Comprehensive security analysis of CRAFT

Hosein Hadipour[1], Sadegh Sadeghi[2], Majid M. Niknam[2] and Nasour Bagheri[3]

[1] Department of Mathematics and Computer Science, Tehran University, Tehran, Iran, hsn.hadipour@gmail.com

[2] Department of Mathematics, Faculty of Mathematical Sciences and Computer, Kharazmi University, Tehran, Iran, (S.Sadeghi.Khu,mmniknam)@gmail.com

[3] Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, Nabgheri@sru.ac.ir

Abstract. CRAFT is a lightweight involuntary block cipher, designed to provide efficient protection against differential fault attack. It is a tweakable cipher which encrypts a 64-bit plaintext using a 128-bit key and 64-bit public tweak. In this paper, compared to the designers' analysis, we provide a more detailed analysis of CRAFT against differential, linear hull, and zero correlation cryptanalysis. Our distinguishers for reduced round CRAFT cover more number of rounds compared to the designers' analysis. In our analysis, we observed a strange differential behavior of CRAFT, more precisely, for any number of rounds, the differential has an extremely higher probability compared to any differential characteristic. As an example, while the best characteristic for 11 rounds of the cipher has the probability of 2^{-80}, we presented a differential with the probability of 2^{-60}, contain 2^{20} characteristic, all with the same optimum probability of 2^{-80}. Next, we are using a partitioning technique, based on an optimal expendable truncated characteristic, to provide a better estimation of the differential effect on CRAFT. Thanks to technique, we were able to find differential distinguishers for 9, 10, 11, 12 and 13 rounds of the cipher in single tweak model with the probabilities of $2^{-40.204463}$, $2^{-45.124812}$, $2^{-49.799815}$, $2^{-54.726466}$ and $2^{-59.399491}$ respectively. These probabilities should be compared with the best distinguishers provided by the designers in the same model for 9 and 10 rounds of the cipher with the probabilities of $2^{-54.67}$ and $2^{-62.61}$ respectively.

In addition, we considered the security of CRAFT against the new concept of related tweak zero correlation (ZC) linear cryptanalysis and present a new distinguisher which covers 14 rounds of the cipher, while the best previous ZC distinguisher covered 13 rounds.

We also provide many related key characteristics for a full round cipher that the probability of any full round distinguisher will not be less than 2^{-32}. It is noteworthy to mention the designers has no claim against the related key attack and even provided a deterministic related key characteristic for full round cipher, and extended it to exhaustive key search with the complexity of 2^{124}. However, given our distinguishers, it is possible to recover the key with the complexity of 2^{40}.

Although the provided analysis does not compromise the cipher, we think it provides a better insight behind the designing of CRAFT.

Keywords: Lightweight block cipher · differential · linear hull · zero correlation · related key · tweak able cipher · MILP · CryptoSMT · CRAFT.

1 Introduction

Lightweight cryptography received extensive attention over the last decade, motivated by the emergent growth of resource-constrained devices such as RFID tags and IoT edge devices.

To address this demand, several lightweight primitives has been proposed by the researchers, to just name some, SKINNY [BJK+16], PRESENT [BKL+07], MIBS [ISSK09], SIMON [BSS+15], SPECK [BSS+15], Quark [AHMN13] and PHOTON [GPP11]. In this direction, recently, the NIST lightweight cryptography competition also announced its first-round candidates. Among lightweight primitives, (tweakable) block ciphers received more attention and many nice designs have been proposed already, each of them targeting different application. A tweakable block cipher maps a n-bit plaintext to a n-bit ciphertext using a k-bit secret key and a t-bit tweak.

On the other hand, Side-Channel Analysis (SCA) attacks, such as power/time analysis and fault analysis, are targeting implementation of ciphers and protecting a cipher against them requires extra cost, e.g. extra area. Given the constraints of target applications of lightweight block ciphers, it may not be possible to protect them using conventional approaches, e.g., protecting using hardware redundancy for fault analysis which commonly requires double area compared to the unprotected cipher. Hence, several researches aimed to provide efficient protection against SCA from design. More precisely, they selected component to design cipher such that they can provide efficient protection against a specific attack,e.g., LS-Designs [GLSV14], ZORRO [GGNS13] and Fides [BBK+13].

In this direction, to provide efficient protection against differential fault analysis, Beierle et al. proposed CRAFT [BLMR19], which is a tweakable lightweight block cipher. In addition, they supported their design by extensive analysis against known attacks, e.g., differential cryptanalysis, impossible differential cryptanalysis, linear cryptanalysis, zero correlation cryptanalysis and so on. Their analysis shows that the cipher provides desired security against these attacks. However, there is room for third-party analysis yet. In addition, related tweak zero correlation [ADG+19] is a new concept which has been proposed after the publication of CRAFT, hence, it worth to investigate the security of the cipher against this attack. Moreover, although the designers have no security claim against related-key attacks, they presented an exhaustive key search based on a trivial deterministic related-key differential characteristic with the complexity of 2^{124}. Hence, we are interested to see whether it is possible to reduce the complexity of the key recovery in this mode. In addition, due to the nature of the differential and linear hull cryptanalysis, which require to search over a very large space of all possible characteristics, it should be always possible to improve the previous analysis by using advanced search approaches. Hence, in this paper, we tackle the detailed security analysis of CRAFT against the above-mentioned analysis. The paper's contribution is summarized as follows:

1. We present a 14 round zero correlation distinguisher characteristic for the cipher in the related tweak mode. It should be compared with the 13 round distinguisher proposed by the designer, however, is single tweak mode.

2. Thanks to the advance automated search models based on CryptoSMT [Köl19] and MILP, we are able to improve the designers' bounds for differential cryptanalysis. More precisely, while the designers claim on the probability of differential for 9 and 10 rounds of the cipher are respectively $2^{-54.67}$ and $2^{-62.61}$, we are able to present 9, 10, 11, 12 and 13 rounds of the cipher in single tweak model with the probabilities of $2^{-40.204463}$,$2^{-45.124812}$,$2^{-49.799815}$,$2^{-54.726466}$ and $2^{-59.399491}$ respectively

3. We present several iterative related-key differential characteristics for 4 round of the cipher each has the probability of 2^{-4}. Hence, any of them can be extended to a full round distinguisher with the probability of at least 2^{-32} (if the last round includes an active Sbox then the probability will be 2^{-31}). Compared to the provided full round related key distinguisher by the designers that have the probability of 1, it can recover the key with much lower complexity, 2^{40} compared to 2^{124}.

The rest of the paper is organized as follows: in Section 2 we present the required preliminaries and also describe CRAFT briefly. In Section 3 we present the zero correlation

in related tweak mode. Differential and linear hull analysis are described in Section 4 and Section 5 respectively. Finally, we conclude the paper in Section 6. In addition, the Appendix A describes the related key cryptanalysis of the cipher.

2 Preliminaries

In this section, we present the required preliminaries and a brief description of `CRAFT`.

2.1 A brief description of `CRAFT`

`CRAFT` is a 64-bit lightweight block cipher which supports 128-bit key and 64-bit tweak. It takes a 64-bit plaintext $m = m_0\|m_1\|\cdots\|m_{14}\|m_{15}$ to initiate a 4×4 internal state $IS = I_0\|I_1\|\cdots\|I_{14}\|I_{15}$ as follows, where $I_i, m_i \in \{0,1\}^4$:

$$IS = \begin{pmatrix} I_0 & I_1 & I_2 & I_3 \\ I_4 & I_5 & I_6 & I_7 \\ I_8 & I_9 & I_{10} & I_{11} \\ I_{12} & I_{13} & I_{14} & I_{15} \end{pmatrix} = \begin{pmatrix} m_0 & m_1 & m_2 & m_3 \\ m_4 & m_5 & m_6 & m_7 \\ m_8 & m_9 & m_{10} & m_{11} \\ m_{12} & m_{13} & m_{14} & m_{15} \end{pmatrix}$$

Then, the internal state is going through 32 rounds $\mathcal{R}_i, i \in 0,\cdots,31$, to generate a 64-bit ciphertext. As it is depicted in Figure 1, each round, exclude the last round, includes five functions, i.e., a binary MixColumn (`MC`), the round dependent combining with round constant AddConstants (`ARC`), the round dependent mixing with the sub-tweakey AddTweakey (`ATK`), a nibble-based permutation PermuteNibbles (`PN`) and the substitution layer S-box (`SB`). The last round only includes `MC`, `ARC` and `ATK`, i.e. $\mathcal{R}_{31} = ATK_{31} \circ ARC_{31} \circ MC$, while for any $0 \leq i \leq 30$, $\mathcal{R}_i = SB \circ PN \circ ATK_i \circ ARC_i \circ MC$.

`MC` is a multiplication of internal state by the following binary matrix:

$$MC = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

After `MC`, in each round i two round dependent constant nibbles $a_i = (a_3^i, a_2^i, a_1^i, a_0^i)$ and $b_i = (b_2^i, b_1^i, b_0^i)$ are XOR-ed with I_4 and I_5 respectively (a_0^i and b_0^i are the least significant bits). A 4-bit LFSR and a 3-bit LFSR are used to update a and b for each round. Those LFSR are initialized by values (0001) and (001) respectively and updated to $a_{i+1} = (a_1^i \oplus a_0^i, a_3^i, a_2^i, a_1^i)$ and $b_{i+1} = (b_1^i \oplus b_0^i, b_2^i, b_1^i)$ from i-th round to $i+1$-th round.

