SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Related-Tweakey Impossible Differential Attack on QARMA-128

Juan Du, Wei Wang*, Muzhou Li & Meiqin Wang

Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan 250100*, China*

Appendix A Differential Properties of Matrix M

For QARMA-128, denote the column-wise input difference of matrix M as $\Delta In = (\Delta In[0], \Delta In[1], \Delta In[2], \Delta In[3])$, and the output difference as $\Delta Out = (\Delta Out[0], \Delta Out[1], \Delta Out[2], \Delta Out[3])$.

Proposition 1. If the input difference satisfies the conditions: 1) $\Delta In[0] = 0$; 2) $\Delta In[1] = \rho\Delta In[2]$; 3) $\Delta In[1] = \rho^4\Delta In[3]$, the output difference can be represented as $(\rho^3\Delta In[1], 0, 0, 0)$. I.e., if $\Delta In = (0, \alpha, \alpha \ggg 1, \alpha \ggg 4)$, then the output difference $\Delta Out = (\alpha \lll 3, 0, 0, 0)$, where α is an arbitrary 8-bit value.

Proof. Because $\Delta Out = M_{128} \cdot \Delta In$,

$$\begin{pmatrix} \Delta Out[0] \\ \Delta Out[1] \\ \Delta Out[2] \\ \Delta Out[3] \end{pmatrix} = \begin{pmatrix} 0 & \rho^1 & \rho^4 & \rho^5 \\ \rho^5 & 0 & \rho^1 & \rho^4 \\ \rho^4 & \rho^5 & 0 & \rho^1 \\ \rho^1 & \rho^4 & \rho^5 & 0 \end{pmatrix} \begin{pmatrix} \Delta In[0] \\ \Delta In[1] \\ \Delta In[2] \\ \Delta In[3] \end{pmatrix} = \begin{pmatrix} \rho\Delta In[1] + \rho^4\Delta In[2] + \rho^5\Delta In[3] \\ \rho^5\Delta In[0] + \rho\Delta In[2] + \rho^4\Delta In[3] \\ \rho^4\Delta In[0] + \rho^5\Delta In[1] + \rho\Delta In[3] \\ \rho\Delta In[0] + \rho^4\Delta In[1] + \rho^5\Delta In[2] \end{pmatrix}.$$

Since $\Delta In[0] = 0$,$\Delta In[1] = \rho\Delta In[2]$, $\Delta In[1] = \rho^4\Delta In[3]$, the above equations lead to the following results directly.

$$\begin{cases} \Delta Out[0] = \rho^3\Delta In[1] \\ \Delta Out[1], \Delta Out[2], \Delta Out[3] = 0. \end{cases}$$

In a similar way, we can obtain the following properties.

Proposition 2. For any arbitrary 8-bit value α, if $\Delta In = (\alpha \ggg 4, 0, \alpha, \alpha \ggg 1)$, then the output difference $\Delta Out = (0, \alpha \lll 3, 0, 0)$.

Proposition 3. For any arbitrary 8-bit value α, if $\Delta In = (\alpha \ggg 1, \alpha \ggg 4, 0, \alpha)$, then the output difference $\Delta Out = (0, 0, \alpha \lll 3, 0)$.

Proposition 4. For any arbitrary 8-bit value α, if $\Delta In = (\alpha, \alpha \ggg 1, \alpha \ggg 4, 0)$, then the output difference $\Delta Out = (0, 0, 0, \alpha \lll 3)$.

Appendix B Distinguisher Family No.2

As depicted in Fig. B1, the related-tweakey impossible differential characteristic

$$(\varepsilon_1(\alpha \ggg 1)(\beta \ggg 1)(\gamma \ggg 1),\ 0\varepsilon_2 00,\ \beta(\gamma \ggg 4)\varepsilon_3\alpha,\ \gamma(\beta \ggg 4)(\alpha \ggg 4)\varepsilon_4) \nrightarrow (0000, 0000, \delta000, 0000)$$

exists, if the following conditions are satisfied:

1) $\Delta T_7[10]$ is the only active cell of ΔT_7,
2) $\Delta W_{13}[8]$ is the only active cell of ΔW_{13}, and the equation $\Delta W_{13}[8] = \Delta T_{12}[8] = \delta$ is satisfied,

where δ is an arbitrary non-zero value, α, β, γ and ε_i(for $1 \leqslant i \leqslant 4$) could be zero or non-zero freely.

Two special cases are explained below, which are adopted in key recovery attack for QARMA-128.

