Comprehensive security analysis of CRAFT

Hosein Hadipour, Sadegh Sadeghi, Majid M. Niknam, and Nasour Bagheri

1 Department of Mathematics and Computer Science, University of Tehran, Tehran, Iran, hsn.hadipour@gmail.com
2 Department of Mathematics, Faculty of Mathematical Sciences and Computer, Kharazmi University, Tehran, Iran, s.sadeghi.khu@gmail.com
3 LIMOS, University Clermont Auvergne, France
4 Electrical Engineering Department, Shahid Rajaee Teacher Training University, Tehran, Iran, nabgheri@srut.ac.ir
5 School of Computer Science (SCS), Institute for Research in Fundamental Sciences (IPM), Tehran, Iran

Abstract. CRAFT is a lightweight block cipher, designed to provide efficient protection against differential fault attacks. It is a tweakable cipher that includes 32 rounds to produce a ciphertext from 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 and zero-correlation cryptanalysis, aiming to provide better distinguishers for the reduced rounds of the cipher. Our distinguishers for reduced-round CRAFT cover a higher number of rounds compared to the designers' analysis. In our analysis, we observed that, for any number of rounds, the differential effect of CRAFT has an extremely higher probability compared to any differential trail. As an example, while the best trail for 11 rounds of the cipher has a probability of at least $2^{-80}$, we present a differential with probability $2^{-49.79}$, containing $2^{29.66}$ optimal trails, all with the same optimum probability of $2^{-80}$. Next, we use a partitioning technique, based on optimal expandable truncated trails to provide a better estimation of the differential effect on CRAFT. Thanks to this technique, we are able to find differential distinguishers for 9, 10, 11, 12, 13, and 14 rounds of the cipher in single tweak model with the probabilities of at least $2^{-40.20}$, $2^{-45.12}$, $2^{-49.79}$, $2^{-54.49}$, $2^{-59.13}$, and $2^{-63.80}$, 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 at least $2^{-54.67}$ and $2^{-62.61}$, respectively. In addition, we consider 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. Thanks to the related tweak ZC distinguisher for 14 rounds of the cipher, we also present 14 rounds integral distinguishers in related tweak mode of the cipher. Although the provided analysis does not compromise the cipher, we think it provides a better insight into the designing of CRAFT.

Keywords: Lightweight block cipher · differential · zero-correlation · tweakable cipher · MILP · SAT · 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 have been proposed by 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 second-round candidates. Among lightweight primitives, (tweakable) block ciphers received more attention and many nice designs have already been proposed, each of which targets different applications.

On the other hand, Side-Channel Analysis (SCA) attacks, such as power/time analysis and fault analysis, target 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 have aimed to provide efficient protection against SCA from design. More precisely, they selected a component to design cipher such that they can provide efficient protection against a specific attack, e.g., LS-Designs [GLSV14], FRIT [SBD+18], 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 (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). 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 still room for third-party analysis. In addition, related tweak zero-correlation [ADG+19] is a new concept which has been proposed after the publication of CRAFT, hence, the security of the cipher against this attack is worth an investigation. Moreover, due to the nature of differential cryptanalysis, which requires to search over a very large space of all possible trails, 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 analyses. The paper’s contribution is summarized as follows (also, Table 1 shows a comparison of our results with previous ones for CRAFT):

1. We present 14 rounds zero-correlation distinguishers for the cipher in the related tweak mode. It should be compared with the 13-round distinguisher proposed by the designers, however, in the single tweak mode.

2. Given the related tweak ZC distinguisher for 14 rounds of the cipher and following the connection between zero-correlation and integral distinguisher [SLR+15], we also present 14 rounds integral distinguishers in the related tweak mode of the cipher.

3. Thanks to the advanced automated search models based on CryptoSMT [Köl19] and MILP [MWGP11, SHW+14b, SHW+14a], we are able to improve the designers’ lower bounds for differential cryptanalysis. More precisely, while the designers’ lower bound on the probability of differential for 9 and 10 rounds of the cipher are least $2^{-54.67}$ and $2^{-62.61}$, respectively, we are able to present $9, 10, 11, 12, 13$, and $14$ rounds of the differential in single-tweak model with the probabilities of at least $2^{-49.20}, 2^{-44.89}, 2^{-49.79}, 2^{-54.48}, 2^{-59.13}$, and $2^{-63.80}$, respectively, that improve the previous lower bounds significantly. We make our implementations of the attacks and our modeling of algorithms in MILP and SAT freely available at: https://github.com/hadipourh/craftanalysis.

4. We also show some typos in the designers’ analysis which could be useful for later studies. For example, we show that two out of 12 zero-correlation masks for 13 rounds of CRAFT, that are provided by the designers, are not valid. We also provide exact trails, with non zero-correlation, for those masks. A similar result is also presented for their proposed impossible differential trails.
Table 1: Summary of the main results of attacks on CRAFT. Where ST, RT and RK denotes single tweak mode, related tweak mode and related key mode respectively and RT<sub>i</sub> denotes RT mode that is started with TK<sub>i</sub>. In addition, D, TD, LH, ID, INT and ZC denote differential effect, truncated differential, linear hull, impossible differential, integral, and zero-correlation cryptanalysis, respectively. For example, RT<sub>0</sub>-D denotes differential effect of CRAFT in related tweak mode, starting with TK<sub>0</sub>.

