AN INVARIANT OF THE ROUND FUNCTION OF QARMA V2-64

TIM BEYNE

JUNE 19, 2023

Abstract

This note shows that there exists a nontrivial invariant for the unkeyed round function of QARMA v2-64. It is invariant under translation by a set of 2^{32} constants. The invariant does not extend over all rounds of QARMA v2-64 and probably does not lead to full-round attacks. Nevertheless, it might be of interest as it can be expected to give meaningful weak-key attacks on round-reduced instances when combined with other techniques such as integral cryptanalysis.

QARMA v2-64 is a family of tweakable block ciphers that was recently proposed by Avanzi *et al.* [1]. The authors argue that QARMA v2-64 does not have invariant subspaces for any number of rounds. This note shows that there exists a nonlinear invariant for the unkeyed round function of QARMA v2-64, and that this property can be extended to multiple rounds for weak keys. Nevertheless, full-round instances of QARMA v2-64 are not affected. It is worth noting that QARMA does not have a similar invariant.

Using the optimization tool from [2], one can search for joint eigenvectors of the correlation matrices of the linear and nonlinear layers. To ensure invariance under all cell permutations, the search was limited to symmetric rank-one invariants, *i.e.* functions of the form $v^{\otimes 16}$ with $v \in \mathbb{R}^{\mathbb{F}_2^4}$. It turns out that there exists a nontrivial eigenvector of this form, given by

$$v = 1/2 \cdot (0,0,0,1,0,0,1,0,0,-1,0,0,1,0,0,0)\,.$$

Since $\operatorname{supp} v = \mathtt{3} + \{\mathtt{0},\mathtt{5},\mathtt{a},\mathtt{f}\}$, it holds that $C^k v = (-1)^{k_1+k_2}\, v$ if $k_1 = k_3$ and $k_2 = k_4$. Hence, $v^{\otimes 16}$ is preserved under the addition of a set of 2^{32} constants. Note that v is the Walsh-Hadamard transformation of a quadratic Boolean function $f : \mathbb{F}_2^4 \to \mathbb{F}_2$, with

$$f(x_4, x_3, x_2, x_1) = (x_1 + x_3)(x_2 + x_4) + x_2 + x_3\,.$$

That is, every input/output pair (x, y) of the unkeyed QARMA v2-64 round function satisfies $\sum_{i=1}^{16} f(x_i) = \sum_{i=1}^{16} f(y_i)$, with $x_1, \ldots x_{16}$ and $y_1, \ldots, y_{16}$ the nibbles of x and y respectively.

References

[1] Roberto Avanzi, Subhadeep Banik, Orr Dunkelman, Maria Eichlseder, Shibam Ghosh, Marcel Nageler, and Francesco Regazzoni. The tweakable block cipher family QARMAv2. Cryptology ePrint Archive, Paper 2023/929, 2023. `https://eprint.iacr.org/2023/929`.

[2] Tim Beyne. A geometric approach to linear cryptanalysis. In Mehdi Tibouchi and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I*, volume 13090 of *Lecture Notes in Computer Science*, pages 36–66. Springer, 2021.