After AddConstants (`ARC`), a 64-bit round tweakey is XOR-ed with IS. The tweakey scheduled of `CRAFT` is rather simple. Given the secret key $K = K_0\|K_1$ and the tweak $T \in \{0,1\}^{64}$, where $K_i \in \{0,1\}^{64}$, four round tweakeys $TK_0 = K_0 \oplus T$, $TK_1 = K_1 \oplus T$, $TK_2 = K_0 \oplus Q(T)$ and $TK_3 = K_1 \oplus Q(T)$ are generated, where given $T = T_0\|T_1\|\cdots\|T_{14}\|T_{15}$, $Q(T) = T_{12}\|T_{10}\|T_{15}\|T_5\|T_{14}\|T_8\|T_9\|T_2\|T_{11}\|T_3\|T_7\|T_4\|T_6\|T_0\|T_1\|T_{13}$. Then at the round $\mathcal{R}_i$, $TK_{i \bmod 4}$ is XOR-ed with the IS, where rounds are started from $i = 0$.

The next round function is PermuteNibbles (`PN`) which is applying an involuntary permutation P over nibbles of IS, where given $IS = I_0\|I_1\|\cdots\|I_{14}\|I_{15}$, $P(IS) = I_{15}\|I_{12}\|I_{13}\|I_{14}\|I_{10}\|I_9\|I_8\|I_{11}\|I_6\|I_5\|I_4\|I_7\|I_1\|I_2\|I_3\|I_0$.

The final round-function is a linear 4×4-bit S-box, which has been borrowed from MIDORI [BBI+15]. The table representation of the S-box is represented in Table 1.

Through the paper, we represent the internal state at the input of round-r by $x^r = x_0^r\|x_1^r\|\cdots\|x_{14}^r\|x_{15}^r$, after `MC` by $y^r = y_0^r\|y_1^r\|\cdots\|y_{14}^r\|y_{15}^r$ and after the `PN` layer by $z^r = z_0^r\|z_1^r\|\cdots\|z_{14}^r\|z_{15}^r$. It is clear that the state after `SB` is the input of the next round which is x^{r+1}. The tweak which is used in that round is denoted by $TK^r = TK_0^r\|TK_1^r\|\cdots\|TK_{14}^r\|TK_{15}^r$.

Table 1: A round of CRAFT

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$S(x)$	c	a	d	3	e	b	f	7	8	9	1	5	0	2	4	6

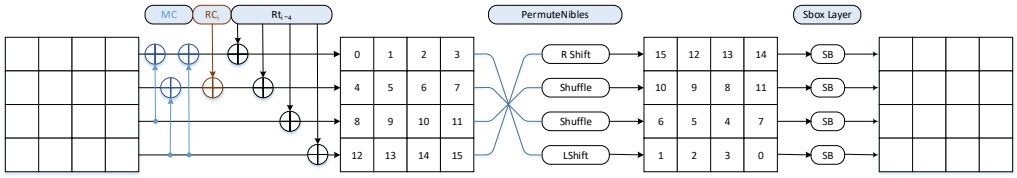


Figure 1: A round of CRAFT

3 Related tweak key zero correlation cryptanalysis

In this section, we apply the related tweak key zero correlation attack [ADG+19] to a reduced-round version of CRAFT. As a result, we found a 14-round zero-correlation linear hull for CRAFT, where the number of forward and backward rounds are both reduced to 7. With respect to Figure 2, active linear masks are applied to two cells 4 and 12 at the input, and the active linear mask is applied to cell 4 in the state at the output. Then, we focus on the tweak cell labeled 11, where is depicted by using a red frame in Figure 2. Let T shows the XOR of all tweaks in the rounds 1 to 14. In the following, we show if we choose the following active linear mask in the tweak T, we can have a 14-round related tweak zero correlation for CRAFT:

$$T = \bigoplus_{i=1}^{14} Ti = \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & 8 \\ * & * & * & * \end{pmatrix},$$

where $*$ can take any constant. Note that the permutation Q operated on Ti, when $i = 3, 4, 7, 8, 11, 12$.

Based on the Figure 2, we have $T[11] = T6[11] \oplus T7[8]$ (the XOR of red frames) and so,

$$T6[11] \oplus T7[8] = 8. \tag{1}$$

Now, based on the properties of PN and SB operation of 6-th round, we have

$$C[0] = LAT(B[15])), \tag{2}$$

where LAT shows the Linear Approximation Table of CRAFT S-box (see Table 2). Due to the MC operation on the active cells of col(3) of state A in the input of 6-th round, we have

$$B[15] = B[11]$$

and so, based on the (2), we have

$$\begin{aligned} C[0] =& LAT(B[11])). \\ =& LAT(T6[11])). \end{aligned} \tag{3}$$

Now, due to the MC operation on the active cells of col(1) of state C in the input of 7-th round, we have

$$\begin{aligned} T7[8] =& C[0] \\ \overset{(3)}{=}& LAT(T6[11])). \end{aligned} \tag{4}$$

Therefore, based on the (1) and (4), $T6[11]$ and $T7[8]$ must satisfy the following conditions.

$$\begin{cases} T6[11] \oplus T7[8] = 8, \\ T7[8] = LAT(T6[11]). \end{cases}$$

These conditions are equivalent to find an input mask x ($x = T6[11]$) and an output mask y ($y = T7[8]$) so that

$$\begin{cases} x \oplus y = 8, \\ \Pr(y = LAT(x)) \neq 0. \end{cases}$$

Note that, by referring to linear approximation table of `CRAFT` S-box (see Table 2), we observe there is no input/output mask that satisfies these conditions.

Table 2: Linear approximation table of `CRAFT` S-box.

x/y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	4	2	-2	0	2	0	-2	0	2	0	4	-2	0	-2
2	0	4	0	0	4	0	0	0	-4	0	0	0	0	4	0	0
3	0	2	0	2	-2	0	2	4	2	-4	-2	0	0	2	0	2
4	0	-2	4	-2	2	0	-2	0	-2	-4	-2	0	0	-2	0	2
5	0	0	0	0	0	0	0	0	0	0	-4	-4	0	0	4	-4
6	0	2	0	2	-2	0	2	-4	-2	0	-2	0	-4	-2	0	2
7	0	0	0	4	0	0	-4	0	0	0	0	-4	0	0	-4	0
8	0	-2	-4	2	-2	0	-2	0	-4	-2	0	2	2	0	2	0
9	0	0	0	-4	-4	0	0	0	-2	2	-2	-2	2	2	-2	2
A	0	2	0	-2	-2	-4	-2	0	0	-2	4	-2	-2	0	2	0
B	0	0	0	0	0	-4	0	-4	2	-2	-2	2	2	2	-2	-2
C	0	4	0	0	0	0	-4	0	2	2	-2	2	2	-2	2	2
D	0	-2	4	2	-2	0	-2	0	0	2	0	2	-2	4	2	0
E	0	0	0	0	0	4	0	-4	2	-2	2	-2	2	2	2	2
F	0	-2	0	2	2	-4	2	0	0	2	0	-2	2	0	2	4

Based on [SLR+15], we can convert our zero-correlation linear hull for 14 rounds of `CRAFT`, to a related-tweak integral distinguisher covering the same number of rounds.

4 Differential effect cryptanalysis

The designers of `CRAFT` provided extensive security analysis against differential and linear cryptanalysis [BLMR19, See Table 5]. They have provided the minimum number of active S-boxes for differential/linear cryptanalysis in single and related tweak (for differential) mode. In addition, they have provided their analysis for differential (resp. linear hull) of round reduced `CRAFT`. In single tweak mode, they presented a differential distinguisher for 9 and 10 rounds of the cipher with the probability of $2^{-54.67}$ and $2^{-62.61}$ respectively. For related tweak mode, depending on the starting round based on the TK value, they have presented 15, 16, 17 and 16 round differential distinguisher when the cipher is started from round 0, 1, 2, and 3 respectively. The probability of the presented distinguisher are $2^{-55.14}$, $2^{-57.18}$, $2^{-60.14}$, and $2^{-55.14}$ respectively.

We developed automated tools, based on MILP and CryptoSMT, to verify their results at the first. In the ST-mode, we reached the same number of active S-boxes, but an interesting observation was finding paths with optimum probability, i.e. all S-boxes where activated by the maximum possible probability, i.e. 2^{-4} in differential/linear cryptanalysis (we only found a typo for their report of 17 rounds of RT_1, and 13 rounds of RT_0 which were reported to be 44, and 36 active S-boxes respectively, while it should be 46, and 35 respectively). Table 3 represented the minimum number of active S-boxes and also the maximum probability of a single trail for the different number of rounds in different model of analysis.

Table 3: Optimum Differential/linear Characteristics for reduced CRAFT in different model, where for each model the upper row determines the minimum number of active S-boxes and the bellow row shows the $-log_2 P$ and P denotes the probability of the best-found characteristic.

