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 $v \in \mathbb{F}_2^7$. It turns out that there exists a nontrivial eigenvector of this form, given by

$$v = \frac{1}{2} \cdot (0, 0, 0, 1, 0, 0, 1, 0, 0, -1, 0, 0, 1, 0, 0, 0).$$

Since $\text{supp } v = 3 + \{0, 5, a, f\}$, 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 $f : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2$, 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