Case 1. For QARMA-128, if the conditions (1,2) are satisfied, the related-tweakey impossible differential characteristic

$$(\alpha000, 0\beta00, 00\gamma0, 000\sigma) \nrightarrow (0000, 0000, \delta000, 0000)$$

* Corresponding author (email: weiwangsdu@sdu.edu.cn)

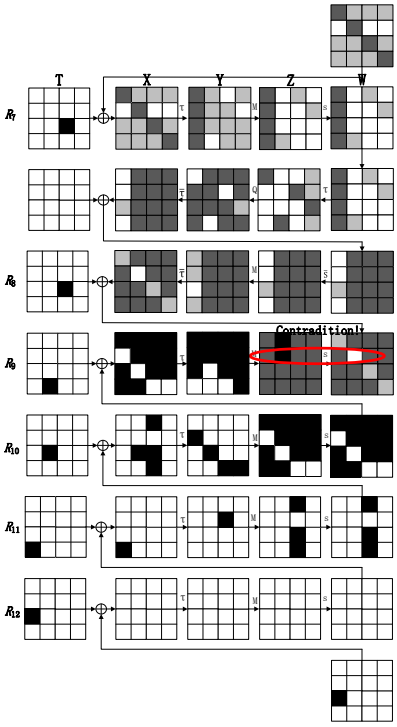

Figure B1 Distinguisher Family No.2. Black cells are active while the white ones are inactive, dark and light gray cells could be active or inactive.

exists, where α, β, γ, σ and δ are non-zero values.

Case 2. For QARMA-128, if the conditions (1,2) are satisfied, the related-tweakey impossible differential characteristic

$$(\varepsilon_1(\alpha \ggg 1)(\beta \ggg 1)(\gamma \ggg 1),\ 0\varepsilon_2 00,\ \beta(\gamma \ggg 4)\varepsilon_3\alpha,\ \gamma(\beta \ggg 4)(\alpha \ggg 4)\varepsilon_4) \nrightarrow (0000, 0000, \delta 000, 0000)$$

exists, where α, β, γ, δ and ε_i(for $1 \leqslant i \leqslant 4$) are non-zero values.

Appendix C Attack on 10-Round QARMA-128

In this section, we proceed an attack on QARMA-128 taking the outer whitening keys into consideration. Based on two parallel 6-round distinguishers which are proposed in Section Appendix B, we can mount the key recovery attack on 10-round QARMA-128 by adding one round before the distinguisher and three rounds after it. Note that this variant is not symmetric since there are two rounds before *Pseudo-Reflector* and eight rounds after.

For convenience, we guess equivalent keys in our 10-round key recovery attacks. Let $ek_0 = M(\tau(k_0))$, $sk_0 = k_0 \oplus w_0$ and $sk_1 = k_0 \oplus w_1$, then ek_0, sk_0 and sk_1 will be used instead of k_0, w_0.

Attack Based on Distinguisher Family No.1 (Case 1)

As shown in Figure C1, we derive a related-tweakey impossible differential attack based on Distinguisher Family No.1 (Case 1) of QARMA-128. The attack is illustrated in the following part.

Offline Phase.

1. Choose two tweaks(T, T') that satisfy $T_6 \oplus T'_6 = (000*, 0000, 0000, 0000)$, where $*$ is an arbitrary non-zero difference.
2. Under the chosen (T, T'), construct 2^n structures. Inside each structure, the plaintext pairs satisfy the condition

$$P \oplus P' = (00 * \Delta T_6[3], 000*, *000, 0 * 00),$$

where $*$ traverses all possible non-zero values. Since each structure contains $2^{32} \times (2^{32} - 1)$ pairs, we get 2^{n+64} pairs in total. In order to match the end of distinguisher, only the pairs that satisfy the conditions $\Delta C[0, 1, 3, 9, 12] = 0$ and $\Delta C[2] = \Delta T_{15}[2]$ are saved, and there are about $2^{n+64} \times 2^{-8\times 6} = 2^{n+16}$ pairs left.

Online Phase.