Model	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Linear	1	2	4	6	10	14	20	26	32	36	40	44	48	52	56	60	64
$-log2$	2	4	8	12	20	28	40	52	64	72	80	88	96	104	112	120	128
ST Diff.	1	2	4	6	10	14	20	26	32	36	40	44	48	52	56	60	64
$-log2$	2	4	8	12	20	28	40	52	64	72	80	88	96	104	112	120	128
RT0 Diff.	0	1	2	4	6	12	14	19	22	25	27	32	35	38	40	46	49
-log2	1	2	4	8	12	24	28	38	44	50	54	64	70	76	80	92	98
RT1 Diff.	0	1	2	5	7	10	15	18	22	24	28	32	35	38	43	45	44
$-log2$	1	2	4	10	14	20	30	36	44	48	56	64	70	76	86	90	92
RT2 Diff.	0	1	2	4	6	12	16	19	21	24	27	30	34	39	41	42	44
$-log_2$	1	2	4	8	12	24	32	38	42	48	54	60	68	78	82	84	88
RT3 Diff.	0	1	2	5	7	10	15	18	21	24	28	31	34	38	39	41	47
$-log_2$	1	2	4	10	14	20	30	36	42	48	56	62	68	76	78	82	94

In the next sections, to enumerate differential characteristics in a differential effect, we will use the following observation such as the papers [LWR16, KLT15] to enumerate all solutions in a SAT solver.

1. Build the CNF model for the problem, ask the solver to give one solution x if it exists.
2. Add a new condition to the current CNF model in order to remove x.
3. Ask solver to give a solution, repeat step 2 until the solver returns unsatisfiable.

4.1 Differential effect

In this section, we evaluated the differential behavior of the cipher against differential effect, by fixing the input and output mask and try to find a better differential probability. We observed that for an input/output mask that satisfy a characteristic with minimum number of active S-boxes there are many trails with optimum probability and all of them have an identical truncated patterns. While finding an estimation of the real differential behavior of a cipher could be a very time consuming task in general, this observation motivated us to use the bellow steps to provide a lower bound on the differential probability of CRAFT for different number of rounds:

1. Using MILP, find a truncated differential characteristic with the minimum number of active S-boxes.
2. Verify the correctness of the truncated differential characteristic by finding at least one characteristic that matches the found truncated patterns.
3. Based on the found characteristic, develop the constraints for CryptoSMT, to limit the search to the truncated pattern with fixed input/output in the previous step.

Following the above steps, we were able to accelerate the differential search for reduced rounds CRAFT dramatically. For instance, finding a bound for differential of 11 rounds of CRAFT coasted 86379s on a personal computer (Intel Core (TM)i-5, 8 Gig RAM, Windows 10 x64), were we reached $2^{-58.7704}$ based on 2458966 characteristics (all with optimum probability of 2^{-80}), while using this approach we reached the identical probability in half that time. Based on this approach, for 9 rounds of CRAFT, we find the following input/output mask with the differential of $2^{-44.37}$, contains 810592 trails, all with the probability of 2^{-64} and have been founded in 5417s on the above mentioned PC, which

has an advantage of $2^{10.3}$ compared to the distinguisher provided by the designers for the same number of rounds:

$$\texttt{7F0F 7F00 0000 7F00} \xrightarrow{\text{9-rounds;} \quad pr \geq 2^{-44.37}} \texttt{0A00 0000 0000 00DF}$$

It should be noted the presented bound is only the lower bounds, given that we limited our searches to optimum characteristics and a specific truncated differential path. In addition, given a truncated differential pattern that minimize the number of active S-boxes for a specific number of rounds, different characters with different input/output can be presented that satisfy optimum probability. In the above search, we selected one of them randomly (the first optimum characteristic which is found by the tool) and bounded its lower-bound of differential. However, it may be possible to find a better bound for that number of rounds using another input/output mask or considering other possibilities also, e.g., non-optimum patterns. For example, for 9 rounds, we changed all active nibbles of the input and the output mask of the above-mentioned characteristic to `A` and observed a considerable improvement. To be more precise, for the bellow mask we found 2024500 optimum trails, before interrupting the run due to the RAM limitation:

$$\texttt{AA0A AA00 0000 AA00} \xrightarrow{\text{9-rounds;} \quad pr \geq 2^{-43.051}} \texttt{0A00 0000 0000 00AA}$$

In the case of 10 rounds, with the input mask "`0AAA 00AA 0000 00AA`" and the output mask "`0A00 0000 0000 00AA`", using a `G9 Hp` server with 32 Gig RAM and Windows 10 x64 as the operating system, we were able to observe 3513898 optimal characteristics in 4 days, before interrupting the run, which provides the probability of the 10-round distinguisher to be at least $2^{-50.2554}$.

Although the above mentioned approach provides advantage over naive search, using the same computer system, to extended this approach to more number of rounds, e.g. 12 rounds and more, it was very time consuming. Hence, we used another approach. We observed that it is possible to comp up with expendable truncated characteristics for even (started from 8) and odd (started from 9) rounds of the cipher. Interestingly, this characteristics match the optimum number of active S-boxes for any round larger than 9. Figure 3 and Figure 4 represented the details of the construction of those characteristics. Moreover, setting active nibbles of input and output of each characteristic to `A`, provide us with a valid optimum characteristic. Hence, denoting the probability of an optimum characteristic for r-round of the cipher by $pr_c^{o,r}$, the bellow characteristic is valid for any even round-$r > 8$:

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{r-rounds;} \quad pr_c^{o,r} = 2^{-(56+8(r-8))}} \texttt{0A00 0000 0000 00AA}$$

For an odd round-$r > 8$, the differential characteristic will be as follows:

$$\texttt{AA0A AA00 0000 AA00} \xrightarrow{\text{r-rounds;} \quad pr_c^{o,r} = 2^{-(64+8(r-9))}} \texttt{0A00 0000 0000 00AA}$$

Any of Figure 3 and Figure 4 includes three partition, denoted by E_{in}, E_m and E_{out}. From now on, E_{in}^{even}, E_m^{even} and E_{out}^{even} and E_{in}^{odd}, E_m^{odd} and E_{out}^{odd} denote partitions of the cipher in Figure 3 and Figure 4 receptively, while $E_{in}^{even/odd}$, $E_m^{even/odd}$ and $E_{out}^{even/odd}$ denote partitions of any of them. Hence, to design 10-round and 12-round characteristics we respectively need the structures $E_{out}^{even} \circ E_m^{even} \circ E_{in}^{even}$ and $E_{out}^{even} \circ E_m^{even} \circ E_m^{even} \circ E_{in}^{even}$ while to design 9-round and 11-round characteristics we respectively need the structures $E_{out}^{odd} \circ E_{in}^{odd}$ and $E_{out}^{odd} \circ E_m^{odd} \circ E_{in}^{odd}$.

It worth-noting, the output mask E_{out}^{even} and E_{out}^{odd} are identical and the input mask of E_{in}^{even} can be matched to the input of E_{in}^{odd} by two nibbles rotation to right in each row.

Table 4: Differential distribution table (DDT) of `CRAFT` S-box.

x/y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	4	0	2	2	2	0	2	0	0	0	0	0	2	0
2	0	4	0	0	4	0	0	0	0	4	0	0	4	0	0	0
3	0	0	0	0	2	0	4	2	2	2	0	0	0	2	0	2
4	0	2	4	2	2	2	0	0	2	0	0	2	0	0	0	0
5	0	2	0	0	2	0	0	4	0	2	4	0	2	0	0	0
6	0	2	0	4	0	0	0	2	2	0	0	0	2	2	0	2
7	0	0	0	2	0	4	2	0	0	0	0	2	0	4	2	0
8	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
9	0	0	4	2	0	2	0	0	2	2	0	2	2	0	0	0
A	0	0	0	0	0	4	0	0	0	0	4	0	0	4	0	4
B	0	0	0	0	2	0	0	2	2	2	0	4	0	2	0	2
C	0	0	4	0	0	2	2	0	2	2	0	0	2	0	2	0
D	0	0	0	2	0	0	2	4	0	0	4	2	0	0	2	0
E	0	2	0	0	0	0	0	2	2	0	0	0	2	2	4	2
F	0	0	0	2	0	0	2	0	0	0	4	2	0	0	2	4

Moreover, form the DDT of the `CRAFT`'s S-box (Table 4), one can observe that if $x \in \{$`5,7,A,D,F`$\}$ then we can find at least one entry $y \in \{$`5,7,A,D,F`$\}$ such that with the probability of 2^{-2} also $s(x) = y$ and for any $y \in \{$`0,1,2,3,4,6,8,9,B,C,E`$\}$, the probability of $s(x) = y$ will be upper-bounded by 2^{-3}. On the other hand, we observed that any differential include many optimum characteristic, where each active S-box is activated with the probability 2^{-2}, and we were not even able to count all of them using our computational resources. These properties motivated us to do semi-truncated differential search for different parts of our models for even and odd rounds, i.e., E_{in}, E_m and E_{out} in Figures 3 and 4. For semi-truncated differential search, we programmed a model with the bellow constraints:

1. We set any active nibbles in the input of $E_{in}^{even/odd}$ and any active nibbles in the output of $E_{out}^{even/odd}$ to be `A`.

2. We limited any active intermediate nibble at the output of $E_{in}^{even/odd}$, the input/output of $E_m^{even/odd}$ and input of $E_{out}^{even/odd}$ to be in the set $\{$`5,7,A,D,F`$\}$.

