SCIENCE CHINA
Information Sciences

• LETTER •

February 2022, Vol. 65 129102:1–129102:2
https://doi.org/10.1007/s11432-019-2628-9

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*

Received 5 May 2019/Revised 21 July 2019/Accepted 16 August 2019/Published online 21 May 2021

Citation Du J, Wang W, Li M Z, et al. Related-tweakey impossible differential attack on QARMA-128. Sci China Inf Sci, 2022, 65(2): 129102, https://doi.org/10.1007/s11432-019-2628-9

Dear editor,

QARMA [1] is a family of hardware-oriented lightweight tweakable block ciphers designed by Avanzi. It contains two versions, which support block sizes of 64 and 128 bits, denoted by QARMA-64 and QARMA-128, respectively. The structure of QARMA is an Even-Mansour scheme [2] with a keyed pseudo-reflector, and the TWEAKEY framework is taken as an inspiration. Avanzi claimed that QARMA is understood to offer n bits of (time-data tradeoff) security if no better attacks are possible than time $2^{n-d-\epsilon}$ with 2^d chosen or known {plaintext, ciphertext, tweak} triples, for a small ϵ, e.g., 2. The security declaration is under the assumption that the attacker does not have control over the key, but may have full control over the tweak. Impossible differential cryptanalysis was first proposed by Biham et al. [3], the attacker can take advantage of the relation of two tweakeys in related-tweakey scenarios [4]. Yang et al. [5] proposed an impossible differential attack on QARMA, but the results are invalid due to the security claim of the designers.

Differential properties of matrix M. Denote the columnwise input difference of matrix M by $\Delta\mathrm{In}$, and the output difference by $\Delta\mathrm{Out}$.

Proposition 1. If $\Delta\mathrm{In} = (0, \alpha, \alpha \ggg 1, \alpha \ggg 4)$, then the output difference $\Delta\mathrm{Out} = (\alpha \lll 3, 0, 0, 0)$, where α is an arbitrary 8-bit value.

The proof and other three propositions are presented in Appendix A.

Distinguishers. Zong et al. [6] proposed an interesting method to search related-key impossible differentials from single key impossible differentials. Inspired by their idea, we also perform automatic search first. However, in order to reduce the data complexity, more active cells at the beginning of the distinguishers are preferred, so that we can construct structures to reduce plaintexts. Therefore, by combining the differential properties proposed above and transition properties [1] of matrix M, we revise the result of our automatic search, and obtain two families of 6-round related-tweakey impossible differential distinguisher for QARMA-128, which are placed between Rounds 7 and 12. We explain distinguisher family No.1 in this part and show distinguisher family No.2 in Appendix B.

The entire trail is depicted in Figure 1. The related-tweakey impossible differential characteristic

$$\begin{aligned}&(\alpha(\beta \ggg 4)\varepsilon_1\gamma,\ \beta(\alpha \ggg 4)(\gamma \ggg 4)\varepsilon_2,\\ &\quad \varepsilon_3(\gamma \ggg 1)(\alpha \ggg 1)(\beta \ggg 1),\ 0\varepsilon_4 00)\\ &\nrightarrow (0000, \delta000, 0000, 0000)\end{aligned}$$

exists, if the following conditions are satisfied:

(1) $\Delta T_7[7]$ is the only active cell of ΔT_7;

(2) $\Delta W_{13}[4]$ is the only active cell of ΔW_{13}, and the equation $\Delta W_{13}[4] = \Delta T_{12}[4] = \delta$ 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 attacks.

Case 1. If the conditions (1, 2) are satisfied, then the characteristic

$$\begin{aligned}&(00\alpha 0, 000\beta, \gamma 000, 0\sigma 00)\\ &\quad \nrightarrow (0000, \delta000, 0000, 0000)\end{aligned}$$

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

Case 2. If the conditions (1, 2) are satisfied, then the characteristic

$$\begin{aligned}&(\alpha(\beta \ggg 4)\varepsilon_1\gamma,\ \beta(\alpha \ggg 4)(\gamma \ggg 4)\varepsilon_2,\\ &\quad \varepsilon_3(\gamma \ggg 1)(\alpha \ggg 1)(\beta \ggg 1),\ 0\varepsilon_4 00)\\ &\nrightarrow (0000, \delta000, 0000, 0000)\end{aligned}$$

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

Key recovery attacks. Based on two parallel 6-round distinguishers – distinguisher family No.1 (Case 1) and distinguisher family No.2 (Case 2), we mount a key recovery attack on 10-round QARMA-128 by adding one round before the distinguisher and three rounds after it. The details of this attack are described in Appendix C. The data complexity is $2^{104.02}$ triples while the time complexity is $2^{120.94}$ 10-round encryptions, and the memory complexity is $2^{94.50}$ 128-bit.

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

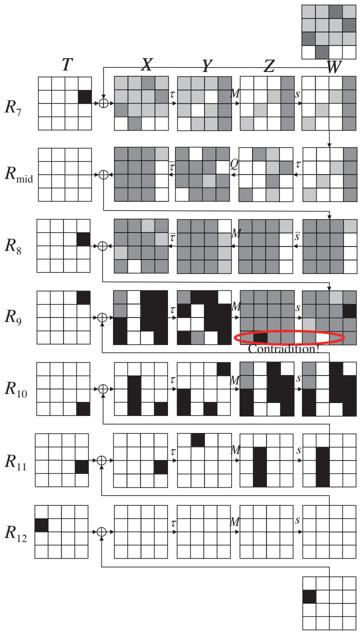

Figure 1 (Color online) Distinguisher family No.1. The black cells are active while the white ones are inactive, the dark and light gray cells could be active or inactive.

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 1), the attack requires $2^{102.54}$ triples and $2^{145.98}$ 11-round encryptions. The memory complexity is $2^{135.54}$ 128-bit. The details of this attack are described in Appendix D.

Conclusion. We investigate some interesting properties of the matrix M firstly, which portray the propogation of differential characteristics. Then we construct two families of 6-round related-tweakey impossible differential distinguishers for QARMA-128. Based on two parallel 6-round distinguishers, we proceed key recovery attacks on 10-round QARMA-128 including the outer whitening keys. We also mount 11-round attacks omitting outer whitening keys in a chosen ciphertext-tweak scenario. Our results are the best impossible differential attacks on QARMA-128 compared to the published ones.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61572293), Science and Technology on Communication Security Laboratory of China (Grant No. 9140c110207150c11050), Key Science Technology Project of Shandong Province (Grant No. 2015GGX101046), and Chinese Major Program of National Cryptography Development Foundation (Grant No. MMJJ20170102). Wei WANG was partially supported by Open Research Fund from Shandong Provincial Key Laboratory of Computer Network (Grant No. SDKLCN-2017-04).

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Avanzi R M. 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

2 Even S, Mansour Y. A construction of a cipher from a single pseudorandom permutation. J Cryptol, 1997, 10: 151–161

3 Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. J Cryptol, 2005, 18: 291–311

4 Liu G Z, Ghosh M, Song L. Security analysis of SKINNY under related-tweakey settings. IACR Trans Symmetric Cryptol, 2017, 2017: 37–72

5 Yang D, Qi W F, Chen H J. Impossible differential attack on QARMA family of block ciphers. IACR Cryptol ePrint Arch, 2018, 2018: 334

6 Zong R, Dong X Y, Wang X Y. MILP-aided related-tweak/key impossible differential attack and its applications to QARMA, Joltik-BC. IACR Cryptol ePrint Arch, 2018, 2018: 142