1. Starting at the ciphertext pairs, i.e., *Round 15*, we proceed the following steps.

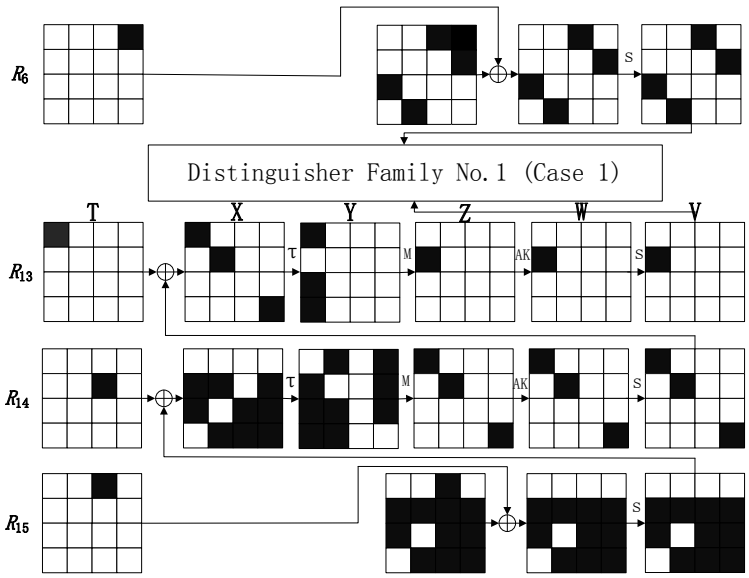

Figure C1 Key Recovery Attacks on 10-Round QARMA-128 with Distinguisher Family No.1 (Case 1). Cells with color are active while the others are inactive.

(a) Guess $sk_1[6]$, decrypt and get $V_{15}[6]$, $V'_{15}[6]$. In order to guarantee $\Delta X_{14}[6] = 0$, pairs that satisfy the condition $\Delta T_{14}[6] = \Delta V_{15}[6]$ remain, and $2^{n+16} \times 2^{-8} = 2^{n+8}$ pairs are left.

(b) Guess $sk_1[5, 10]$, decrypt and get $Y_{14}[4, 8]$, $Y'_{14}[4, 8]$. According to Property 1 in Section Appendix A, there must be $\rho\Delta Y_{14}[8] = \Delta Y_{14}[4]$ to make sure that $\Delta Z_{14}[0]$ is the only active cell in the first column of ΔZ_{14}, so that $2^{n+8} \times 2^{-8} = 2^n$ pairs are left.

(c) Guess $sk_1[15]$, decrypt and get $Y_{14}[12]$, $Y'_{14}[12]$. As step (1b), there should be $\Delta Y_{14}[4] = \rho^4\Delta Y_{14}[12]$, and $2^n \times 2^{-8} = 2^{n-8}$ pairs are left.

(d) Similarly, guess $sk_1[4, 11]$, decrypt and get $Y_{14}[1, 13]$, $Y'_{14}[1, 13]$. Detect pairs that satisfy the condition $\Delta Y_{14}[13] = \rho^3\Delta Y_{14}[1]$, and $2^{n-8} \times 2^{-8} = 2^{n-16}$ pairs are left.

(e) Guess $sk_1[14]$, decrypt and get $Y_{14}[9]$, $Y'_{14}[9]$. Pairs that satisfy $\rho^4\Delta Y_{14}[1] = \Delta Y_{14}[9]$ are saved, and $2^{n-16} \times 2^{-8} = 2^{n-24}$ pairs are left.

(f) Guess $sk_1[7, 8]$, decrypt and get $Y_{14}[7, 11]$, $Y'_{14}[7, 11]$. Keep pairs that satisfy $\Delta Y_{14}[7] = \rho^3\Delta Y_{14}[11]$, and $2^{n-24} \times 2^{-8} = 2^{n-32}$ pairs are left.

(g) Guess $sk_1[13]$, decrypt and get $Y_{14}[3]$, $Y'_{14}[3]$. Save pairs that satisfy the condition $\rho^4\Delta Y_{14}[11] = \Delta Y_{14}[3]$, and $2^{n-32} \times 2^{-8} = 2^{n-40}$ pairs are left.

2. After step 1, the value of $Y_{14}[1, 3, 4, 7, 8, 9, 11, 12, 13]$ and $Y'_{14}[1, 3, 4, 7, 8, 9, 11, 12, 13]$ are obtained, and the left ciphertext pairs ensure only the cells with indexes 0, 5, 15 are active in ΔZ_{14}. Moreover, according to the definition of matrix M and the relation

$$\begin{pmatrix} \Delta Z_{14}[0] \\ \Delta Z_{14}[4] \\ \Delta Z_{14}[8] \\ \Delta Z_{14}[12] \end{pmatrix} = \begin{pmatrix} 0 & \rho^1 & \rho^4 & \rho^5 \\ \rho^5 & 0 & \rho^1 & \rho^4 \\ \rho^4 & \rho^5 & 0 & \rho^1 \\ \rho^1 & \rho^4 & \rho^5 & 0 \end{pmatrix} \begin{pmatrix} \Delta Y_{14}[0] \\ \Delta Y_{14}[4] \\ \Delta Y_{14}[8] \\ \Delta Y_{14}[12] \end{pmatrix},$$

the value of $Z_{14}[0] = \rho Y_{14}[4] + \rho^4 Y_{14}[8] + \rho^5 Y_{14}[12]$, which is irrelevant to $Y_{14}[0]$, thus $Z_{14}[0]$, $Z'_{14}[0]$ can be computed. Similarly, the value of $Z_{14}[5, 15]$ and $Z'_{14}[5, 15]$ are deduced.