3. we find the differential probability of all possible input/output mask of $E_{in}^{even/odd}$, $E_m^{even/odd}$ and $E_{out}^{even/odd}$, concern to the above constraints.

It is trivial that we have only one possible mask for the input of $E_{in}^{even/odd}$ and one possible mask for the output of $E_{out}^{even/odd}$. To determine possible output-masks of E_{in}^{even}, we should consider the pattern before (y^4) and after (z^4) the last `MC`. It can be seen that to satisfy the truncated differential pattern, we should have $y_{14}^4 = y_{10}^4 \neq y_6^4$. Hence, there are only $5 \times 5 \times 4 = 100$ possible values for z^4. A similar argument can be provided for the output mask of $E_{in}^{even/odd}$, and input/output masks of $E_m^{even/odd}$, and the input mask of $E_{out}^{even/odd}$. In the next step, we need to determine the differential probability of any possible input/output mask for any cipher's partition. Given those probabilities, we can design a joint probability vector/matrix for any of those cipher's partitions and then calculating the differential probability of any characteristic will be just multiplication of those joint probability vectors/matrices, which can be done very efficiently. To this end, we determined the joint probabilities vectors/matrices of all cipher's partitions. The joint probability vector of E_{in}^{even} includes 76 non-zero entry (out of 100) and it is identical to the joint probability vector derived for E_{in}^{odd}. The joint probability vectors of both E_{out}^{even} and E_{out}^{odd} include 92 non-zero entry (each out of 100). The joint probability matrices derived for E_m^{even} and E_m^{odd} also include 2734 non-zero entry (each out of 10000). Next, we used

those joint probability vectors/matrices to determine the differential effect of different variants of CRAFT.

$$\texttt{AA0A AA00 0000 AA00} \xrightarrow{\text{9-rounds; } pr = 2^{-40.204463}} \texttt{0A00 0000 0000 00AA}$$

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{10-rounds; } pr = 2^{-45.124812}} \texttt{0A00 0000 0000 00AA}$$

$$\texttt{AA0A AA00 0000 AA00} \xrightarrow{\text{11-rounds; } pr = 2^{-49.799815}} \texttt{0A00 0000 0000 00AA}$$

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{12-rounds; } pr = 2^{-54.726466}} \texttt{0A00 0000 0000 00AA}$$

$$\texttt{AA0A AA00 0000 AA00} \xrightarrow{\text{13-rounds; } pr = 2^{-59.399491}} \texttt{0A00 0000 0000 00AA}$$

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{14-rounds; } pr = 2^{-64.325252}} \texttt{0A00 0000 0000 00AA}$$

$$\texttt{0AAA 00AA 0000 00AA} \xrightarrow{\text{15-rounds; } pr = 2^{-68.998607}} \texttt{0A00 0000 0000 00AA}$$

The above distinguishers, to the best of our knowledge, are the best-known differential distinguishers for CRAFT in single tweak model. An interesting point for this approach is its extendability and time efficiency also. This result shows partitioning works well against CRAFT.

5 Linear hull

Linear cryptanalysis [Mat93] is a known plaintext attack and the attacker tries to find a high probability characteristic with an estimate for the parity bits of the plaintext (P), the ciphertext (C), and the secret key (K). In other words, the adversary finds an input mask α and an output mask β which yields a higher absolute bias ϵ as

$$\Pr[\alpha.P \oplus \beta.C = \gamma.K] = \frac{1}{2} + \epsilon(\alpha, \beta).$$

The correlation of a linear approximation is defined as $corr(\alpha, \beta) = 2\epsilon(\alpha, \beta)$. A linear hull [Nyb94] is a set of linear approximations with the same input mask α and the same output mask β. The potential (averaged linear probability over the key space K) of a linear hull is defined as

$$ALP(\alpha, \beta) = \sum_{\gamma} corr^2(\alpha, \beta) = \overline{corr}^2$$

Note that, the linear hull $\overline{corr}^2$ may be higher than $corr^2$ and so, there needs less plaintexts in the linear hull cryptanalysis than linear cryptanalysis .

In the following, we will investigate the linear hull effect on CRAFT. The 11-round of CRAFT, with input mask "0550000005500555" and output mask "A00A000000000A00" has average squared correlation $2^{-58.76}$ and the number of trails is 2464015 (all with optimum squared correlation of 2^{-80}). Note that, to reach this squared correlation, we limited the time of running to 86396 seconds on a personal computer (Intel Core (TM)i-5, 8 Gig RAM, Windows 10 x64).

Similar to the differential effect, for the linear hull, we observed that it is possible to come up with expendable truncated linear characteristics for CRAFT. Interestingly, this characteristic match the optimum number of active S-boxes for any round larger than 8. Figure 5 and Figure 6 represent the details of the construction of those characteristics for 13 and 14 rounds respectively. Moreover, setting active nibbles of input and output of each characteristic to $0x5$, provide us with a valid optimum characteristic. Hence, denoting the average squared correlation of an optimum characteristic for r-round of the cipher by $(corr^2)o, r_c$, the bellow characteristic is valid for any round-$r > 8$:

$$\texttt{0550 0000 0550 5550} \xrightarrow{\text{r-rounds;}\quad (corr^2)o, r_c = 2^{-(24+8(r-4))}} \texttt{0550 0000 0000 5000}$$

Moreover, from the LAT of the CRAFT's S-box (Table 4), one can observe that if $x \in \{\texttt{5,A,B,E,F}\}$ then we can find at least one entry $y \in \{\texttt{5,A,B,E,F}\}$ such that with the square correlation of 2^{-2} we have $\alpha.x = \beta.y$. These properties, and our results for differential effect of the cipher, motivated us to do semi-truncated linear hull search for different parts of our model, i.e., E_{in}, E_m and E_{out} in Figures 5 and 6, for 13 and 14 rounds. For semi-truncated linear hull search, we programmed a model with the bellow constraints:

1. We set any active nibbles in the input of E_{in} and active nibbles in the output of E_{out} to be 5.
2. We limited any active intermediate nibble at the output of E_{in}, the input/output of E_m and input of E_{out} to be in the set $\{\texttt{5,A,B,E,F}\}$.
3. We find the linear hull of all possible input/output mask of E_{in}, E_m and E_{out}, concern to the above constrains.

The primary results of these experiment is compliant with our results for differential effect analysis, reported in the previous section.

6 Conclusion

In this work, we provided a detailed analysis of CRAFT against differential and related tweak zero correlation cryptanalysis. Our related tweak zero correlation cryptanalysis, which covers 14 rounds, is the first analysis of CRAFT against this attack, given that the designers analyzed its security against single tweak zero correlation cryptanalysis. Our differential analysis improved the designers results significantly. For example, the designers report claims the probability of differential effect for 10 rounds of the cipher in single tweak model to be $2^{-62.61}$ while we presented a differential distinguisher for the same number of rounds with the probability of $2^{-51.84}$ and a differential distinguisher for 11 rounds with the probability of $2^{-58.44}$.

Through our differential analysis, we observed that for many fixed input/output mask, CRAFT include very strong clusters of high-probable characteristics that helped us to improve the probability of our differential distinguishers significantly. Although we did not provide bounds for extra rounds of the cipher, due to the computational limitation, we believe that the results for other rounds can also be improved significantly.

As a side result, we also provide related key characteristics for full round cipher which each has the probability of at least 2^{-32}. Although the designers have no claim against the related key attack, but they have provided a deterministic related key characteristic for full round cipher and extended it to exhaustive key search with the complexity of 2^{124}. However, given our distinguishers, it is possible to recover the key with the complexity of 2^{40}.

References

[ADG+19] Ralph Ankele, Christoph Dobraunig, Jian Guo, Eran Lambooij, Gregor Leander, and Yosuke Todo. Zero-correlation attacks on tweakable block ciphers with linear tweakey expansion. *IACR Trans. Symmetric Cryptol.*, 2019(1):192–235, 2019.

[AHMN13] Jean-Philippe Aumasson, Luca Henzen, Willi Meier, and María Naya-Plasencia. Quark: A lightweight hash. *J. Cryptology*, 26(2):313–339, 2013.

[BBI+15] Subhadeep Banik, Andrey Bogdanov, Takanori Isobe, Kyoji Shibutani, Harunaga Hiwatari, Toru Akishita, and Francesco Regazzoni. Midori: A block cipher for low energy. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part II*, volume 9453 of *Lecture Notes in Computer Science*, pages 411–436. Springer, 2015.

[BBK+13] Begül Bilgin, Andrey Bogdanov, Miroslav Knezevic, Florian Mendel, and Qingju Wang. Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware. In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 142–158. Springer, 2013.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe. PRESENT: an ultra-lightweight block cipher. In Pascal Paillier and Ingrid Verbauwhede, editors, *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings*, volume 4727 of *Lecture Notes in Computer Science*, pages 450–466. Springer, 2007.

[BLMR19] Christof Beierle, Gregor Leander, Amir Moradi, and Shahram Rasoolzadeh. CRAFT: lightweight tweakable block cipher with efficient protection against DFA attacks. *IACR Trans. Symmetric Cryptol.*, 2019(1):5–45, 2019.