<table>
<thead>
<tr>
<th>Attack</th>
<th># Rounds</th>
<th>Probability</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST-D</td>
<td>10</td>
<td>2&lt;sup&gt;-62.61&lt;/sup&gt;</td>
<td>[BLMR19]</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>2&lt;sup&gt;-41.89&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>2&lt;sup&gt;-49.79&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>2&lt;sup&gt;-54.48&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>2&lt;sup&gt;-59.13&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>2&lt;sup&gt;-63.80&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>ST-TD</td>
<td>12</td>
<td>2&lt;sup&gt;-36&lt;/sup&gt;</td>
<td>[MA19]</td>
</tr>
<tr>
<td>ST-LH</td>
<td>14</td>
<td>2&lt;sup&gt;-62.13&lt;/sup&gt;</td>
<td>[BLMR19]</td>
</tr>
<tr>
<td>RT&lt;sub&gt;0&lt;/sub&gt;-D</td>
<td>15</td>
<td>2&lt;sup&gt;-65.14&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>RT&lt;sub&gt;1&lt;/sub&gt;-D</td>
<td>16</td>
<td>2&lt;sup&gt;-57.18&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>RT&lt;sub&gt;2&lt;/sub&gt;-D</td>
<td>17</td>
<td>2&lt;sup&gt;-60.14&lt;/sup&gt;</td>
<td>[BLMR19]</td>
</tr>
<tr>
<td>RT&lt;sub&gt;3&lt;/sub&gt;-D</td>
<td>16</td>
<td>2&lt;sup&gt;-55.14&lt;/sup&gt;</td>
<td></td>
</tr>
<tr>
<td>ST-ID</td>
<td>13</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>ST-INT</td>
<td>13</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>ST-ZC</td>
<td>13</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>RT-ZC</td>
<td>14</td>
<td>-</td>
<td>this paper</td>
</tr>
<tr>
<td>RT-INT</td>
<td>14</td>
<td>-</td>
<td>this paper</td>
</tr>
<tr>
<td>RK-D</td>
<td>32</td>
<td>2&lt;sup&gt;-32&lt;/sup&gt;</td>
<td>[EY19]</td>
</tr>
</tbody>
</table>
The rest of the paper is organized as follows: in Section 2, we present the required preliminaries and also briefly describe CRAFT. In Section 3, we present the zero-correlation analysis in related tweak mode. Differential effect analysis of the cipher is described in Section 4. Section 5 presents our investigation results on some of the designers security claims and points out some of their typos. Finally, we conclude the paper in Section 6.

2 Preliminaries

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

2.1 Notations

The notation used in the paper is summarized in Table 2.

2.2 A brief description of CRAFT

CRAFT is a 64-bit lightweight block cipher which supports 128-bit key and 64-bit tweak and its round function is composed of involutory building blocks. It takes a 64-bit plaintext \(m = m_0 \parallel m_1 \parallel \cdots \parallel m_{14} \parallel m_{15}\) to initiate a \(4 \times 4\) internal state \(IS = I_0 \parallel I_1 \parallel \cdots \parallel I_{14} \parallel I_{15}\) as follows, where \(I_i, m_i \in \mathbb{F}_2^4\):

\[
IS = \begin{pmatrix}
I_0 & I_1 & I_2 & I_3 \\
I_4 & I_5 & I_6 & I_7 \\
I_8 & I_9 & I_{10} & I_{11} \\
I_{12} & I_{13} & I_{14} & I_{15}
\end{pmatrix} = 
\begin{pmatrix}
m_0 & m_1 & m_2 & m_3 \\
m_4 & m_5 & m_6 & m_7 \\
m_8 & m_9 & m_{10} & m_{11} \\
m_{12} & m_{13} & m_{14} & m_{15}
\end{pmatrix}
\]
Those LFSRs are initialized by values (0001) and (001), respectively and are updated to with round constant AddRoundConstants (ATK). A 4-bit LFSR and a 3-bit LFSR are used to update the substitution layer S-box (SB), and the substitution layer S-box (SB) includes five functions, i.e., a binary MixColumn (MC), the round dependent combining with the sub-tweak key 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., \( R_{31} = ATK_{31} \circ ARC_{31} \circ MC \), while for any \( 0 \leq i \leq 30 \), \( R_i = SB \circ PN \circ ATK_i \circ ARC_i \circ MC \).

\( MC \) is a multiplication of internal state by the following binary matrix:

\[
MC = \begin{pmatrix}
1 & 0 & 1 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1
\end{pmatrix}
\]

Then, the internal state is going through 32 rounds \( R_i, i \in \{0, \ldots, 31\} \), to generate a 64-bit ciphertext. As is depicted in Figure 1, each round, excluding the last round, includes five functions, i.e., a binary MixColumn (MC), the round dependent combining with the sub-tweak key 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., \( R_{31} = ATK_{31} \circ ARC_{31} \circ MC \), while for any \( 0 \leq i \leq 30 \), \( R_i = SB \circ PN \circ ATK_i \circ ARC_i \circ MC \).

\( MC \) 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 \( a_i = (a_i^1, a_i^2, a_i^3, a_i^4) \) and \( b_i = (b_i^0, b_i^1, b_i^2, b_i^3) \) are XOR-ed with \( I_4 \) and \( I_5 \) respectively (\( a_i^0 \) and \( b_i^0 \) 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 LFSRs are initialized by values (0001) and (001), respectively and are updated to \( a_{i+1} = (a_i^1 \oplus a_i^0, a_i^2, a_i^0, a_i^1) \) and \( b_{i+1} = (b_i^1 \oplus b_i^0, b_i^2, b_i^1) \) from \( i \)-th round to \( i+1 \)-th round.

After AddRoundConstants (ARC), a 64-bit round tweak key is XOR-ed with IS. The tweak key schedule of \( CRAFT \) is rather simple. Given the secret key \( K = K_0 \parallel K_1 \) and the tweak \( T \in \{0, 1\}^{64} \), where \( K_i \in \{0, 1\}^{64} \), four round tweak keys \( TK_0 = K_0 \oplus T \), \( TK_1 = K_1 \oplus T \), \( TK_2 = K_0 \oplus Q(T) \) and \( TK_3 = K_1 \oplus Q(T) \) are generated, where given \( T = T_0 \parallel T_1 \parallel \cdots \parallel T_{14} \parallel T_{15} \) (\( Q(T) = T_{12} || T_{10} || T_{15} || T_5 || T_4 || T_8 || T_2 || T_11 || T_7 || T_4 || T_0 || T_0 || T_1 || T_{13} \)). Then at the round \( R_i \), \( TK_{i,64} \) is XOR-ed with the IS, where the rounds start from \( i = 0 \).

