 0, *, 0, 0, *, 0, *, *, 0].$$

Thus, there are $\left(\frac{2^m-1}{2^m}\right)^{15} \times 2^{n+8m}$ left.

3. For each of the remaining pairs do:

   3.1. For the $2^m - 1$ differences in Γ_0 do:

      3.1.1 Guess the value of $x_2[0, 11, 13]$, obtain the difference $\Delta x_1[5..8, 9..14]$. With the input and output differences of S-boxes in the 1-th round, deduce the value of $kw_0[5..8, 10..14]$.

      3.1.2 With values of $x_2[0, 11, 13]$ and $kw_0[5..8, 10..14]$, deduce the value of $uk_0[0, 11, 13]$. Store the value of $kw_0[5..8, 10..14]||uk_0[0, 11, 13]$ in a hash table T_0.

   3.2. For the $2^2 - 1$ differences in Γ_1 do:

      3.2.1 Guess the value of $w_8[0, 13]$, obtain the difference $\Delta y_9[5, 6, 8, 11, 13, 14]$. With input and output differences of S-boxes in the 10-th round, deduce the value of $kw_1[5, 6, 8, 11, 13, 14]$.

      3.2.2 With values of $kw_1[5, 6, 8, 11, 13, 14]$ and $w_8[0, 13]$, deduce the value of $uk_0[0, 11]$. Store the value of $kw_1[5, 6, 8, 11, 13, 14]||uk_0[0, 11]$ in a hash table T_1.

4. Check keys in T_0 and T_1 by table look-up. If the value of $kw_0[5..8, 10..14]||uk_0[0, 11, 13]$ in T_0 and the value of $kw_1[5, 6, 8, 11, 13, 14]||uk_0[0, 11]$ in T_1 match on the value of $uk_0[0, 11]$, then discard the value of $kw_0[5..8, 10..14]||uk_0[0, 11, 13]||kw_1[5, 6, 8, 11, 13, 14]$ from the candidate key. Recover the right key by exhaustively searching the remaining keys.

3.3. Complexities of the 10-Round Attack

Let Δ_{in} be the set of all possible input differences, and Δ_{out} be the set of all possible output differences. It can be seen that $|\Delta_{in}| = (2^m - 1)^9$ and $|\Delta_{out}| = (2^m - 1)^6$. Let P_{in} and P_{out} denote the probability of the truncated differentials $\Delta_{in} \longrightarrow \Gamma_0$ and $\Delta_{out} \longrightarrow \Gamma_1$, respectively. Then we have

$$P_{in} = \frac{|\Gamma_0|}{|\Delta_{in}|}, P_{out} = \frac{|\Gamma_1|}{|\Delta_{out}|}.$$

According to [19], the probability that a trivial key is kept in the remaining key candidate is

$$P = (1 - P_{in} \times P_{out})^{N_d},$$

where N_d is the number of remaining pairs left in Step 2, namely $N_d = \left(\frac{2^m-1}{2^m}\right)^{15} \times 2^{n+8m}$. Thus, there are $P \times 2^{32m}$ keys required to exhaustively search in Step 4. The time complexity of Step 3 is about

$$2 \times \left(\frac{2^m-1}{2^m}\right)^{15} \times 2^{n+8m} \times \left(\frac{2^m-1}{2^m} \times 2^{3m} + 3 \times 2^{2m}\right) \approx (2^m-1)^{16} \times 2^{n-5m+1}$$

2-round encryptions. The time complexity of Step 1 and 2 is 2^{n+9m} 10-round encryptions and 2^{n+9m} memory access, respectively. Thus, the total time complexity of this attack is about

$$T_{comp} = \frac{1}{5} \times (2^m-1)^{16} \times 2^{n-5m+1} + 2 \times 2^{n+9m} + P \times 2^{32m} \quad (1)$$

10-round encryptions.

To achieve a trade-off between the data and time complexities, we choose $n = 25$ for QARMA-64. Thus, 2^{61} chosen plaintexts are required in this attack, which implies $N_d \approx 2^{55.6}$. Since $P_{in} = 15^{-8}$ and $P_{out} = 3 \cdot 15^{-6}$ for QARMA-64, we can compute that $P \approx e^{-2^{2.6}} \approx 2^{-8.7}$, where e is the Euler's constant. According to (1), the total time complexity of the 10-round attack on QARMA-64 is about $2^{119.3}$ 10-round encryptions. The memory complexity is dominated by $T_0 \times T_1$, which requires 2^{72} 72-bit space.

