NONLINEAR INVARIANTS OF CRAFT

TIM BEYNE AND MICHIEL VERBAUWHEDE

Abstract. This note shows that the round function of Craft admits nonlinear invariants that activate only four S-boxes. These invariants extend to invariants of the full cipher that hold for 2^{120} out of 2^{128} keys and 2^{60} out of 2^{64} possible tweaks. Since there are four similar nonlinear invariants that hold under independent conditions on the master key, this yields nearly 2^{122} weak keys for the all-zero tweak. If 64 different weak tweaks can be chosen, then for at least half of the keys, one or more of these nonlinear invariants holds. Further invariants with a slightly different structure can also be found. The same invariants were found independently by Roberto Civino. These results imply that Craft is, for all practical purposes, insecure.

1. Introduction

Craft is a tweakable block cipher designed by Beierle, Leander, Moradi, and Rasoolzadeh [2] for efficient protection against differential fault attacks. It is a 32-round cipher with 64-bit blocks, 128-bit keys, and 64-bit tweaks. For the details, refer to the original specification [2]. This note shows that the round function of Craft exhibits nonlinear invariants that activate only four cells of the state. This is despite the fact that the designers rely on the security arguments from Beierle, Canteaut, Leander, and Rotella [1] to argue that no nonlinear invariants exist. However, the arguments of [1] do not cover all possible cases, which makes Craft an interesting case study.

Throughout this note, we use an updated version of the notation introduced in [3] to describe rank-one approximations. It is possible to find the invariants reported here using the automated tool from [3, §6]. All properties are described in terms of functions $\mathbf{F}_2^n \to \mathbf{R}$, i.e. the 'dual' point of view in the geometric approach to cryptanalysis. Throughout this note, for u in $\mathbf{F}_2^n$, let $\chi^u \colon \mathbf{F}_2^n \to \mathbf{R}$ denote the additive character of $\mathbf{F}_2^n$ defined by $\chi^u(x) = (-1)^{u^\mathsf{T} x}$.

Remark 1. The observations in this note were found as a result of investigating the properties of Craft that were discovered in [4] by Roberto Civino, who contacted the authors about his work. The authors subsequently suspected the existence of invariants, and this turned out to be the case. After finding the invariants described in this note, they reported them to Civino, who meanwhile had independently discovered the same nonlinear invariants. His results have appeared in another ePrint paper [5].

2. A nonlinear invariant of the Craft round function

Consider the following two functions on $\mathbf{F}_2^4$, where S denotes the Craft S-box:

$$v = \chi^{\mathtt{0101}} \circ S = -\frac{1}{2}\left(\chi^{\mathtt{1010}} + \chi^{\mathtt{1011}} - \chi^{\mathtt{1110}} + \chi^{\mathtt{1111}}\right),$$
$$w = -\frac{1}{2}\left(\chi^{\mathtt{1010}} - \chi^{\mathtt{1011}} + \chi^{\mathtt{1110}} + \chi^{\mathtt{1111}}\right).$$

The pullback of the function $\chi^{\mathtt{0101}} \otimes \chi^{\mathtt{0101}} \otimes w \otimes \chi^{\mathtt{0000}}$ under the MixColumn operation M of Craft is $\chi^{\mathtt{0101}} \otimes \chi^{\mathtt{0101}} \otimes v \otimes \chi^{\mathtt{0000}}$:

$$T^{M^\vee}\left(\chi^{\mathtt{0101}} \otimes \chi^{\mathtt{0101}} \otimes w \otimes \chi^{\mathtt{0000}}\right) = \chi^{\mathtt{0101}} \otimes \chi^{\mathtt{0101}} \otimes v \otimes \chi^{\mathtt{0000}}.$$

The function v is invariant under addition by k in $\{\mathtt{0000}, \mathtt{0010}, \mathtt{1000}, \mathtt{1010}\}$. In addition, for k in $\{\mathtt{0101}, \mathtt{0111}, \mathtt{1101}, \mathtt{1111}\}$, we have $T^{k^\vee} w = \pm v$ with $T^{k^\vee}$ the pullback operator of $x \mapsto x + k$. These relations lead to the invariant shown in Figure 1, where $\chi^{\mathtt{5}} = \chi^{\mathtt{0101}}$.