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

The final function is a non-linear \( 4 \times 4 \)-bit S-box which has been borrowed from MID OR [BBI+15]. The table representation of the S-box is given in Table 3.

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>a</th>
<th>b</th>
<th>c</th>
<th>d</th>
<th>e</th>
<th>f</th>
</tr>
</thead>
<tbody>
<tr>
<td>S(x)</td>
<td>c</td>
<td>a</td>
<td>d</td>
<td>3</td>
<td>e</td>
<td>b</td>
<td>f</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>1</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
</tbody>
</table>

Table 3: The S-box used in CRAFT in hexadecimal form.

Figure 1: A round of CRAFT.
In this section, we apply the related tweak zero-correlation attack [ADG+19] to a reduced-round version of CRAFT. In the zero-correlation cryptanalysis of a tweakable block cipher $E_K(P, T)$, e.g., CRAFT, tweak bits can also be involved into the linear combination of input bits. Hence, in this case, when one looks for a linear hull with zero correlation, input mask consists of two components, one for plaintext, and another one for (master)-tweak. The correlation of a linear approximation with input mask $(\alpha_1, \alpha_2)$, and output mask $\beta$, is calculated as follows:

$$corr((\alpha_1, \alpha_2), \beta) = 2 \Pr (\langle \alpha_1, P \rangle \oplus \langle \alpha_2, T \rangle \oplus \langle \beta, E_K(P, T) \rangle = 0) - 1,$$

where the probability is taken over all values of $P$, and $T$.

CRAFT has a linear twekey-scheduling $L_K : \mathbb{F}_2^{64} \rightarrow (\mathbb{F}_2^{32})^r$, to map the tweak to the sub-tweakeys. The generated sub-tweakeys are then XORed to the internal states of the cipher as depicted in Figure 2. For a linear trail with input-output masks $((\alpha_1, \alpha_2), \beta)$, and internal linear masks $\Gamma = (\Gamma X^0, \Gamma Y^0, \Gamma Z^0, \Gamma X^1, \Gamma Y^1, \Gamma Z^1, \ldots, \Gamma X^{r-1}, \Gamma Y^{r-1}, \Gamma Z^{r-1}, \Gamma X^r)$, covering $r$ rounds of CRAFT, correlation can be calculated as follows:

$$C_\Gamma = \prod_{i=0}^{r-1} corr((\Gamma X^i, \Gamma TK_i^{i \% 4}), \Gamma X^{i+1}).$$

According to the rule of propagation of linear masks through XOR, linear mask $\Gamma Y^i$ must be the same as the linear mask $\Gamma TK^{i \% 4}_{i \% 4}$, for all $0 \leq i \leq r - 1$. According to the twekey-scheduling of CRAFT, which is a linear mapping, the linear masks $\Gamma Y^i$, for all $0 \leq i \leq r - 1$, should satisfy the following relation:

$$\alpha_2 = \mathcal{L}(\Gamma Y^0, \ldots, \Gamma Y^{r-1}) := \bigoplus_{i=0, \ i \% 4 < 2}^{r-1} \Gamma Y^i \oplus \bigoplus_{i=0, \ i \% 4 \geq 2}^{r-1} Q^{-1}(\Gamma Y^i).$$

In other words, there is a linear relation between nibbles of linear masks $\Gamma Y^i$, for $0 \leq i \leq r - 1$, as follows:

$$\alpha_2[j] = \bigoplus_{i=0, \ i \% 4 < 2}^{r-1} \Gamma Y^i[j] \oplus \bigoplus_{i=0, \ i \% 4 \geq 2}^{r-1} \Gamma Y^i[Q^{-1}(j)], \text{ for all } 0 \leq j \leq 15.$$
The correlation of a linear hull, with the input linear masks \((\alpha_1, \alpha_2)\) and the output linear mask \(\beta\), can be calculated as follows:

\[
corr((\alpha_1, \alpha_2), \beta) = \sum_{\Gamma X^0 = \alpha_1, \Gamma X^r = \beta, (\Gamma X^3, \ldots, \Gamma X^{r-1}) \in (F_2, r-1)} C_\Gamma.
\]

The additional constraint \(\alpha_2 = \mathcal{L}(\Gamma Y^0, \ldots, \Gamma Y^{r-1})\), which is induced by the tweakey-scheduling, introduces additional restriction on linear trails that are included in a linear hull. Hence, the probability of achieving a zero-correlation is higher than the single tweak zero-correlation cryptanalysis, where the tweakey-scheduling is not considered.

In the related tweak cases, the zero-correlation linear hull behavior of CRAFT is dependent on the starting round, i.e., the index of \(RT_i\), \((i = 0, 1, 2, 3)\). Hence, we investigated the security of CRAFT against the related tweak zero-correlation attack in \(RT_0, RT_1, RT_2\) and \(RT_3\) modes. To find the related tweak zero-correlation trails, we modeled CRAFT in MILP to find a zero-correlation mask for \(RT_i\) and proved it manually. As a result, in the case of \(RT_0\), we found a 14-round zero-correlation linear hull for CRAFT, where the number of forward and backward rounds are both 7. With respect to Figure 3, active linear masks are applied to two cells \(X^0[4]\) and \(X^0[12]\) at the input, and the active linear mask is applied to cell \(X^{14}[4]\) in the state at the output. Then, we focus on the tweak cell labeled 11, where it is depicted by using a red frame in Figure 3. In the following section, based on the given active linear mask in the master tweak \(T\), we present a 14-round related tweak zero-correlation for CRAFT:

\[
\Gamma T = \bigoplus_{i=0}^{r-1} \Gamma TK^i_3 \oplus \bigoplus_{i=0}^{r-1} Q^{-1} (\Gamma TK^i_3) = \begin{pmatrix}
* & * & * & * \\
* & * & * & 8 \\
* & * & * & * \\
* & * & * & *
\end{pmatrix}.
\]