[BSS+15] Ray Beaulieu, Douglas Shors, Jason Smith, Stefan Treatman-Clark, Bryan Weeks, and Louis Wingers. The SIMON and SPECK lightweight block ciphers. In *Proceedings of the 52nd Annual Design Automation Conference, San Francisco, CA, USA, June 7-11, 2015*, pages 175:1–175:6. ACM, 2015.

[GGNS13] Benoît Gérard, Vincent Grosso, María Naya-Plasencia, and François-Xavier Standaert. Block ciphers that are easier to mask: How far can we go? In Guido Bertoni and Jean-Sébastien Coron, editors, *Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings*, volume 8086 of *Lecture Notes in Computer Science*, pages 383–399. Springer, 2013.

[GLSV14] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici. Ls-designs: Bitslice encryption for efficient masked software implementations. In Carlos Cid and Christian Rechberger, editors, *Fast Software Encryption - 21st International Workshop, FSE 2014, London, UK, March 3-5, 2014.*

Revised Selected Papers, volume 8540 of *Lecture Notes in Computer Science*, pages 18–37. Springer, 2014.

[GPP11] Jian Guo, Thomas Peyrin, and Axel Poschmann. The PHOTON family of lightweight hash functions. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings*, volume 6841 of *Lecture Notes in Computer Science*, pages 222–239. Springer, 2011.

[ISSK09] Maryam Izadi, Babak Sadeghiyan, Seyed Saeed Sadeghian, and Hossein Arabnezhad Khanooki. MIBS: A new lightweight block cipher. In Juan A. Garay, Atsuko Miyaji, and Akira Otsuka, editors, *Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings*, volume 5888 of *Lecture Notes in Computer Science*, pages 334–348. Springer, 2009.

[KLT15] Stefan Kölbl, Gregor Leander, and Tyge Tiessen. Observations on the simon block cipher family. In *Annual Cryptology Conference*, pages 161–185. Springer, 2015.

[Köl19] Stefan Kölbl. CryptoSMT an easy to use tool for cryptanalysis of symmetric primitives based on SMT/SAT solvers. available on-line, 2019. https://kste.dk/cryptosmt.html, Last accessed, 5/17/2019.

[LWR16] Yunwen Liu, Qingju Wang, and Vincent Rijmen. Automatic search of linear trails in arx with applications to speck and chaskey. In *International Conference on Applied Cryptography and Network Security*, pages 485–499. Springer, 2016.

[Mat93] Mitsuru Matsui. Linear cryptanalysis method for des cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 386–397. Springer, 1993.

[Nyb94] Kaisa Nyberg. Linear approximation of block ciphers. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 439–444. Springer, 1994.

[SLR+15] Bing Sun, Zhiqiang Liu, Vincent Rijmen, Ruilin Li, Lei Cheng, Qingju Wang, Hoda AlKhzaimi, and Chao Li. Links among impossible differential, integral and zero correlation linear cryptanalysis. In *Advances in Cryptology - CRYPTO 2015 - 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part I*, pages 95–115, 2015.

A Related-key cryptanalysis of CRAFT

Although the designers clearly stated they have no claim of the security against related-key cryptanalysis, however, they presented a key recovery attack based on the related key attack which has the complexity of 2^{124}. Hence, in this section, we more deeply investigate the security of CRAFT against this type of attack to see whether it is possible to reduce the complexity of the key recovery in this adversary model.

To analyze the security of the cipher we searched for a related tweak/key characteristic using the MILP model and CryptoSMT [Köl19], exclude the characteristic provided by the designers. As a result, we came up with many 4-round iterative characteristics that each has only two active S-boxes and its probability is 2^{-4}. The detailed of a characteristic is depicted in Figure 7. Given this characteristic, we can do key recovery efficiently.

Considering a characteristic include 31 rounds, as a distinguisher based on the iterating Figure 7, the last 4 rounds of the cipher will be similar to Figure 8 and the probability of the distinguisher will be 2^{-31}. Hence, by query 2^{31} pairs of P_i and P_i' under related tweaks, such that:

$$P_i \oplus P_i' = \texttt{0F00000000000000}, K_0 \oplus K_0' = \texttt{F0F0000F00F0FF0F},$$

$$K_1 \oplus K_1' = \texttt{F0F0000F00F0FF0F}, T \oplus T' = \texttt{F0F0000F00F0FF0F}$$

we expect to receive a pair of x^{30} and x'^{30} that stratify the 31-round distinguisher. For the correct pair, which satisfies the distinguisher, we expect to have $z^{30} \oplus z'^{30} =$ $\texttt{000000000000000F0}$. On the other hand, it is easy to verify it by checking whether $C_i \oplus C_i' =$ $\texttt{0F00000000000000}$. Given that the probability of satisfying $C_i \oplus C_i'$ for a non-correct pair is 2^{-64}, we expect to detect the correct pair successfully. Given C_i and C_i', we use $z_1^{30} \oplus z_1'^{30}$ as the test point to filter the guessed nibbles of the last round tweak, i.e., TK^{31}. From Figure 9, it can be seen that to determine $z_1^{30} \oplus z_1'^{30}$ we need to guess the values of TK_1^{31}, TK_9^{31} and TK_{13}^{31}. Given those tweak nibbles, we can easily invert the last round and determine whether $z_1^{30} \oplus z_1'^{30} = 0xF$. Based on the DDT of the `CRAFT` S-box, given in table 4, for a wrong guess of tweak nibbles the probability of passing this test will be '2^{-2}' while for the correct guess the probability is '1'. Hence, given 6 correct pairs of C_i and C_i' we expect to determine 12 bits of TK^{31}, i.e., TK_1^{31}, TK_9^{31} and TK_{13}^{31}, uniquely. The Data/Time complexity of this phase of the attack is 6×2^{32} for generating the required C_i and C_i' and 6×2^{12} for filtering the wrong guesses. It is possible to determine other nibbles of TK^{31} using other related key characteristics. For example, using another characteristic and considering the bellow conditions we will be able to determine other nibbles of TK^{31}:

$$P_i \oplus P_i' = \texttt{000000000000000E}, K_0 \oplus K_0' = \texttt{00E000EE0E00E000},$$

$$K_1 \oplus K_1' = \texttt{00EE00E00E00E00E}, T \oplus T' = \texttt{00EE00E00E00E00E}$$

In this case also for a correct pair, which satisfies the distinguisher, we expect to have$z^{30} \oplus z'^{30} =$ $\texttt{E000000000000000}$. On the other hand, it is easy to verify it by checking whether $C_i \oplus C_i' =$ $\texttt{000000000000000E}$. Using this distinguisher, given 6 correct pairs of C_i and C_i' we expect to determine 12 bits of TK^{31}, i.e., TK_0^{31}, TK_8^{31} and TK_{12}^{31}, uniquely. The Data/Time complexity of this phase of attack is also 6×2^{32} for generating required C_i and C_i' and 6×2^{12} for filtering the wrong guesses. Continuing this approach, we can recover nibbles of TK^{31} with the Data/Time complexity of 2^{38}. Given TK^{31}, it is easy to invert the last round and repeat a similar approach to recover TK^{30}. For example, using another characteristic and considering the bellow conditions we will be able to determine three nibbles of TK^{30}:

$$P_i \oplus P_i' = \texttt{6000000000000000}, K_0 \oplus K_0' = \texttt{0000000000000003},$$

$$K_1 \oplus K_1' = \texttt{0000000000000000}, T \oplus T' = \texttt{00EE00E00E00E00E}$$

Here also, for a correct pair which satisfies the distinguisher, we expect to have $z^{29} \oplus z'^{29} =$ $\texttt{6000000000000000}$. On the other hand, it is easy to verify it by checking whether $C_i \oplus C_i' =$ $\texttt{6000000000000000}$. Using this distinguisher, given 6 correct pairs of C_i and C_i' we expect to determine 12 bits of TK^{30}, i.e., TK_0^{30}, TK_8^{30} and TK_{12}^{30}, uniquely. The Data/Time complexity of this phase of attack is also 6×2^{32} for generating required C_i and C_i' and 6×2^{12} for filtering the wrong guesses. We repeat this approach to recover other nibbles TK^{30} also. Based on this approach the Data/Time complexity of recovery whole TK^{31} and TK^{30} is bellow 2^{40} while the memory is negligible. Given those tweaks and also values of T that are used for any pair, it is easy to determine K_0 and K_1.