3. The value of the active cells in Z_{14} and Z'_{14} have been recovered and the following steps are performed.

(a) Guess $ek_0[0]$, decrypt and get $Y_{13}[0]$, $Y'_{13}[0]$.

(b) Guess $ek_0[5]$, decrypt and get $Y_{13}[8]$, $Y'_{13}[8]$. Choose pairs that satisfy $\rho^4\Delta Y_{13}[0] = \Delta Y_{13}[8]$, and $2^{n-40} \times 2^{-8} = 2^{n-48}$ pairs are left.

(c) Guess $ek_0[15]$, decrypt and get $Y_{13}[12]$, $Y'_{13}[12]$. Choose pairs that satisfy $\rho^3\Delta Y_{13}[0] = \Delta Y_{13}[12]$, and $2^{n-48} \times 2^{-8} = 2^{n-56}$ pairs are left.

Table C1 Time Complexity in Section Appendix C

	Step	Time Complexity(Evaluated by encryption units)
offline	2	In data preparation, we need $2^n \times (2^{32}+2^{32})$ MA, about $2^n \times (2^{32}+2^{32}) \times \frac{1}{16} \times \frac{1}{11}$ 10-round encryptions
online	1a	$2 \times 2^{n+16} \times 2^{8\times 1} \times \frac{1}{16} \times \frac{1}{11}$
	1(b-c)	$2 \times (2^{n+8} \times 2^{8\times 3} \times \frac{2}{16} + 2^n \times 2^{8\times 4} \times \frac{1}{16}) \times \frac{1}{11}$
	1(d-e)	$2 \times (2^{n-8} \times 2^{8\times 6} \times \frac{2}{16} + 2^{n-16} \times 2^{8\times 7} \times \frac{1}{16}) \times \frac{1}{11}$
	1(f-g)	$2 \times (2^{n-24} \times 2^{8\times 9} \times \frac{2}{16} + 2^{n-32} \times 2^{8\times 10} \times \frac{1}{16}) \times \frac{1}{11}$
online	3(a-c)	$2 \times (2^{n-40} \times 2^{8\times 11} + 2^{n-40} \times 2^{8\times 12} + 2^{n-48} \times 2^{8\times 13}) \times \frac{1}{16} \times \frac{1}{11}$
	SUM	$2^{120.94}$ 10-round encryptions

4. As $Y_{13}[0,8,12]$, $Y'_{13}[0,8,12]$ are known in step 3, we obtain $Z_{13}[4]$ and $Z'_{13}[4]$, which is the only active cell in ΔZ_{13} according to Property 2.

5. Guess $ek_0[4]$, decrypt and get $V_{13}[4]$, $V'_{13}[4]$. If $\Delta V_{13}[4] = \Delta T_{12}[4]$ is satisfied, we get the tail of the distinguisher. After this step, about $2^{n-56} \times 2^{-8} = 2^{n-64}$ pairs remain. Keys that suggest this distinguisher would be discarded. Repeat step 1 to step 5 until all wrong $sk_1[4,5,6,7,8,10,11,13,14,15] \,||\, ek_0[0,4,5,15]$ are discarded, and only one subkey remains, which is the right one.

Let $n = 70.40$, for 112-bit subkeys $sk_1[4,5,6,7,8,10,11,13,14,15] \,||\, ek_0[0,4,5,15]$, about $2^{112} \times (1-2^{-80})^{2^{n+16}} = 0.001$ wrong subkeys are left. The data complexity of is $2^{70.40} \times (2^{32}+2^{32}) = 2^{103.40}$ {plaintext,ciphertext,tweak} triples. We need to store pairs obtained after the offline phase, so the memory required is $2^{87.40}$ 128-bit. The time consumed for each step is illustrated in Table C1, and the total time complexity is about $2^{120.94}$ 10-round encryption units.