Note that the permutation \(Q\) operated on \(TK^i_3\), when \(i = 2, 3, 6, 7, 10, 11\). Based on Figure 3, we have \(\Gamma T[11] = \Gamma TK^1_3 [11] \oplus \Gamma TK^6_3 [8]\) (the XOR of red frames) and so,

\[
\Gamma TK^1_3 [11] \oplus \Gamma TK^6_3 [8] = 8. \tag{1}
\]

We denote the Linear Approximation Table of CRAFT S-box by \(LAT\) and \(LAT[i][j]\) is the element of \(i\)-th row and \(j\)-th column of it and \(LAT[i]\) is defined as the set \(LAT[i] = \{ j \in F_2^3 | LAT[i][j] \neq 0 \}\) (see Table 4). Now, based on the properties of \(PN\) and \(SB\) operations of 5-th round, we have

\[
\Gamma X^6[0] \in LAT[\Gamma Y^5[15]], \tag{2}
\]

Due to the \(MC\) operation on the active cells of column 3 of state \(X^5\) in the input of 5-th round, we have

\[
\]

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

\[
\Gamma X^6[0] \in LAT[\Gamma Y^5[11]] = LAT[\Gamma TK^1_3[11]]. \tag{3}
\]

Now, due to the \(MC\) operation on the active cells of column 0 of state \(X^6\), we have

\[
\Gamma TK^6_3[8] = \Gamma X^6[0] \in LAT[\Gamma TK^6_3[11]]. \tag{4}
\]
Figure 3: Related tweak zero-correlation of 14-round CRAFT in $TK_0$ mode
Therefore, based on (Equation 1) and (Equation 4), $\Gamma_{TK}^{[11]}$ and $\Gamma_{TK}^{[8]}$ must satisfy the following conditions:

\[
\begin{align*}
\Gamma_{TK}^{[11]} \oplus \Gamma_{TK}^{[8]} &= 8, \\
\Gamma_{TK}^{[8]} &\in \text{LAT}[\Gamma_{TK}^{[11]}].
\end{align*}
\]

These conditions are equivalent to finding an input mask $x (x = \Gamma_{TK}^{[11]})$ and an output mask $y (y = \Gamma_{TK}^{[8]})$, such that:

\[
\begin{align*}
x \oplus y &= 8, \\
\text{LAT}[x][y] &\neq 0.
\end{align*}
\]

Note that, by referring to linear approximation table of CRAFT S-box, we observe there is no input/output mask that satisfies these conditions (see Table 4).

Table 4: Linear approximation table of CRAFT S-box.

<table>
<thead>
<tr>
<th>$x$/$y$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>-2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>-2</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>-4</td>
<td>-2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>-2</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>-2</td>
<td>-4</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>-4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>-4</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>-2</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>-2</td>
<td>0</td>
<td>2</td>
<td>-4</td>
<td>-2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>-2</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>-4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>0</td>
<td>0</td>
<td>-4</td>
<td>0</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>-2</td>
<td>2</td>
<td>-2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-2</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>-4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>-2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>-2</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

We also searched the zero-correlation linear hulls for each cases $RT_1$, $RT_2$, and $RT_3$. For $RT_1$, we could not find a zero-correlation linear hull covering more than 13 rounds, but for both $RT_2$, and $RT_3$, we found new zero-correlation linear hulls covering 14 rounds of CRAFT.

The activity patterns of linear masks, for the obtained zero-correlation linear hulls in cases $RT_2$, and $RT_3$ are as follows:

\[
\begin{align*}
0000 &\gamma 000 0000 0000 14\text{-round-}RT_2 \rightarrow 0000 0\delta 00 0000 0000, \\
0000 &0\gamma 00 0000 0000 14\text{-round-}RT_3 \rightarrow 0000 \delta 000 0000 0000.
\end{align*}
\]

where in both cases, $\gamma T = **** ***** **** 0 ****$, and $\gamma$, and $\delta$ are non-zero elements in $F_2^4$.

### 3.1 Linking zero-correlation linear hull to integral

The following theorems show how to convert a zero-correlation linear hull to an integral distinguisher.

**Theorem 1.** [SLR$^{+15}$] Let $F : F_2^n \rightarrow F_2^n$ be a function, and $A$ be a subspace of $F_2^n$ and $\beta \in F_2 \setminus \{0\}$. Suppose that $(\alpha, \beta)$ is a zero-correlation linear approximation for any $\alpha \in A$, then for any $\lambda \in F_2^n$, $(\beta, F(x + \lambda))$ is balanced on the following set

\[
A^\perp = \{x \in F_2^n | (\alpha, x) = 0, \alpha \in A\}.
\]
The following theorem shows that the input masks should not necessarily form a subspace.

**Theorem 2.** [SLR\(^{+}\)15] A nontrivial zero-correlation linear hull of a block cipher always implies the existence of an integral distinguisher.

The number of the required data to verify whether \(\langle \beta, F(x + \lambda) \rangle\) in Theorem 1, and Theorem 2, is balanced over \(A^\perp\), is equal to the cardinality of \(A^\perp\) which is \(2^{\text{dim}(A^\perp)}\). Therefore, if the input-size of \(F\) is \(n\) bits, and the dimension of the subspace \(A\) is \(m\), the data complexity of the corresponding integral distinguisher is \(2^{n-m}\). Considering the tweak in the zero-correlation linear hull on a general tweakable block cipher may expand the domain space form \(n\) to \(n + t\), when \(n\), and \(t\), are data-size and tweak-size respectively [ADG\(^{+}\)19], but considering tweak in our related-tweak zero-correlation linear hulls for CRAFT increases the domain space \(n\) only by 4.