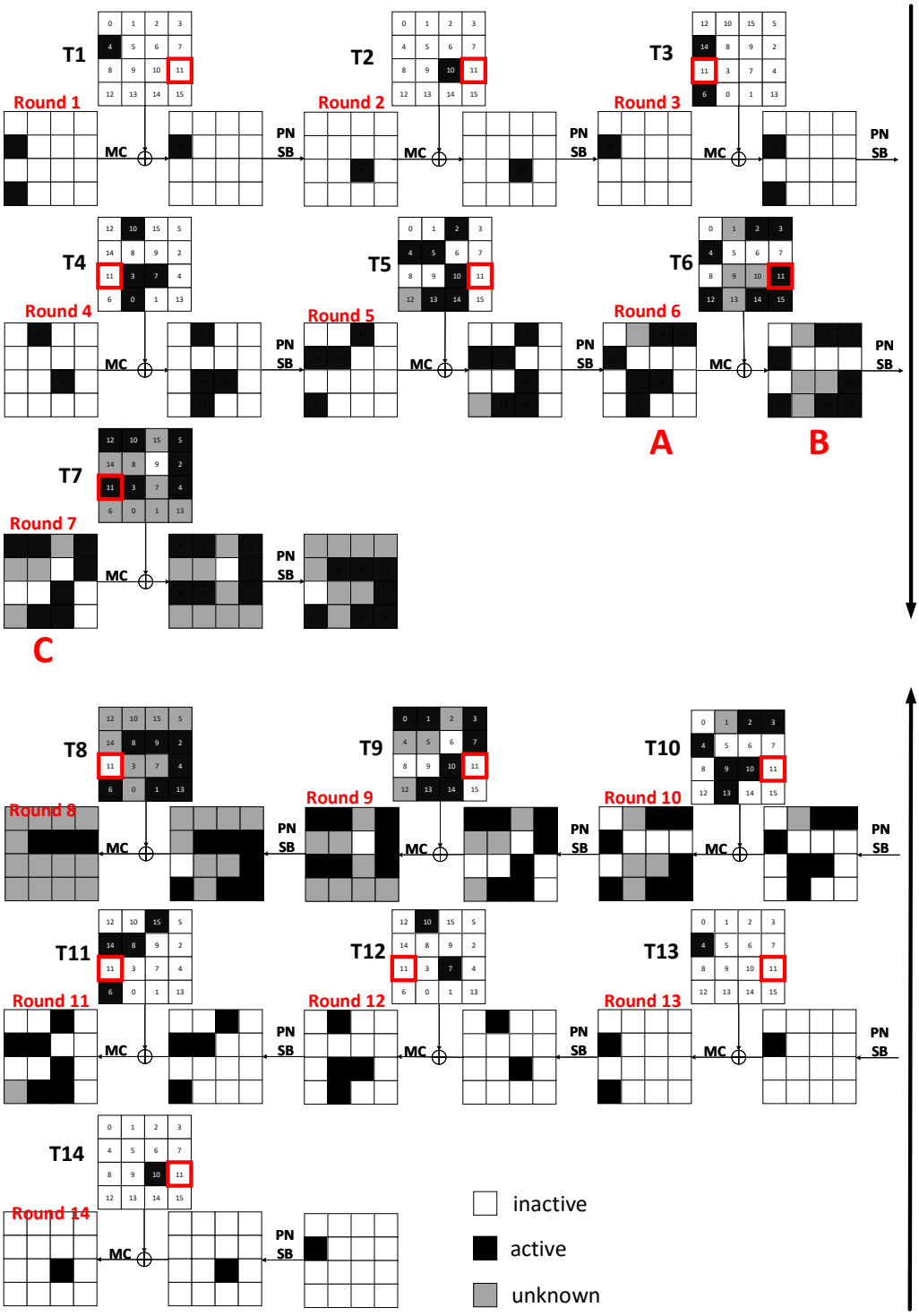
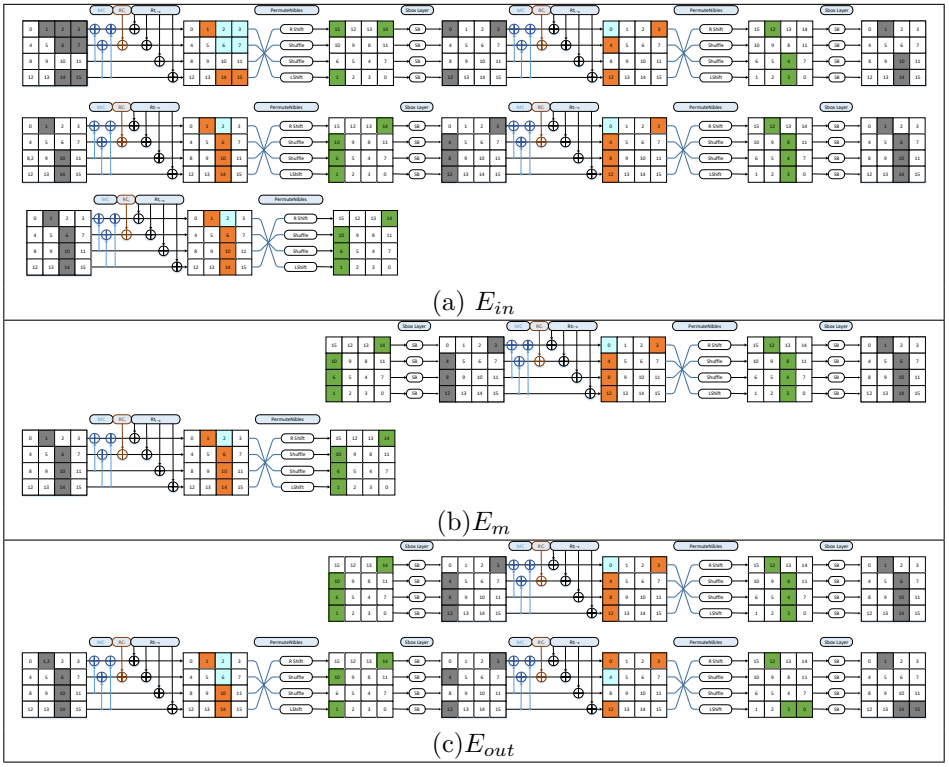


Figure 2: Related tweak zero correlation of 14-round CRAFT

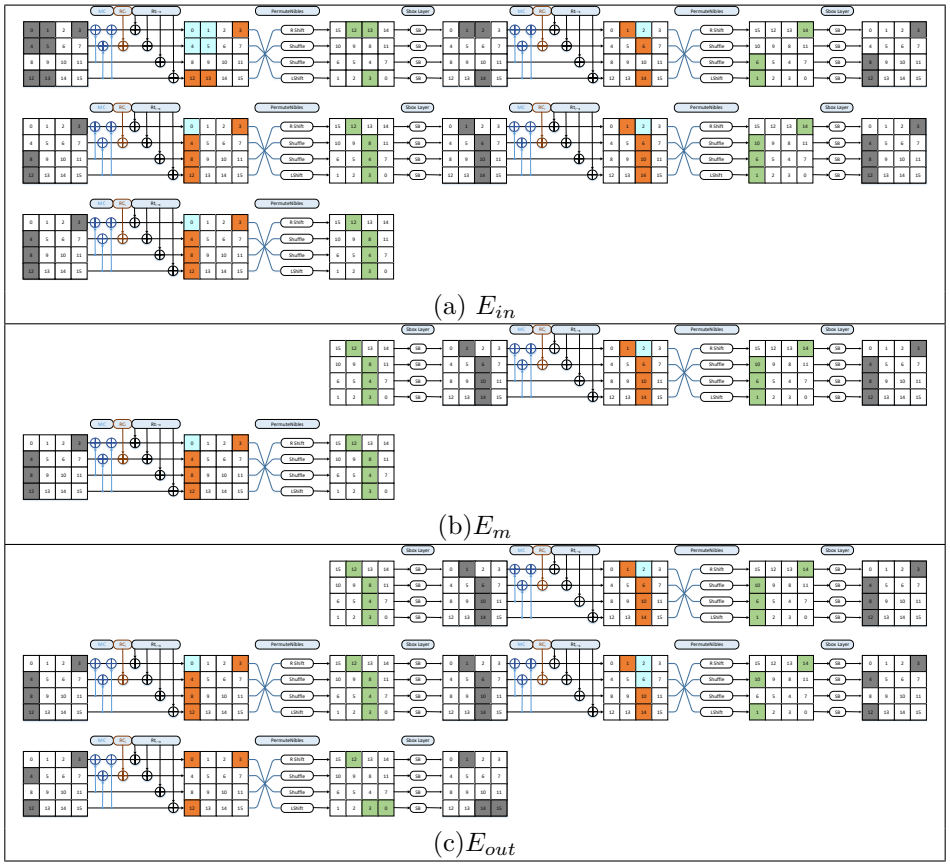


(a) E_{in}

(b)E_m

(c)E_{out}

Figure 3: An expendable truncated characteristic for even rounds, where E_{in} and E_{out}denotes the first 4 and the last 4 rounds respectively and E_m is a repeatable 2-round truncated characteristic that can be used as much as required. For example, to design a 10 round characteristic this stage is repeated once and, the current characteristic. The Cyan-colored cells are inactive due to cancellation after `MC` step, white-colored cells are inactive, and {Gray, Orange, Green} colors are active cells in different stage of the cipher.



(a) E_{in}

(b)E_m

(c)E_{out}

Figure 4: An expendable truncated characteristic for odd rounds, where E_{in} and E_{out}denotes the first 4 and the last 5 rounds respectively and E_m is a repeatable 2-round truncated characteristic that can be used as much as required. For example, to design a 9 round characteristic this stage is omitted.