Attack Based on Distinguisher Family No.2 (Case 1)

Based on Distinguisher Family No.2 (Case 1) of QARMA-128, we can perform a related-tweakey impossible differential attack in a similar way as described in Section Appendix C. Since $sk_1[4,5,6,7,8,10,11,13,14,15]$ and $ek_0[0,4,5,15]$ are recovered in Section Appendix C, we only need to guess $sk_1[2,3,9,12]||ek_0[7,8,10]$ and the details of the attack are omitted. The data complexity is $2^{69.50} \times (2^{32}+2^{32}) = 2^{102.50}$ triples, while $2^{95.46}$ encryptions are required. Memory complexity is $2^{94.5}$ 128-bit.

Recovery of the Master Key

Combine 112-bit subkeys $sk_1[4,5,6,7,8,10,11,13,14,15]||ek_0[0,4,5,15]$ obtained in Section Appendix C with 56-bit subkeys $sk_1[2,3,9,12]||ek_0[7,8,10]$ obtained in Section Appendix C, we get 168 bits subkeys in total, they are $sk_1[2,3,4,5,6,7,8,9,10,11,12,13,14,15]||ek_0[0,4,5,7,8,10,15]$. Then search the master key exhaustively. The time complexity is 2^{88} 10-round encryptions, the data complexity is $o(1)$ and the memory complexity can be ignored.

Total Complexity. The data complexity of the whole attack is $2^{103.40}+2^{102.50} = 2^{104.02}$ triples while the time complexity is $2^{120.94}+2^{95.46}+2^{88} = 2^{120.94}$ 10-round encryption, and the memory complexity is $2^{87.40}+2^{94.50} = 2^{94.50}$ 128-bit.

Appendix D Attack on 11-Round QARMA-128

We tried to mount a key recovery attack on 11-round QARMA-128 including the outer whitening keys but the product of time and data is greater than 2^{256}, thus, we proceed an attack on 11-round variant without the outer whitening keys. In order to reduce the time complexity of memory access(Offline Phase), we derived our attack in a chosen ciphertext-tweak scenario. Based on Distinguisher Family No.1 (Case 2), a 11-round key recovery attack is derived.

Attack Based on Distinguisher Family No.1 (Case 2)

As shown in the Figure D1, an attack on 11-round QARMA-128 is obtained by appending two rounds on the top of Distinguishers No.1 (Case 2) and three rounds on the bottom.

Offline Phase.

1. Choose a tweak T randomly and find 2^8-1 T' to construct 2^8-1 (T,T') pairs, for each (T,T'), the internal state satisfy the condition

$$\Delta T_{15} = T_{15} \oplus T'_{15} = (00*0, 0000, 0000, 0000).$$

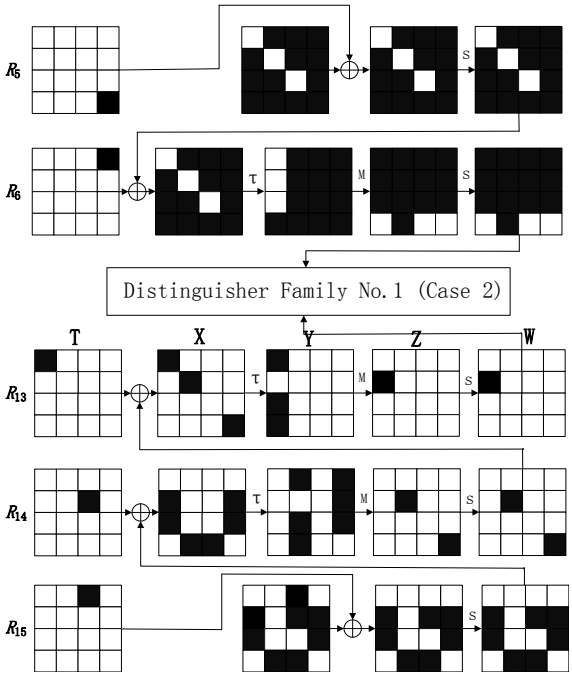

Figure D1 Key Recovery Attacks on 11-Round QARMA-128 with Distinguisher Family No.1 (Case 2). Cells with colors are active while the others are inactive.

where $*$ is an arbitrary value.

2. For each (T, T'), construct 2^n structures. Inside each structure the ciphertext pairs satisfy the condition

   1) $\Delta C = (00\Delta T_{15}[2]0, *0**, *00*, 0**0)$,

   2) $C[2] = \alpha$, then $C'[2] = C[2] \oplus \Delta T_{15}[2] = \alpha \oplus \Delta T_{15}[2]$

   where $*$ traverses all possible non-zero values, and α is a constant. Since each structure contains $2^{56} \times (2^{56} - 1)$ pairs, we obtain $2^n \times (2^8 - 1) \times 2^{56} \times (2^{56} - 1) = 2^{n+120}$ pairs in total. To construct these pairs, $((2^8 - 1) \times 2^{8\times 7} + 2^{8\times 7}) \times 2^n$ {plaintext,ciphertext,tweak} triples are required. Choose pairs that satisfy the condition $\Delta P[0, 5, 10] = 0$, there are about $2^{n+120} \times 2^{-3\times 8} = 2^{n+96}$ pairs left.