There is a second invariant obtained by shifting the invariant in Figure 1 to the last two columns. Each round imposes four linearly independent conditions on the round keys, and

Date: 17/11/2026.

Tim Beyne is supported by the Research Foundation – Flanders (FWO) with reference № 1221827N.

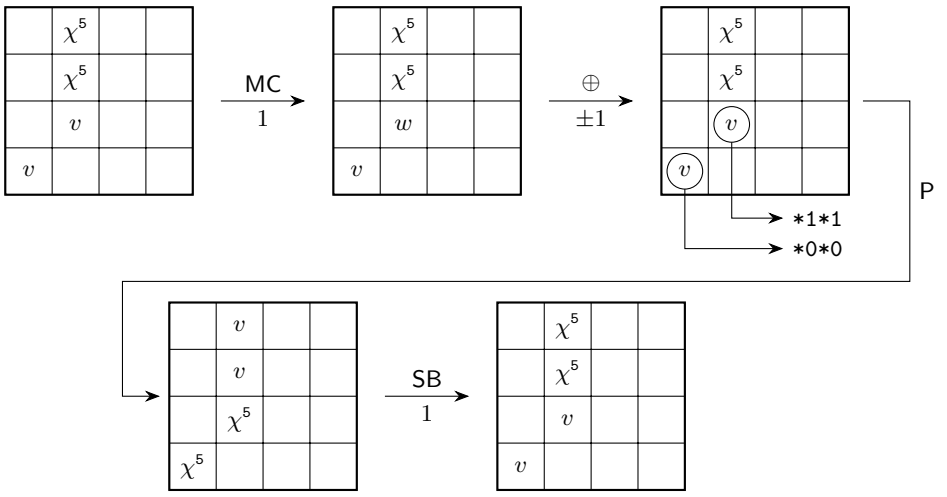


FIGURE 1. Nonlinear invariant of one-round CRAFT. Empty cells correspond to χ^{0000}. Circled cells indicate linear conditions on the round tweakey.