For QARMA-128, we choose $n = 50$. Thus, the data complexity is 2^{122} chosen plaintexts and $N_d \approx 2^{114}$. As $P_{in} = 255^{-8}$ and $P_{out} = 3 \cdot 255^{-6}$ for QARMA-128, we have $P \approx e^{-2^{3.7}} \approx 2^{-18.7}$. According to 1, the total time complexity of the 10-round attack on QARMA-128 is about $2^{237.3}$. The memory complexity is also dominated by $T_0 \times T_1$, which requires 2^{144} 144-bit space.

4. 11-Round Impossible Differential Attack on QARMA

By appending one round on the bottom of the 10-round attack, we get the 11-round attack on QARMA (shown in Figure 4).

It can be seen that $kw_0[5..8, 10..14], uk_0[0, 5, 6, 8, 11, 13, 14], kw_0[0, 2..10, 12..15]$ are keys involved in the 11-round attack, which contain $30m$ bits. Since the key schedule of QARMA is linear, we have the following observation by analyzing the key schedule.

Observation 1. There are m-bit linear independent relations between the above keys for QARMA.

Observation 1 implies that the above keys of QARMA-64 and QARMA-128 will assume 2^{116} and 2^{232} values, respectively. Based on this observation, the memory complexity of the 11-round attack can be reduce by a factor of 2^4 for QARMA-64, and 2^8 for QARMA-128.

4.1. Details of the 11-Round Attack

1. The similar with the 10-round attack, take 2^n structures of plaintext with the form

   $$P(C_0, C_1, C_2, C_3, C_4, X_0, X_1, X_2, X_3, C_5, X_4, X_5, X_6, X_7, X_8, C_6),$$

   which will provide $\left(\frac{2^m-1}{2^m}\right)^9 \times 2^{n+18m}$ plaintext pairs with the difference form

   $$(0, 0, 0, 0, 0, *, *, *, *, 0, *, *, *, *, *, *, 0).$$

2. Obtain the corresponding ciphertext of each plaintext. Choose only the pairs by birthday paradox such that

   $$\Delta x_{10} = [*, 0, *, *, ?, ?, *, *, *, *, *, 0, *, *, ?, ?],$$

   where "?" represents the difference that can be zero or non-zero. Thus, there are $\left(\frac{2^m-1}{2^m}\right)^{19} \times 2^{n+16m}$ left.