Online Phase.

1. Starting at the ciphertext pairs, the following steps are performed.

   (a) Guess $k_0[7]$, decrypt and get $Y_{14}[7]$, $Y'_{14}[7]$.

   (b) Guess $k_0[8]$, decrypt and get $Y_{14}[11]$, $Y'_{14}[11]$. Save pairs that satisfy the condition $\Delta Y_{14}[7] = \rho^3 \Delta Y_{14}[11]$, and $2^{n+96} \times 2^{-8} = 2^{n+88}$ pairs are left.

   (c) Guess $k_0[13]$, decrypt and get $Y_{14}[3]$, $Y'_{14}[3]$. Save pairs that satisfy the condition $\Delta Y_{14}[3] = \rho^4 \Delta Y_{14}[11]$, and $2^{n+88} \times 2^{-8} = 2^{n+80}$ pairs are left.

   (d) Since the value of $Y_{13}[3, 7, 11]$ and $Y'_{13}[3, 7, 11]$ are achieved in step(1a-1c), we get $Z_{14}[15]$, $Z'_{14}[15]$, which is the only active cell in $\Delta Z_{14}[3, 7, 11, 15]$ according to Property 4. Then we get the value of $W_{14}[15]$ and $W'_{14}[15]$, save pairs that satisfy the condition $\Delta W_{14}[15] = \rho^3 \Delta T_{13}[0]$, about $2^{n+80} \times 2^{-8} = 2^{n+72}$ pairs are left after this step.

2. $k_0[7, 8, 13]$ have been guessed in step1, encrypt *round 5* partially and get $Y_6[3, 7, 11]$, $Y'_6[3, 7, 11]$, pairs that satisfy the condition $\rho\Delta Y_6[3] + \rho^4 \Delta Y_6[7] + \rho^5 \Delta Y_6[11] = 0$ remain, about $2^{n+72} \times 2^{-8} = 2^{n+64}$ pairs are left.

3. Starting at the ciphertext pairs, we proceed the following steps.

   (a) Guess $k_0[4]$, decrypt and get $Y_{14}[13]$, $Y'_{14}[13]$.

   (b) Guess $k_0[11]$, decrypt and get $Y_{14}[1]$, $Y'_{14}[1]$. Save pairs that satisfy the condition $\Delta Y_{14}[13] = \rho^3 \Delta Y_{14}[1]$, and $2^{n+64} \times 2^{-8} = 2^{n+56}$ pairs are left.

   (c) Guess $k_0[14]$, decrypt and get $Y_{14}[9]$, $Y'_{14}[9]$. Save pairs that satisfy the condition $\rho^4 \Delta Y_{14}[1] = \Delta Y_{14}[9]$, and $2^{n+56} \times 2^{-8} = 2^{n+48}$ pairs are left.

(d) As the value of $Y_{14}[1,9,13]$ and $Y'_{14}[1,9,13]$ are achieved in step(3a-3c), we get $Z_{14}[5]$ and $Z'_{14}[5]$, which is the only active cell in $\Delta Z_{14}[1,5,9,13]$ by Property 2. Then $W_{14}[5]$ and $W'_{14}[5]$ can be inferred. Choose pairs that satisfy the condition $\Delta W_{14}[5] = \rho^4 \Delta T_{13}[0]$, which is about $2^{n+48} \times 2^{-8} = 2^{n+40}$ pairs are left after this step.

4. Guess $k_0[6]$, decrypt and get $W_{15}[6]$, $W'_{15}[6]$. Pairs that satisfy the condition $\Delta W_{15}[6] = \Delta T_{14}[6]$ are saved, there are about $2^{n+40} \times 2^{-8} = 2^{n+32}$ pairs left.