The CRAFT's tweak scheduling algorithm never mixes the different nibbles, and as mentioned above, the tweak, excluding the nibble \(T[11]\), is independent of the obtained linear hull in our zero-correlation linear hulls for all cases \(RT_0, RT_2,\) and \(RT_3\), and it actually can take any (arbitrary) constants. Therefore, the domain space of our zero-correlation linear hulls is \(64 + 4 = 68\) bits instead of \(128\) bits. In other words, to evaluate the correlation of the obtained linear hull in the online phase, an arbitrary constant is taken for those nibbles labeled by \(\ast\), and the inputs are chosen so that the vector consisting of 17 remaining nibbles, take all the possible values, since the correlation of our linear hulls is equal to zero, independent of those nibble labeled by \(\ast\).

Suppose that we denote the 14 rounds of CRAFT starting with \(RT_0\), as follows:

\[
E_K : \mathbb{F}_2^{64} \times \mathbb{F}_2^{64} \rightarrow \mathbb{F}_2^{64}
\]

\[
(P, T) \mapsto E_K(P, T),
\]

where \(P\) and \(T\) denote plaintext and tweak, respectively. We also denote the function obtained by fixing 15 nibbles of tweak, excluding the cell 11, by an arbitrary value from \(\mathbb{F}_2^{60}\) in function \(E_k\) by \(F\), which is actually a function from \(\mathbb{F}_2^{64} \times \mathbb{F}_2^{4}\) to \(\mathbb{F}_2^{64}\). Let \(M\) be the set of all input masks in our zero-correlation linear hull in case \(RT_0\), as follows:

\[
M := \{(\gamma_0, \ldots, \gamma_{15}, \gamma) \in (\mathbb{F}_2^4)^{17} | \gamma_{12} \neq 0, \gamma = 8, \gamma_i = 0 \text{ for all } i \neq 4, 12\},
\]

where \((\gamma_0, \ldots, \gamma_{15})\) corresponds to input mask for plaintext, and \(\gamma\) corresponds to the input mask for \(T[11]\). Although, \(M\) is not a subspace of \(\mathbb{F}_2^{68}\), for each \(\alpha = (\gamma_0, \ldots, \gamma_{15}, \gamma) \in M\), if \(A = \{0, \alpha\}\), then \(A\) is a subspace of dimension 1 of \(\mathbb{F}_2^{68}\). Suppose that \(\beta\) is chosen from the set of all output masks of our zero-correlation linear hull for 14 rounds of CRAFT in case \(RT_0\) which is depicted in Figure 3. Thus, based on Theorem 1, for each \(\lambda \in \mathbb{F}_2^{68}\), \(\langle \beta, F(x + \lambda) \rangle\) is balanced over \(A^\perp\). Since \(\text{dim}(A^\perp) = 67\), the data complexity of the integral distinguisher corresponding to the zero-correlation linear hull covering 14 rounds, in case \(RT_0\) is equal to \(2^{67}\). For more details, \(A, A^\perp\) can be displayed as follows:

\[
A = \{0, 0, \ldots, 0, c_4, 0, \ldots, 0, c_{12}, 0, 0, 0, 8\},
\]

where \(c_4 = c_{12}\) are non-zero constants from \(\mathbb{F}_2^4\), and,

\[
A^\perp = \{(x_0, \ldots, x_{15}, t_{11}) \in (\mathbb{F}_2^4)^{17} | \langle c_4, x_4 \rangle \oplus \langle c_{12}, x_{12} \rangle \oplus \langle 8, t_{11} \rangle = 0\}.
\]

The required data for our integral distinguisher must be taken form \(A^\perp\), such that \((x_0, \ldots, x_{15})\) corresponds to the plaintext and \(t_{11}\) corresponds to cell 11 of tweak. To generate the vectors of \(A^\perp\), we can choose an arbitrary value for \(t_{11}\) at first, and then choose a suitable value for \((x_0, \ldots, x_{15})\), such that vector \((x_0, \ldots, x_{15}, t_{11})\) is in \(A^\perp\). Since,
there are $2^4$ possible values for $t_{11}$, and for each of them there are $2^{63}$ plaintexts, the total data complexity is $2^{67}$.

The zero-correlation linear hulls covering 14 rounds of CRAFT in the related-tweak model for cases $RT_2$ and $RT_3$ can also be converted to the integral distinguishers in a similar manner. In case $RT_2$, we apply any same linear mask to two cells 4, and 12, and apply zero linear masks to the remaining 14 nibbles. We also apply linear mask 0 to the cell 11 of tweak. In contrast to case $RT_0$, the set of all input masks in case $RT_2$ is a subspace of $\mathbb{F}_2^{\mathbb{F}_2^{68}}$ with dimension 4 which is again denoted by $A$. Thereby, $\dim(A^+) = 68 - 4 = 64$, and the data complexity of the corresponding integral distinguisher is equal to $2^{64}$, or equivalently, $2^4$ tweaks, and for each of them $2^{60}$, plaintexts are required. The integral distinguishers share the same input linear mask, and the cell 5 of the output is balanced.

Due to the high similarity between zero-correlation linear hulls for cases $RT_2$, and $RT_3$, the data complexity of the related-tweak integral distinguisher corresponding to case $RT_3$ is exactly the same as the case $RT_2$, and has the same input, and output linear masks as the zero-correlation linear hulls obtained for 14 rounds in case $RT_3$.

### 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 differential related tweak mode. In addition, they have provided their analysis for differential effect (resp. linear hull) of round reduced CRAFT. In single tweak mode (ST-mode), they presented a differential distinguisher for 9 and 10 rounds of the cipher with the lower bounds of probabilities $2^{-54.67}$ and $2^{-62.61}$, respectively. For related tweak mode (RT-mode), depending on the starting round based on the TK value, they have presented 15, 16, 17, and 16 rounds differential distinguisher when the cipher is started from round 0, 1, 2, and 3, respectively (denoted as $RT_0$, $RT_1$, $RT_2$ and $RT_3$ respectively). The probability of the presented distinguisher are $2^{-55.14}$, $2^{-57.18}$, $2^{-60.14}$, and $2^{-55.14}$, respectively.