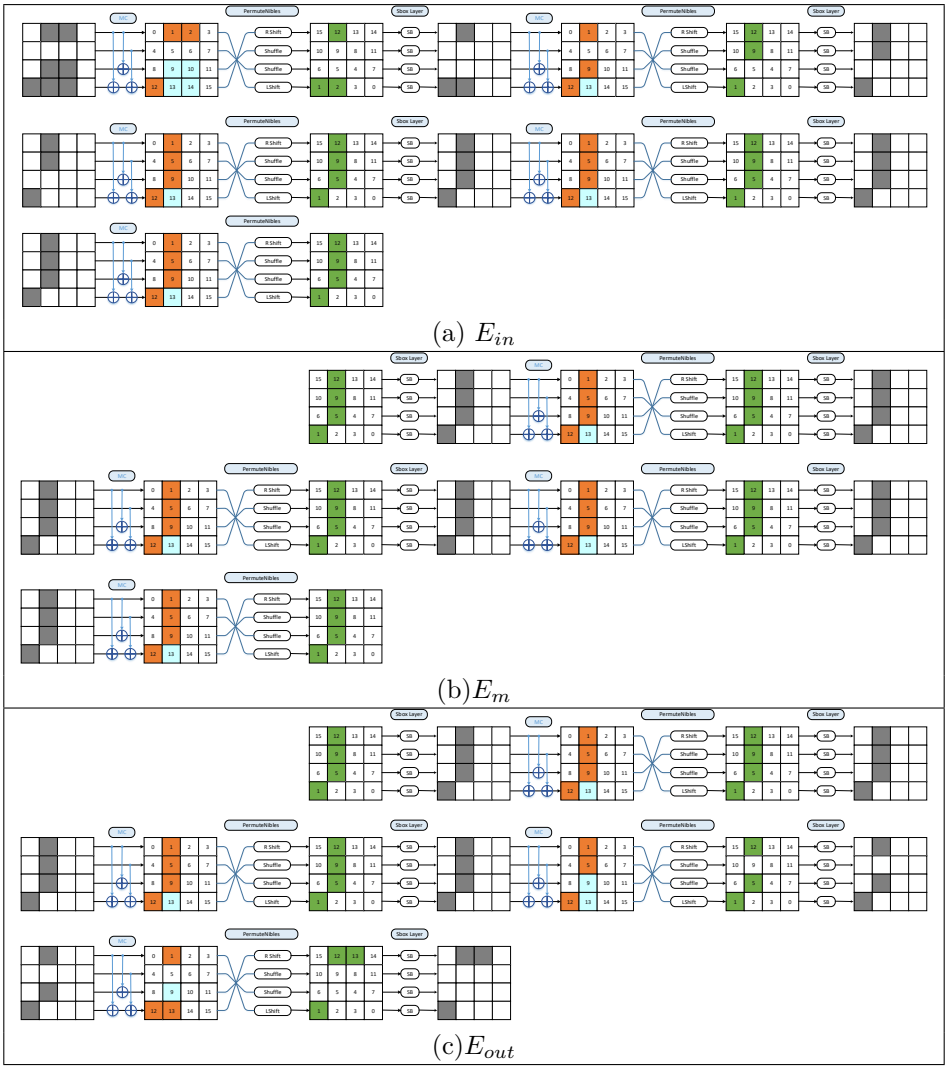


Figure 5: An expendable truncated linear characteristic for 13 rounds of `CRAFT`, where E_{in} and E_{out} denotes the first 4 and the last 5 rounds respectively and E_m is the middle 4-round truncated characteristic.

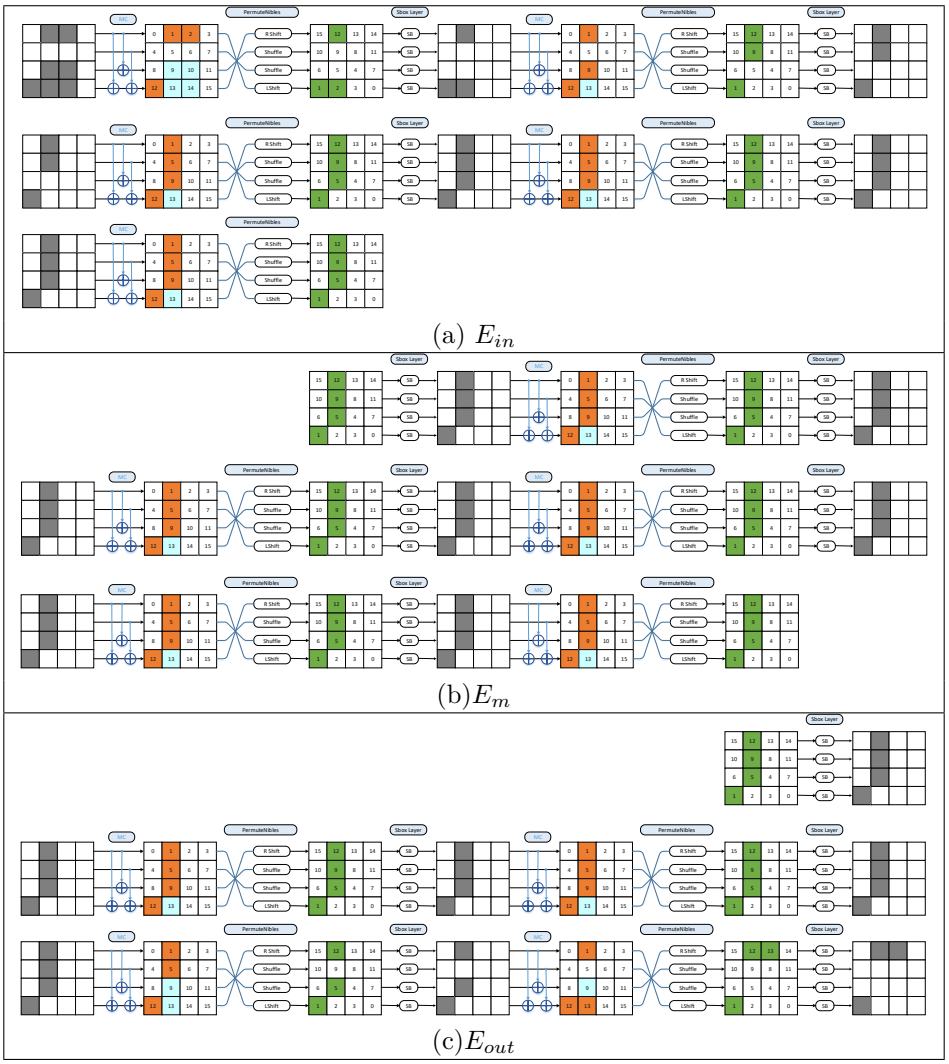


Figure 6: An expendable truncated linear characteristic for 14 rounds of `CRAFT`, where E_{in} and E_{out} denote the first 4 and the last 5 rounds respectively and E_m is a 5-round truncated linear characteristic.

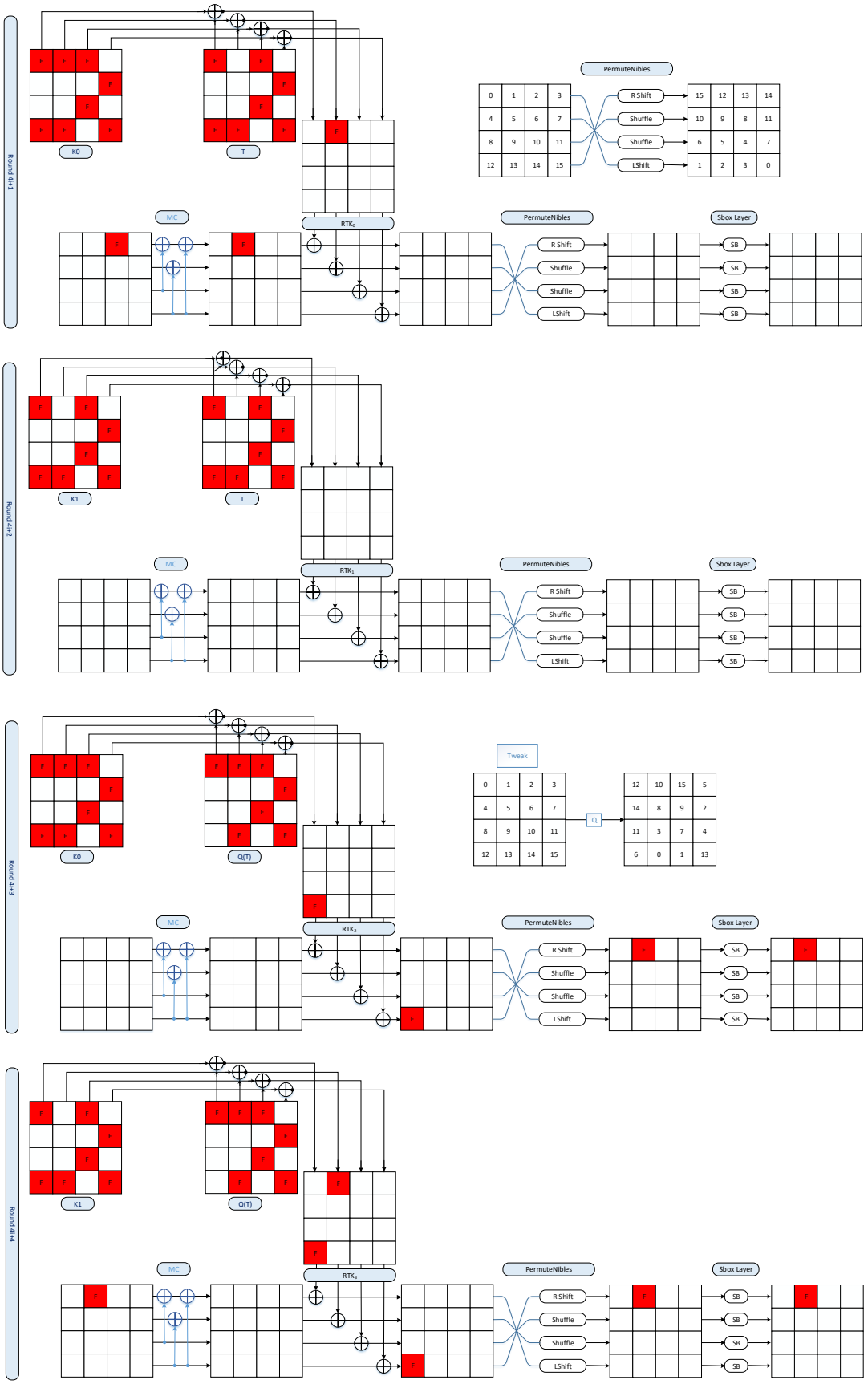


Figure 7: A 4-round iterative Related-Tweakey differential characteristic for `CRAFT`