5. Starting at the plaintext pairs, i.e., the *Round 5*, we proceed the following steps.
   (a) $k_0[4,11,14]$ have been guessed in step 3, encrypt and get $Y_6[1,9,13]$, $Y'_6[1,9,13]$, then $W_6[5]$ and $W'_6[5]$ can be deduced.
   (b) Guess $k_0[1]$, encrypt and get $Y_6[5]$, $Y'_6[5]$, so $Y_6[1,5,9,13]$ and $Y'_6[1,5,9,13]$ are achieved, encrypt and get $W_6[1,9]$, $W'_6[1,9]$.
   (c) Guess $k_0[2]$, encrypt and get $Y_6[15]$, $Y'_6[15]$.
   (d) As $Y_6[3,7,11,15]$ and $Y'_6[3,7,11,15]$ are achieved in step(2,5c), encrypt and get $W_6[3,11]$, $W'_6[3,11]$. Pairs that satisfy the conditions $\rho^3 \Delta W_6[1] = \Delta W_6[11]$ and $\Delta W_6[3] = \rho \Delta W_6[9]$ remain, there are about $2^{n+32} \times 2^{-8\times 2} = 2^{n+16}$ pairs are left.

6. As step 5, starting at the *Round 5*, the following steps are performed.
   (a) $k_0[6]$ has been guessed, encrypt and get $Y_6[2]$, $Y'_6[2]$.
   (b) Guess $k_0[3]$, encrypt and get $Y_6[10]$, $Y'_6[10]$.
   (c) Guess $k_0[12]$, encrypt and get $Y_6[6]$, $Y'_6[6]$. Since $Y_6[2,10]$ and $Y'_6[2,10]$ are obtained in step(6a,6b), pairs that satisfy $\rho \Delta Y_6[2] + \rho^4 \Delta Y_6[6] + \rho^5 \Delta Y_6[10] = 0$ remain, there are about $2^{n+16} * 2^{-8} = 2^{n+8}$ pairs left.
   (d) Guess $k_0[9]$, encrypt and get $Y_6[14]$, $Y'_6[14]$. Since $Y_6[2,6,10]$ and $Y'_6[2,6,10]$ are obtained in step(6a-6c), we get the value of $W_6[6]$ and $W'_6[6]$. Pairs that satisfy the condition $\Delta W_6[3] = \rho^4 \Delta W_6[6]$ remain, about $2^{n+8} \times 2^{-8} = 2^n$ pairs are left.
   (e) Since $Y_6[2,6,10,14]$ and $Y'_6[2,6,10,14]$ are obtained, we get the value of $W_6[10]$ and $W'_6[10]$. Pairs that satisfy the condition $\rho^3 \Delta W_6[5] = \Delta W_6[10]$ are saved, about $2^n \times 2^{-8} = 2^{n-8}$ pairs are left.

7. As step 5, starting at the *Round 5*, the following steps are performed.
   (a) Guess $k_0[5]$, encrypt and get$Y_6[8]$, $Y'_6[8]$.
   (b) Guess $k_0[10]$, encrypt and get $Y_6[4]$, $Y'_6[4]$.
   (c) Guess $k_0[15]$, encrypt and get $Y_6[12]$, $Y'_6[12]$, then we get $W_6[0]$, $W'_6[0]$. Pairs that satisfy the condition $\Delta W_6[0] = \rho^4 \Delta W_6[5]$ remain, there are about $2^{n-8} \times 2^{-8} = 2^{n-16}$ pairs left.
   (d) Guess $k_0[0]$, encrypt and get $Y_6[0]$, $Y'_6[0]$. Pairs that satisfy the condition $\rho^4 \Delta W_6[1] = \Delta W_6[4]$ remain, there are about $2^{n-16} \times 2^{-8} = 2^{n-24}$ pairs left.

8. $k_0[0,5,15]$ have been guessed, the value of $W_{14}[5,15]$ and $W'_{14}[5,15]$ are obtained in step(3d,1d). Decrypt *round 13* partially and get $Y_{13}[0,8,12]$, $Y'_{13}[0,8,12]$, then $Z_{13}[4]$ and $Z'_{13}[4]$ can be inferred and $\Delta Z_{13}[4]$ is the only active cell in ΔZ_{13} according to Property 2, we get $W_{13}[4]$, $W'_{13}[4]$ after *SubCells* operation. Choose pairs that satisfy the condition $\Delta W_{13}[4] = \Delta T_{12}[4]$, there are about $2^{n-24} \times 2^{-8} = 2^{n-32}$ pairs are left. We obtain the tail of Distinguisher Family No.1 (Case 2). Since $\Delta W_6[12,14,15]$ are inactive, combined with the equations

$$\begin{cases} \rho^4 \Delta W_6[1] = \Delta W_6[4](\text{step } 7d), & \rho^3 \Delta W_6[1] = \Delta W_6[11](\text{step } 5d), \\ \Delta W_6[3] = \rho^4 \Delta W_6[6](\text{step } 6d), & \Delta W_6[3] = \rho \Delta W_6[9](\text{step } 5d), \\ \Delta W_6[0] = \rho^4 \Delta W_6[5](\text{step } 7c), & \rho^3 \Delta W_6[5] = \Delta W_6[10](\text{step } 6e), \end{cases}$$

we obtain the header of Distinguisher Family No.1 (Case 2). Keys that suggest this distinguisher will be discarded. Repeat step 1 to step 8 until all wrong k_0 are discarded.