#### Table 5: Optimum differential/linear trails for reduced CRAFT in different model, where for each model, the upper row determines the minimum number of active S-boxes and the lower row shows the $-\log_2 P$, and also $P$ denotes the probability of the best-found trail.

| Model | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 |
|-------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| ST Diff. | 0 | 1 | 2 | 5 | 7 | 10 | 15 | 18 | 22 | 24 | 28 | 32 | 35 | 38 | 41 | 44 | 46 |
| $-\log_2 P$ | 1 | 2 | 4 | 8 | 12 | 24 | 48 | 96 | 192 | 384 | 768 | 1536 | 3072 | 6144 | 12288 | 24576 |

To verify their results, first, we developed an automated tool, based on MILP and CryptoSMT. In the ST-mode, we reached the same number of active S-boxes, but an interesting observation was finding trails with optimum probability for any number of round and in any analysis mode, i.e., all S-boxes are activated by the maximum possible probability, i.e., $2^{-2}$ in differential/linear cryptanalysis (we only found a typo for their report of 17 rounds of $RT_1$, which was reported to be 44 S-boxes, while it should be 45).
46). Table 5 represents the minimum number of active S-boxes and also the maximum probability of a single trail for the different number of rounds in different mode of analysis.

Next, we evaluated the differential effect of the cipher in ST-mode. To enumerate the differential trails in a differential effect of CRAFT, similar to previous works [LWR16, KLT15], we used the following approach to enumerate all the 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 the solver to give a solution, repeat step 2 until the solver returns unsatisfiable.

4.1 Differential effect

In this section, we evaluated the differential effect behavior of CRAFT, by fixing the input and output difference and try to find a better differential probability. We observed that for input/output differences that satisfies a trail with minimum number of active S-boxes, there are many trails with optimum probability and all of them have an identical truncated pattern. 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 following steps to provide a lower bound on the differential probability of CRAFT for different number of rounds:

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

CryptoSMT, supports primitives with S-boxes [AK18], but it uses a naive approach to encode S-boxes. In the SMT model generated by CryptoSMT, input and output differences of each $n$-bit S-box, are represented by $n$ binary variables $x = (x_0, \ldots, x_{n-1})$, and $y = (y_0, \ldots, y_{n-1})$, respectively. It also introduces additional variables $p = (p_0, \ldots, p_{n-1})$ for each S-box $S$, representing the probability of the transition $x \rightarrow y$, which are linked to the $Pr\{x \rightarrow y\}$, by the following relation:

$$wt(p_0, \ldots, p_{n-1}) = -\log_2(Pr\{x \rightarrow y\}),$$

where $wt(p_0, \ldots, p_{n-1})$ denotes the Hamming weight of binary code $p_0 \ldots p_3$, and is called the weight of the transition $x \rightarrow y$. For example, the entries of $\{2^{-3}, 2^{-2}, 2^{-1}, 1\}$ can be encoded as follows:

<table>
<thead>
<tr>
<th>Pr</th>
<th>2^{-3}</th>
<th>2^{-2}</th>
<th>2^{-1}</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p_0 p_1 p_2 p_3$</td>
<td>0111</td>
<td>0011</td>
<td>0001</td>
<td>0000</td>
</tr>
</tbody>
</table>

In order to generate the constraints of each S-box, CryptoSMT first finds the set of all $3n$-tuple $(a_0, a_{n-1}, b_0, \ldots, b_{n-1}, c_0, \ldots, c_{n-1}) \in F_2^{3n}$ corresponding to the non-zero entries of DDT. Therefore, each $3n$-tuple out of the obtained set corresponds to an invalid assignment for $(x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}, p_0, \ldots, p_{n-1})$. 
Then CryptoSMT generates a CNF for each S-box, as a constraint which is satisfying if and only if the assignment corresponds to a valid trail. In order to generate the CNF of each S-box, it considers all invalid assignments. If an assignment \((a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1}, c_0, \ldots, c_{n-1})\) is an impossible one, then the following clause is added to the CNF:

\[
C = L(a_0, x_0) \lor \cdots \lor L(a_{n-1}, x_{n-1}) \lor \not L(b_0, y_0) \lor \cdots \lor L(b_{n-1}, y_{n-1}) \lor L(c_0, p_0) \lor \cdots \lor L(c_{n-1}, p_{n-1}),
\]

where

\[
L(s_i, t_i) = \begin{cases} t_i & \text{if } s_i = 0 \\ \not t_i & \text{if } s_i = 1, \end{cases}
\]

to exclude the invalid assignment \((a, b, c)\), from the solution space. For example, if \((1, 0, 1, 0, 0, 0, 0, 0, 0, 0)\), is an invalid assignment for the variables \((x_0, \ldots, x_3, y_0, \ldots, y_3, p_0, \ldots, p_3)\), then the following clause is added to the CNF of the S-box in the SMT model.

\[
(\not x_0 \lor x_1 \lor \not x_2 \lor \not x_3 \lor y_0 \lor y_1 \lor y_2 \lor y_3 \lor p_0 \lor p_1 \lor p_2 \lor p_3).
\]

By considering all invalid assignments, the CNF modeling the differential behaviour of a \(n\)-bit S-box is as follows:

\[
\bigwedge_{i=1}^{m} \left( \bigvee_{j=0}^{n-1} L_j(s_i, t_i) \right).
\]

The entries in the DDT of a 4-bit S-box with differential uniformity 4, including CRAFT’s S-box, only take four possible values, which are 0, 2, 4, and 16; therefore, the possible differential probabilities are 0, \(2^{-3}\), \(2^{-2}\), and 1, respectively. In contrast to the CryptoSMT’s encoding, which always uses four variables to encode the probabilities of a given 4-bit S-box, the CRAFT’s S-box probabilities can be encoded via only three binary variables denoted as \(p_0, p_1, p_2\), such that \(\text{wt}(p_0, p_1, p_2) = -\log_2(p)\).