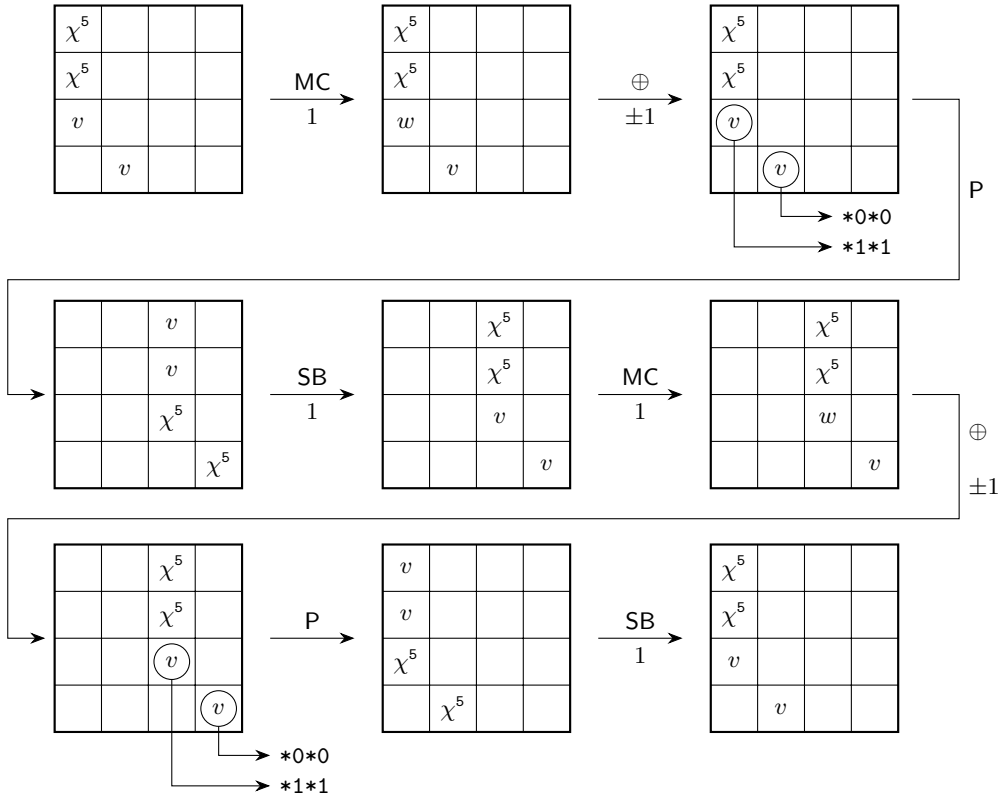


FIGURE 2. Two-round invariant of CRAFT, using the same conventions as Figure 1.

these conditions are compatible with the round constants and the key schedule under the all-zero tweak. Since the round key alternates between two halves of the master key, a fraction 2^{-8} of the keys is weak for each one of these two invariants. In general, these invariants hold for a fraction 2^{-4} of tweaks. For example, for the first invariant, nibbles three and nine, and nibbles six and twelve of the tweak should agree on the two relevant bits.

There are two other (two-round) invariants that are minor variations on the invariant in Figure 1, and that use the same functions χ^{0101}, v and w. Their input state is obtained by taking the mirror image of these two invariants, and they alternate between two shifted activity patterns. This is illustrated in Figure 2. Many other invariants with a slightly different structure

can be found, but they hold for a smaller number of weak keys. Some additional examples are given in Section 3.

Remark 2. All of the invariants described above are nonlinear invariants. An equivalent description is that $v = (-1)^f$, where $f\colon \mathbf{F}_2^4 \to \mathbf{F}_2$ is the quadratic Boolean function with algebraic normal form $f(x_4, x_3, x_2, x_1) = x_1x_3 + x_1 + x_2 + x_4 + 1$.

3. Additional two-round invariants of Craft

As mentioned in Section 2, there are many other nonlinear invariants of Craft. Figures 3 to 5 give three such examples that activate six S-boxes, as opposed to four. For every key, there exists a tweak so that the combined tweakey is weak for one of these three invariants. Turning this into a distinguisher that works for all keys requires 2^{17} chosen tweaks. In these figures, $v^u = \chi^u \circ S$ for u in $\mathbf{F}_2^4$, and in particular, $v = v^{0101}$. Some of the cells are labeled by pointwise products such as $\chi^a v^u$.