Let $n = 38.54$, for the 128-bit k_0, about $2^{128} \times (1 - 2^{-128})^{2^{n+96}} = 0.013$ wrong subkeys are left. The data complexity is $2^{38.54} \times (2^{64} + 2^{56}) = 2^{102.54}$ {plaintext,ciphertext,tweak} triples, and the memory complexity is 2^{n+97} 128-bit. Time consumed for each step is illustrated in D1, the total time complexity of this part is $2^{145.98}$ 11-round encryptions.

Recovery of Master Key

We obtain the 128-bit k_0 after discarding the wrong subkeys in Section Appendix D. Then we search the the 128-bit w_0 exhaustively, 2^{128} 11-round encryptions are needed while the data complexity is o(1).

Total Complexity. The attack requires $2^{102.54}$ {plaintext, ciphertext, tweak} triples and $2^{145.98} + 2^{128} = 2^{145.98}$ 11-round encryptions. The memory complexity is $2^{135.54}$ 128-bit.

Table D1 Time Complexity in Section Appendix D

	Step	Time Complexity(Evaluated by encryption units)
offline	2	In data preparation, we need $2^n \times (2^{64} + 2^{56})$ MA, about $2^n \times (2^{64} + 2^{56}) \times \frac{1}{16} \times \frac{1}{12}$ 11-round encryptions
online	1(a-c)	$2 \times (2^{n+96} \times 2^{8\times1} + 2^{n+96} \times 2^{8\times2} + 2^{n+88} \times 2^{8\times3}) \times \frac{1}{16} \times \frac{1}{12}$
	1d,2	$2 \times 2^{n+80} \times 2^{8\times3} \times \frac{1}{16} \times \frac{1}{12} + 2 \times 2^{n+72} \times 2^{8\times3} \times \frac{3}{16} \times \frac{1}{12}$
	3(a-c)	$2 \times (2^{n+64} \times 2^{8\times4} + 2^{n+64} \times 2^{8\times5} + 2^{n+56} \times 2^{8\times6}) \times \frac{1}{16} \times \frac{1}{12}$
	3d,4	$2 \times 2^{n+48} \times 2^{8\times6} \times \frac{1}{16} \times \frac{1}{12} + 2 \times 2^{n+40} \times 2^{8\times7} \times \frac{1}{16} \times \frac{1}{12}$
online	5a	$2 \times 2^{n+32} \times 2^{8\times7} \times \frac{3}{16} \times \frac{2}{12}$
	5(b-e)	$2 \times (2^{n+32} \times 2^{8\times8} \times 4 + 2^{n+32} \times 2^{8\times9} + 2^{n+32} \times 2^{8\times9} \times 2) \times \frac{1}{16} \times \frac{1}{12}$
online	6(a-d)	$2 \times (2^{n+16} \times 2^{8\times9} + 2^{n+16} \times 2^{8\times10} + 2^{n+16} \times 2^{8\times11} + 2^{n+8} \times 2^{8\times12}) \times \frac{1}{16} \times \frac{1}{12}$
	6e	$2 \times 2^n \times 2^{8\times12} \times \frac{1}{16} \times \frac{1}{12}$
online	7(a-c)	$2 \times (2^{n-8} \times 2^{8\times13} + 2^{n-8} \times 2^{8\times14} + 2^{n-8} \times 2^{8\times15}) \times \frac{1}{16} \times \frac{1}{12}$
	7d,8	$2 \times 2^{n-16} \times 2^{8\times16} \times \frac{1}{16} \times \frac{2}{12} + 2 \times 2^{n-24} \times 2^{8\times16} \times \frac{3}{16} \times \frac{1}{12}$
	SUM	$\frac{1}{3} \times (2^{n+107} \times 4 + 2^{n+99} \times 13) = 2^{145.98}$ 11-round encryptions

References

1 R. Zong, X. Dong, X. Wang. MILP-Aided Related-Tweak/Key Impossible Differential Attack and Its applications to QARMA, Joltik-BC. IACR Cryptology ePrint Archive, 2018, 2018: 142.

2 R. Avanzi. 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, 2017: 4-44.