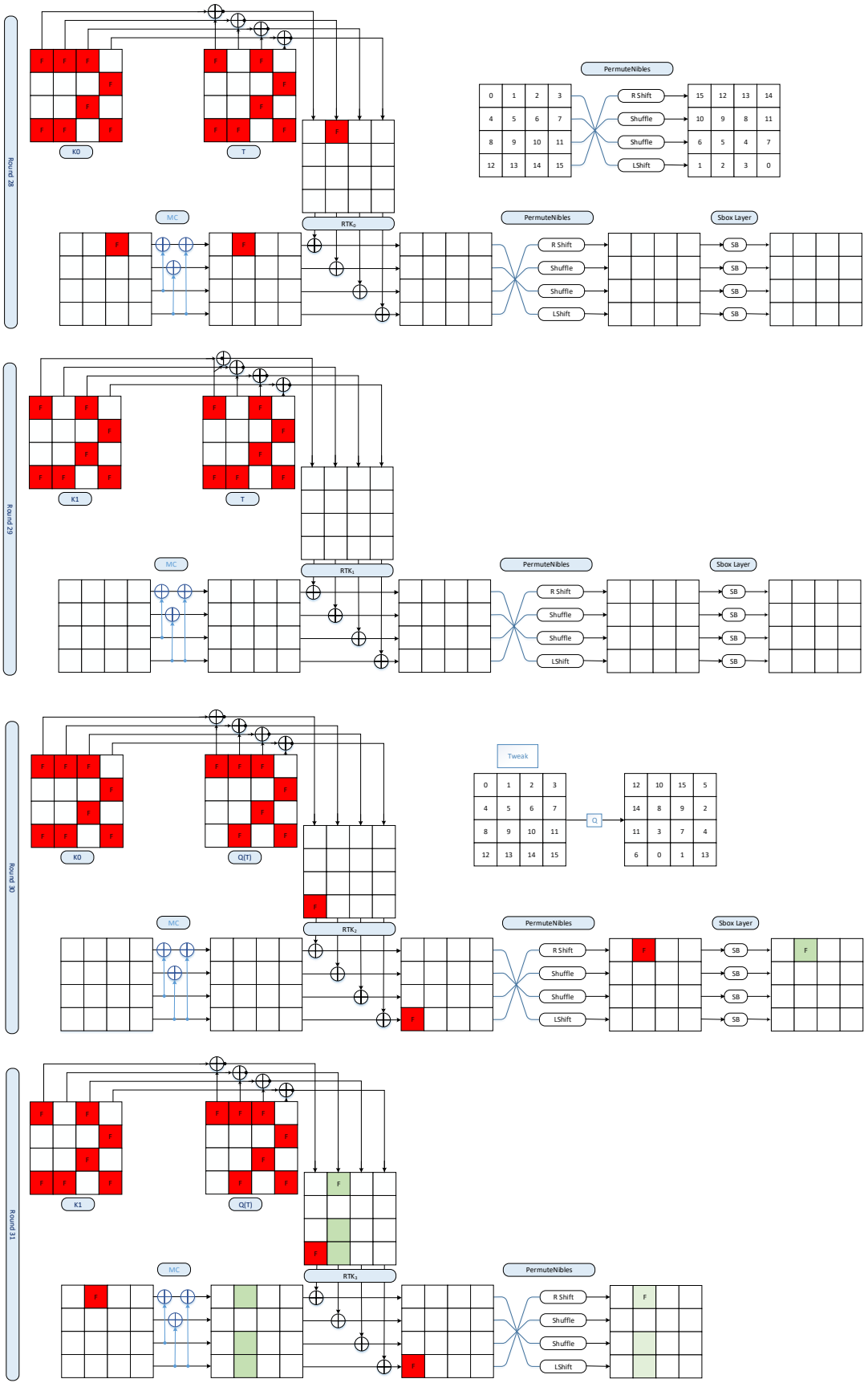


Figure 8: The distinguisher which is used to recover 3 nibbles of the last key. The recovered key's nibbles are highlighted in Green.

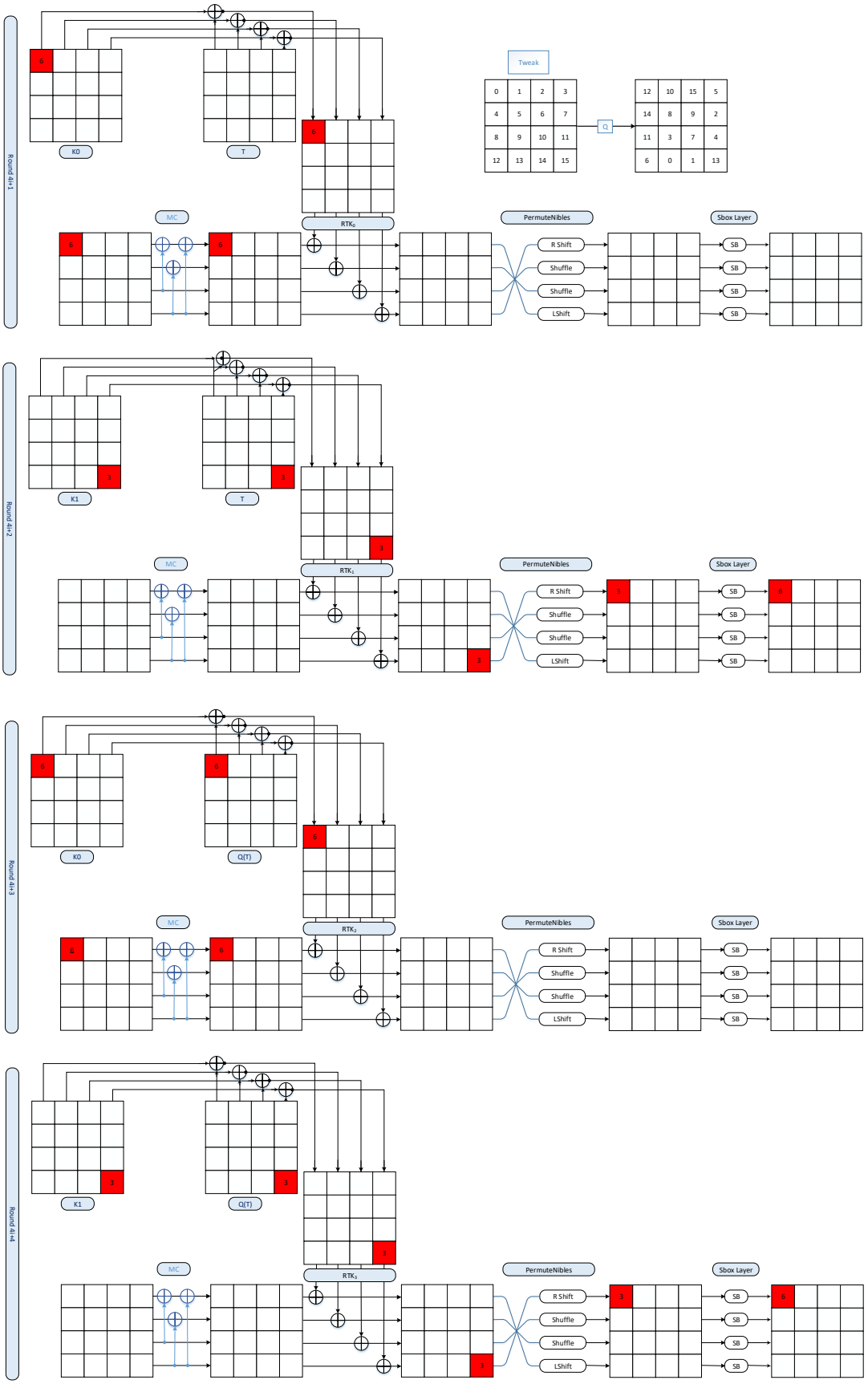


Figure 9: A 4-round iterative Related-Tweakey differential characteristic for `CRAFT`, which is used to recover 3 nibbles of TK^{30}.