3. For each of the remaining pairs do:

   3.1. For the $2^m - 1$ differences in Γ_0 do:

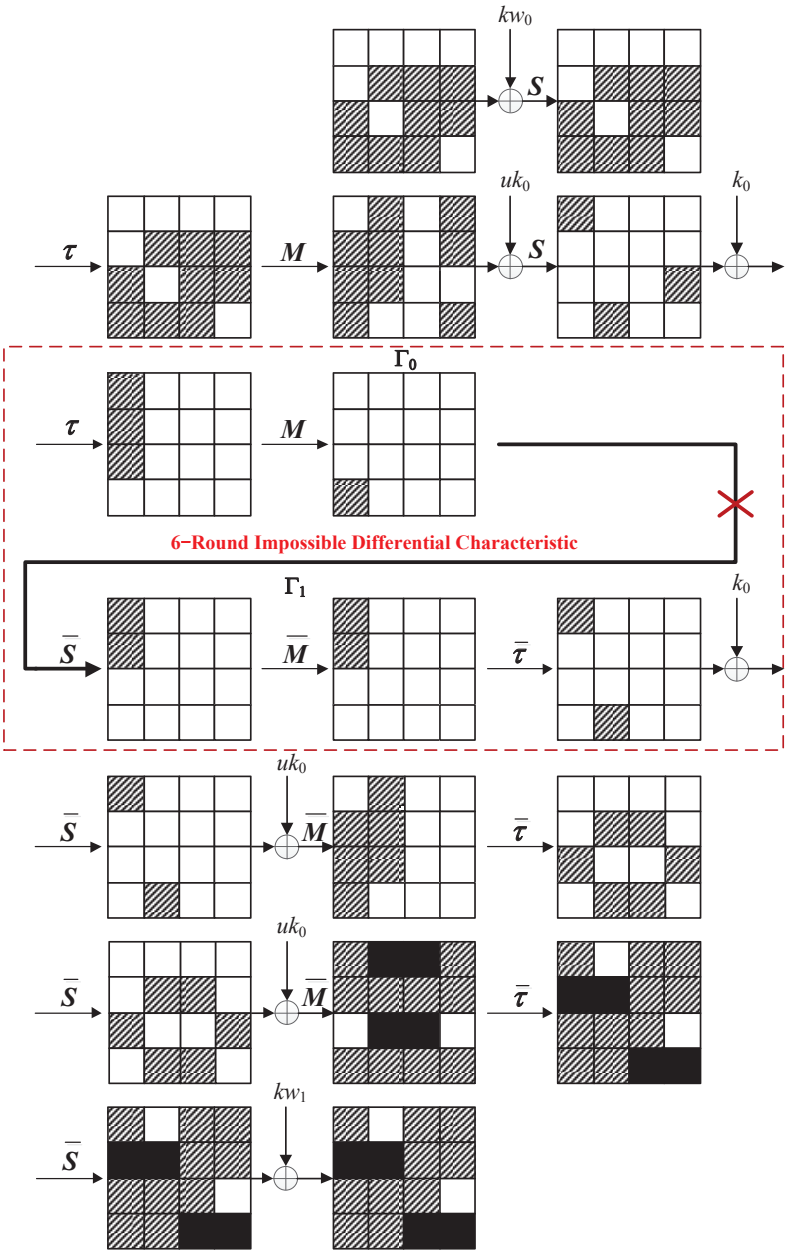


Figure 4: 11-round impossible differential attack on QARMA.

3.1.1 Guess the value of $x_2[0, 11, 13]$, obtain the difference $\Delta x_1[5..8, 9..14]$. With the input and output differences of S-boxes in the 1-th round, deduce the value of $kw_0[5..8, 10..14]$.

3.1.2 With values of $x_2[0, 11, 13]$ and $kw_0[5..8, 10..14]$, deduce the value of $uk_0[0, 11, 13]$. Store the value of $kw_0[5..8, 10..14]||uk_0[0, 11, 13]$ in a hash table T_0.

3.2. For the $2^2 - 1$ differences in Γ_1 do:

3.2.1 Guess the value of $w_8[0, 13]$ and $w_9[5, 6, 8, 11, 13, 14]$, obtain the difference $\Delta y_{10}[0, 2..10, 12..15]$. With the input and output differences of S-boxes of the 11-th round, deduce the key $kw_1[0, 2..10, 12..15]$.

3.2.2 With values of $kw_1[0, 2..10, 12..15]$, $w_8[0, 13]$ and $w_9[5, 6, 8, 11, 13, 14]$, we can further deduce the key $uk_0[0, 4, 5, 8, 11, 13, 14]$. Store the value of $kw_1[0, 2..10, 12..15]||uk_0[0, 4, 5, 8, 11, 13, 14]$ in a hash table T_1.

4. Check keys in T_0 and T_1 by table look-up. If the value of $kw_0[5..8, 10..14]||uk_0[0, 11, 13]$ in T_0 and the value of $kw_1[5, 6, 8, 11, 13, 14]||uk_0[0, 11]$ in T_1 match on the value of $uk_0[0, 11]$ and the m-bit relation between them, then discard the value of $kw_0[5..8, 10..14]||uk_0[0, 11, 13]||kw_1[5, 6, 8, 11, 13, 14]$ from the candidate key. Recover the right key by exhaustively searching the remaining keys.

4.2. Complexities of the 11-Round Attack

For QARMA-64, we have $|\Delta_{in}| = 15^9$ and $|\Delta_{out}| = 15^{10} \cdot 2^{16}$, which implies that $P_{in} = 15^{-8}$ and $P_{out} = 3 \cdot 15^{-10} \cdot 2^{-16}$. We choose $n = 25$, and thus 2^{61} chosen plaintexts are required in this attack. Then, we can compute that $N_d = \left(\frac{2^m-1}{2^m}\right)^{19} \times 2^{n+16m} \approx 2^{87.2}$ and $P \approx e^{-2^{2.5}} \approx 2^{-8.2}$. Thus, there are $P \cdot 2^{128} = 2^{119.8}$ remaining keys required to search in Step 4. The time complexity of Step 3 is about $2 \times 2^{87.2} \times (2 \times 15 \times 2^{12} + 3 \times 2^{32})/11 \approx 2^{119.9}$ 11-round encryptions. For Step 1 and 2, 2^{61} 11-round encryptions and 2^{61} memory access are required, respectively. Thus, the total time complexity of this attack is $2^{119.8} + 2^{119.9} + 2 \cdot 2^{61} \approx 2^{120.9}$ 11-round encryptions. The memory complexity of this attack is dominated by storing the values of $kw_0[5..8, 10..14]||uk_0[0, 4, 5, 8, 11, 13, 14]||kw_1[0, 2..10, 12..15]$, which is 2^{116} 120-bit space by observation 1.