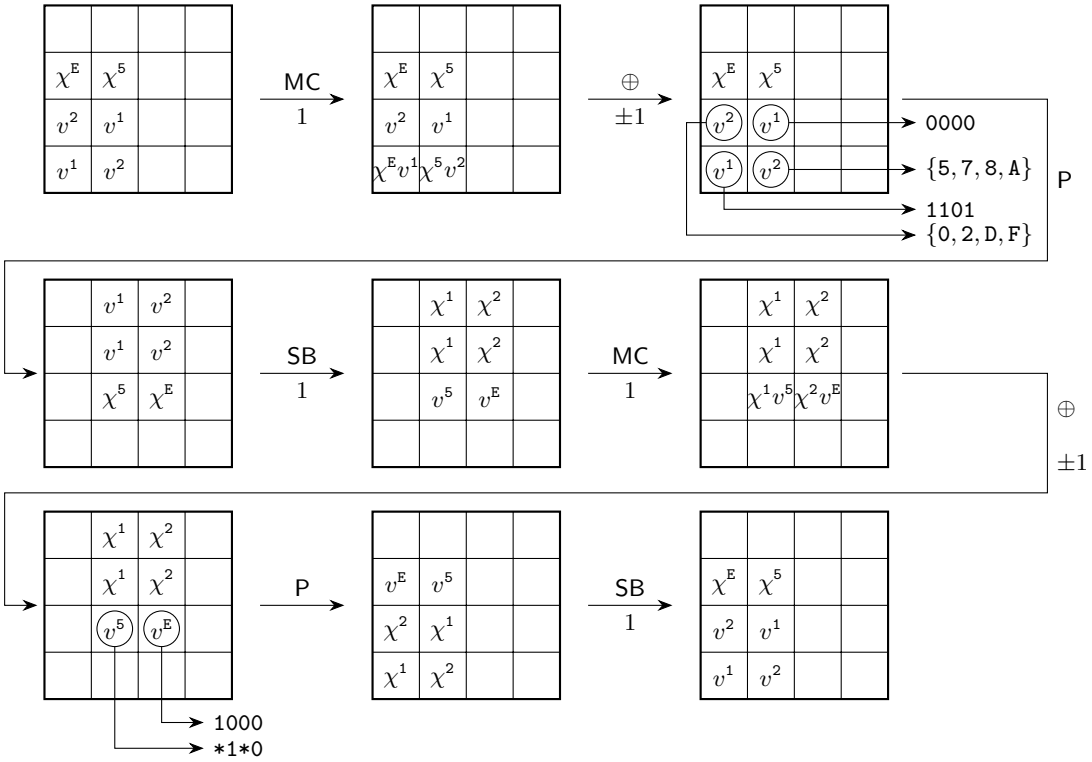


Figure 3. Two-round nonlinear invariant of Craft with six active cells.

4. Use of artificial intelligence tools

Anthropic's Claude Opus 5.5 model was used to automate checking a large number of candidate invariants for the activity pattern shown in Figure 1. This activity pattern was determined by reasoning about the structure of Craft. The other invariants were found by generalizing the first one with the help of Claude Opus 5.5. Up to minor changes, the figures were created by Claude Opus 5.5. All text was written by the authors.

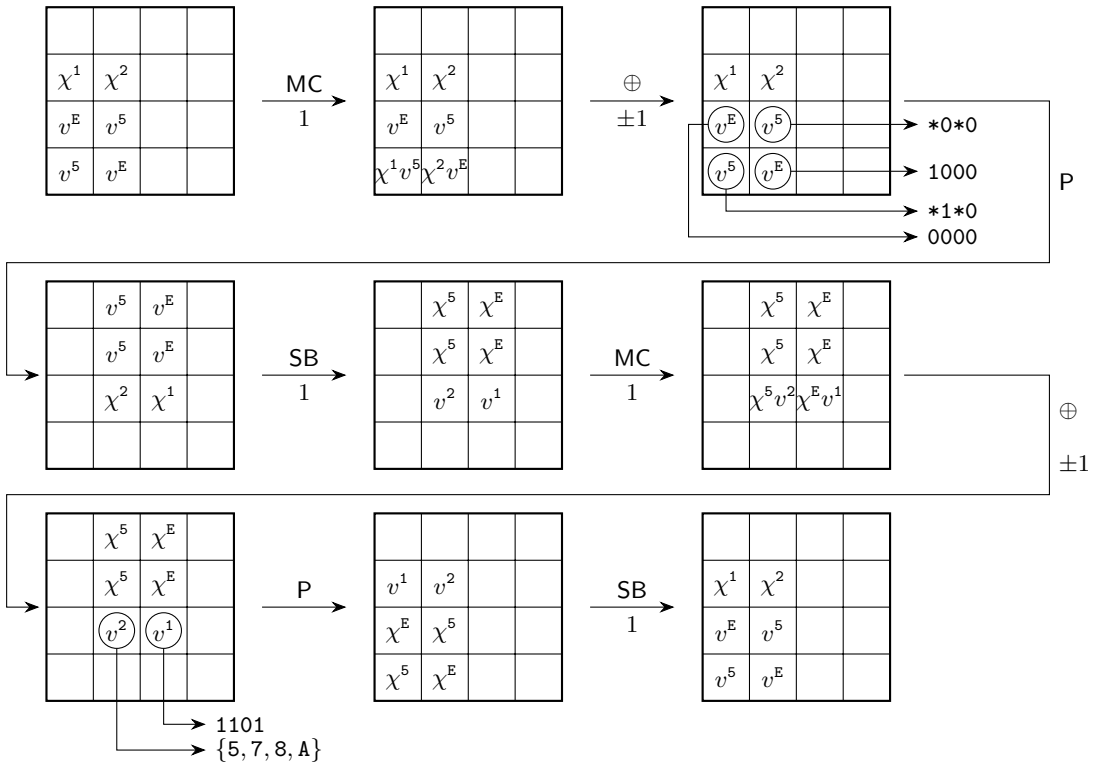


FIGURE 4. Two-round nonlinear invariant of CRAFT with six active cells.