With the aim of optimizing the CryptoSMT’s method for encoding the differential behavior of the CRAFT’s S-box, we use a different method than the CryptoSMT’s original method, which can be easily generalized for an arbitrary \(n\)-bit S-box. We first generate the truth table of the following 11-bit boolean function [SWW18]:

\[
\begin{align*}
    f(x, y, p) &= 0 & \text{if } \Pr\{x \rightarrow y\} &= 0, \\
    f(x, y, p) &= 1 & \text{if } p = (1, 1, 1) & \Pr\{x \rightarrow y\} = 2^{-3}, \\
    f(x, y, p) &= 0 & \text{if } p = (0, 1, 1) & \Pr\{x \rightarrow y\} = 2^{-2}, \\
    f(x, y, p) &= 1 & \text{if } p = (0, 0, 0) & \Pr\{x \rightarrow y\} = 1,
\end{align*}
\]

where \(x = (x_0, \ldots, x_3)\), and \(y = (y_0, \ldots, y_3)\) denote the input and the output differences, and \(p = (p_0, p_1, p_2)\) is used to encode \(\Pr\{x \rightarrow y\} = 2^{-\text{wt}(p)}\). To generate the constraints that model the differential behavior of S-box, we use the minimized product-of-sum representation of the above boolean function, which can be obtained via the Quine-McCluskey [Qui52, Qui55, MJ56], and Espresso algorithm [BHMSV84] implemented at the off-the-shelf program Logic Friday [Log19]. The minimized product-of-sum representation of the above boolean function for the CRAFT’s S-box is represented in Appendix A.
Following the above steps, we were able to accelerate the time of differential search for reduced rounds CRAFT. For instance, using the un-optimized CryptoSMT, finding a bound for differential of 11 rounds of CRAFT costed 86379s on a personal computer (Intel Core (TM)i-5, 8 Gig RAM, running Ubuntu 18.04 LTS), were we reached $2^{-58.7704}$ based on 2458966 trails (all with optimum probability of $2^{-80}$). After optimizing CryptoSMT as above, we reached the identical probability much faster. A comparison of the search time to find the best single differential characteristic for reduced rounds variants of CRAFT is provided in Table 8, and Table 9 of Appendix A. Based on this approach, for 9 rounds of CRAFT, we find the following input/output difference with the differential probability of $2^{-44.37}$, where the least significant nibble appears in the left most position:

$$7F0F\ 7F00\ 0000\ 7F00 \xrightarrow{9\text{-round}} \ 0A00\ 0000\ 0000\ 00DF.$$  

The above differential contains 810592 trails, all with probability $2^{-64}$ that have been found in 5417s on the above mentioned PC. It has an advantage of $2^{10.3}$ compared to the distinguisher provided by the designers for the same number of rounds. It should be noted that the presented bound is only the lower bound, given that we limited our searches to optimum trails and a specific truncated differential pattern. In addition, given a truncated differential pattern that minimizes the number of active S-boxes for a specific number of rounds, different trails with different input/output can be presented that satisfy the optimum probability. In the above search, we randomly selected one of them (the first optimum trail 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 difference or considering other possibilities too, e.g., non-optimum patterns.

For example, for 9 rounds, we changed all active nibbles of the input and the output differences of the above-mentioned trail to $A$ (it is represented in hexadecimal format) and observed a considerable improvement. To be more precise, for the below difference we found 2024500 optimum trails, before interrupting the run due to the RAM limitation:

$$ AA0A\ AA00\ 0000\ AA00 \xrightarrow{9\text{-round}} \ 0A00\ 0000\ 0000\ 00AA.$$  

In the case of 10 rounds, with the input difference “0AAA 00AA 0000 00AA” and the output difference “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 trails 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 extend 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 come up with expendable truncated trails for even (started from 8) and odd (started from 9) rounds of the cipher. Interestingly, this trails match the optimum number of active S-boxes for $9 \leq r \leq 17$, we did not check for $r > 17$. Figure 4 and Figure 5 represent the details of the construction of those trails. Moreover, setting active nibbles of input and output differences of each trail to $A$, provides us with a valid optimum trail. Hence, denoting the probability of an optimum trail for $r$-round of the cipher by $pr_{o,r}^0$, the trail bellow is valid for any even round $r > 8$:

$$ OAAA\ 00AA\ 0000\ 00AA \xrightarrow{r\text{-round}} \ 0A00\ 0000\ 0000\ 00AA.$$  

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

$$ AA0A\ AA00\ 0000\ AA00 \xrightarrow{r\text{-round}} \ 0A00\ 0000\ 0000\ 00AA.$$
Any of Figure 4 and Figure 5 includes three partitions, denoted by $E_{in,r_{in}}$, $E_{m,r_{m}}$ and $E_{out,r_{out}}$, where $r_{x}$ is an integer which is used to indicate the number of rounds in a partition. From now on, $E_{even}^{in,r_{in}}$, $E_{even}^{m,r_{m}}$, and $E_{even}^{out,r_{out}}$, and $E_{odd}^{in}$, $E_{odd}^{m}$ and $E_{odd}^{out}$ denote partitions of the cipher in Figure 4 and Figure 5 respectively, while $E_{in,r_{in}}^{even/odd}$, $E_{m,r_{m}}^{even/odd}$ and $E_{out,r_{out}}^{even/odd}$ denote their partitions. Hence, to design 10-round and 12-round trails, we respectively can use the structures $E_{even}^{out,4} \circ E_{m,2}^{even} \circ E_{in,4}^{even}$ and $E_{even}^{out,4} \circ E_{m,2}^{even} \circ E_{in,4}^{even}$ while to design 9-round and 11-round trails, we can use the structures $E_{odd}^{out,5} \circ E_{m,3}^{odd} \circ E_{in,4}^{even}$ and $E_{odd}^{out,5} \circ E_{m,3}^{odd} \circ E_{odd}^{even}$, respectively. It is also possible to use other combinations. For example, we can construct other 12-round trails as $E_{even}^{out,4} \circ E_{m,4}^{even} \circ E_{in,4}^{even}$, $E_{even}^{out,6} \circ E_{m,2}^{even}$ and $E_{even}^{out,6} \circ E_{in,6}^{even}$ also, where $E_{m,4} \equiv E_{m,2}^{even}$, $E_{in,6} \equiv E_{m,2}^{even}$ and $E_{out,6} \equiv E_{out,4} \circ E_{m,2}$.