For QARMA-128, we have $|\Delta_{in}| = 255^9$ and $|\Delta_{out}| = 255^{10} \cdot 2^{32}$, which implies that $P_{in} = 255^{-8}$ and $P_{out} = 3 \cdot 255^{-10} \cdot 2^{-32}$. We choose $n = 50$, and thus 2^{122} chosen plaintexts are required. It can compute that $N_d \approx 2^{178}$ and $P \approx e^{-2^{3.7}} \approx 2^{-18.7}$. Thus, the time complexity of Step 4 is about $P \cdot 2^{256} = 2^{237.3}$ 11-round encryptions. The time complexity of Step 1, 2 and 3 can be computed like that of QARMA-64, which is about $2 \times 2^{178} \times (2 \times 255 \times 2^{24} + 3 \times 3 \times 2^{64})/11 + 2 \times 2^{122} \approx 2^{242.7}$ 11-round encryptions. Thus, the total time complexity of this attack is about $2^{237.3} + 2^{242.7} \approx 2^{242.8}$ 11-round encryptions. The memory complexity of this attack is also dominated by storing the values of $kw_0[5..8, 10..14]||uk_0[0, 4, 5, 8, 11, 13, 14]||kw_1[0, 2..10, 12..15]$, which is 2^{232} 240-bit space by observation 1.

5. Conclusion

In this paper, we present impossible differential attacks on QARMA. Based on the generalized truncated differential, a 6-round impossible differential charactersitic of QARMA is constructed. Exploiting the 6-round impossible differential characteristic and the time-memory trade-off technique, we present 10-round and 11-round impossible differential attacks on QARMA. To the best of our knowledge, this is the first 11-round attack on QARMA, which also imply that 8-round QARMA is not secure against impossible differential attack. Further analyzing QARMA with other attacks will be our future work.

References

[1] Bogdanov, A., Knudsen, L.R., Leander, *et al.*: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P. and Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466, Springer (2007).

[2] Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: Lopez, J. and Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344, Springer (2011).

[3] Beaulieu, R., Shors, D., Smith J., *et al.*: The SIMON and SPECK Families of Lightweight Block Ciphers. Available at http://eprint.iacr.org/2013/404.pdf, accessed December 2015.
[4] Banik, S., Bogdanov, A., Isobe, T., *et al.*: Midori: A Block Cipher for Low Energy. In: Iwata, T. and Cheon, J.H. (eds.): ASIACRYPT 2015, Part II, LNCS, vol. 9453, pp. 411–436, Springer (2015).
[5] Liskov, M., Rivest, R.L., Wagner, D.: Tweakable Block Cipher. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31-46, Springer (2002).
[6] Avanzi, R.: The QARMA Block Cipher Family. IACR Cryptology ePrint Archive, 2016:444.
[7] Borghoff, J., Canteaut, A., Gűeysu, T., et al.: PRINCE-A Low-Latency Block Cipher for Pervasive Computing Applications- Extended Abstract. In: Wang, X. and Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208-225, Springer (2012).
[8] https://community.arm.com/groups/processors/blog/2016/10/27/armv8-a-architecture-2016-additions.
[9] Biham, E., Shamir, A.: Differential Cryptanalysis of DES-like Cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, pp. 2-21, Springer (1991).
[10] Matsui, M.: Linear Cryptoanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol765, pp. 386-397, Springer (1993).
[11] Knudsen, L.R.: DEAL - A 128-bit Block Cipher. Tech. rep., Department of Informatics, University of Bergen, Norway, technical report (1998).
[12] Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23, Springer (1999).
[13] Bogdanov, A., Rijmen, V.: Linear Hulls with Correlation Zero and Linear Cryptanalysis of Block Ciphers. Des. Codes Cryptogr.70(3), 369-383 (2014).
[14] Sun, B., Liu, M., Guo, J., Rijmen, V., Li, R.: Provable Security Evaluation of Structures against Impossible Differential and Zero-Correlation Linear Cryptanalysis. In: Fischlin, M. and Coron, J. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 196-213, Springer (2016).
[15] Zong, R., Dong, X.Y.: Meet-in–the-Middle Attack on QARMA Block Cipher. IACR Cryptology ePrint Archive, 2016:1160.
[16] Dunkelman, O., Keller, N., Shamir, A.: Improved Single-Key Attacks on 8-Round AES-192 and AES-256. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 158-176, Springer (2010).
[17] Li, L., Jia, K., Wang, X.: Improved Single-Key Attack on 9-Round AES-192/256. In: Cid, C. and Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 127-146, Springer (2015).
[18] Derbez, P., Fouque, P.: Exhausting Demirci-Selçuk.: Meet-in-the-Middle Attacks against Reduced-Round AES. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 541–560, Springer (2013).
[19] Boura, C., Naya-Plasencia M., Suder, V.: Scrutinizing and Improving Impossible Differential Attacks: Applications to CLEFIA, Camellia, LBlock and SIMON. In: Palash Sarkar, P. and Iwata, T. (eds.) AISACRYPT 2014. LNCS, vol. 8873, pp. 179-199, Springer (2014).