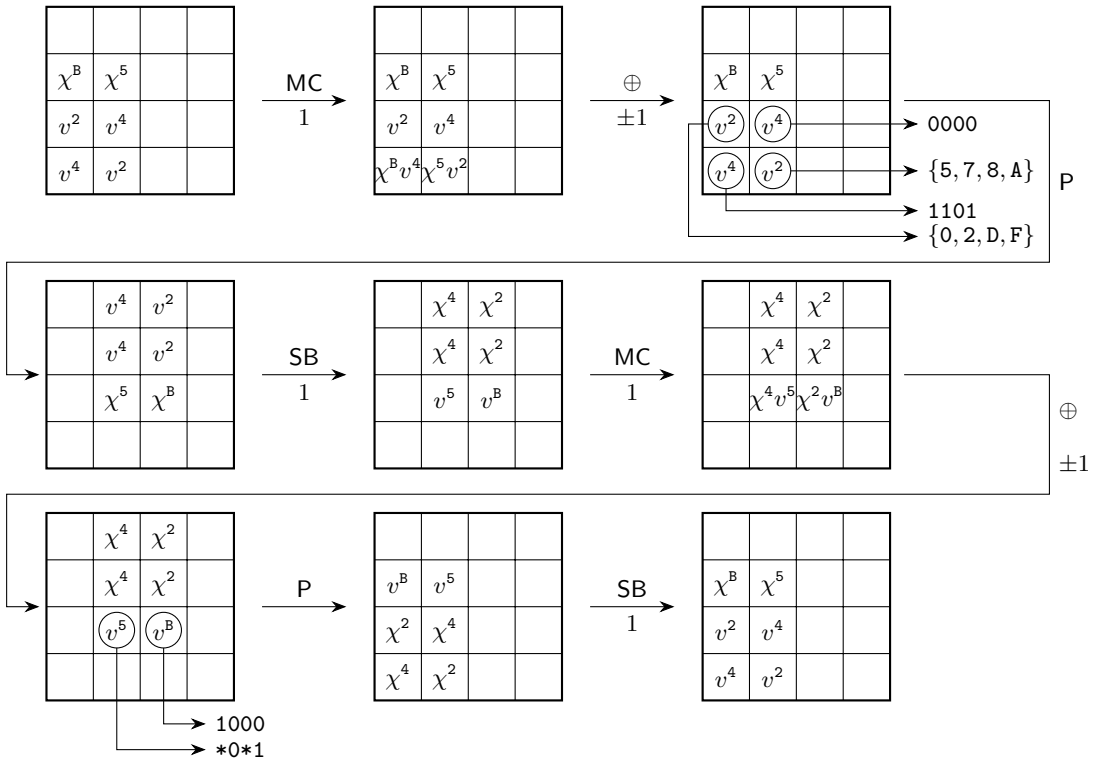


FIGURE 5. Two-round nonlinear invariant of CRAFT with six active cells.

References

[1] Christof Beierle, Anne Canteaut, Gregor Leander, and Yann Rotella. Proving resistance against invariant attacks: How to choose the round constants. In Jonathan Katz and Hovav Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 647–678. Springer, Cham, August 2017.

[2] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. CRAFT: Lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Trans. Symm. Cryptol.*, 2019(1):5–45, 2019.

[3] Tim Beyne. A geometric approach to linear cryptanalysis. In Mehdi Tibouchi and Huaxiong Wang, editors, *ASIACRYPT 2021, Part I*, volume 13090 of *LNCS*, pages 36–66. Springer, Cham, December 2021.

[4] Roberto Civino. Linear cryptanalysis with bibrace characters: Weak-key distinguishers for CRAFT. Cryptology ePrint Archive, Paper 2026/1767, 2026.

[5] Roberto Civino. Nonlinear invariant attacks on full CRAFT: Chosen-tweak key recovery. Cryptology ePrint Archive, Paper 2026/2918, 2026.

Email address: `firstname.lastname@esat.kuleuven.be`