It is worth noting, for the trails presented in Figure 4 and Figure 5, the output differences (nibbles) of $E_{out}^{even}$ and $E_{odd}^{even}$ are identical and the input differences (nibbles) of
Comprehensive security analysis of CRAFT

$E_{\text{even}}$ can be matched to the input of $E_{\text{odd}}$ by two nibbles rotation to right in each row.

On the other hand, from the DDT of the CRAFT’s S-box (Table 6), 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 $s(x) = y$ with probability $2^{-2}$ and for any $z \notin \{5,7,A,D,F\}$ the probability of $s(x) = z$ will be upper-bounded by $2^{-3}$. Moreover, we observed that any differential includes trails, 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, in the previous approach. These properties motivated us to do semi-truncated differential search for the different parts of our models for even and odd rounds, i.e., $E_{\text{even/odd},r_{\text{in}}}$, $E_{\text{even/odd},r_{\text{m}}}$ and $E_{\text{even/odd},r_{\text{out}}}$ in Figure 4 and Figure 5. For semi-truncated differential search, we programmed a model with the constraints below:

**Figure 5:** An expendable truncated trail for odd rounds, where $E_{\text{in}}$ and $E_{\text{out}}$ denote the first 4 and the last 5 rounds, respectively and $E_{\text{m}}$ is a repeatable 2-round truncated trail that can be used as much as required. For example, to design a 9-round trail, this stage is first 4 and the last 5 rounds, respectively.
we counted all the possible trails from the fixed input difference of vectors of both vectors/matrices, which can be done very efficiently. To this end, we determined the joint entry. Next, we used those joint probabilities vectors/matrices to determine the differential difference of out of probability matrices derived for identical to the joint probability vector derived for probability horizontal vector of probabilities vectors/matrices of all cipher’s partitions of Figure 4 and Figure 5. The joint differential probability of any trail, it will be just multiplication of those joint probability containing E partition of the cipher. We provide a horizontal vector containing to determine the differential probability of any possible input/output differences for any there are only E possible values for input/output differences of E in,,r even/odd. For each possible intermediate entry, e.g., an entry in the E in,,r even/odd, we should consider the pattern before the last E out,,r even/odd. It can be seen that to satisfy the truncated differential above constraints up to where our programs could compute. For those constrains, it is trivial that we have only one possible difference for the input of E even/odd in,,r and one possible difference for the output of E even/odd out,,r. To determine possible output-differences of E even in,,r, we should consider the pattern before the last MC, i.e., X4, and after the last MC, i.e., Y4. It can be seen that to satisfy the truncated differential pattern, we should have X4[14] = X4[10] ≠ X4[6]. Hence, there are only 5 × 5 = 100 possible values for X4 or outputs of E even out,,r. A similar argument can be provided for the input/output differences of E even out,,r and the input differences of E even out,,r. Therefore, there are only 50 × 100 possible values for input/output differences of E even and 100 possible values for input/output differences of E even out,,r. In the next step, we need to determine the differential probability of any possible input/output differences for any partition of the cipher. We provide a horizontal vector containing 100 probabilities for E even in,,r, a matrix containing 100 × 100 probabilities for E even out,,r and a vertical vector containing 100 probabilities for E even out,,r. Given those probabilities, we can calculate the differential probability of any trail, it 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 of Figure 4 and Figure 5. The joint probability horizontal vector of E even in,,r includes 76 non-zero entries (out of 100) and it is identical to the joint probability vector derived for E even in,,r. The joint probability vertical vectors of both E even out,,r and E even out,,r include 92 non-zero entries (each out of 100) and the joint probability matrices derived for E even out,,r and E even out,,r also include 2734 non-zero entries (each out of 100 × 100). For each possible intermediate entry, e.g., an entry in the E even in,,r vector, we counted all the possible trails from the fixed input difference of E even in,,r to that possible difference of E even in,,r, which can be directly used to determine the probability related to that entry. Next, we used those joint probabilities vectors/matrices to determine the differential

<table>
<thead>
<tr>
<th>x/y</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>B</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>C</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>D</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>E</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>F</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>
effect of different round reduced variants of CRAFT; in all cases we extended the number of rounds by repeating $E^{even/odd}_{r_m, 2}$ as many times as required:

\[
\begin{align*}
\text{AA0A AA00 0000 AA00} & \quad \text{9-round; Pr} \geq 2^{-60.20} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{OAAA 00AA 0000 00AA} & \quad \text{10-round; Pr} \geq 2^{-45.12} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{AA0A AA00 0000 AA00} & \quad \text{11-round; Pr} \geq 2^{-49.79} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{OAAA 00AA 0000 00AA} & \quad \text{12-round; Pr} \geq 2^{-54.72} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{AA0A AA00 0000 AA00} & \quad \text{13-round; Pr} \geq 2^{-59.39} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{OAAA 00AA 0000 00AA} & \quad \text{14-round; Pr} \geq 2^{-64.32} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{AA0A AA00 0000 AA00} & \quad \text{15-round; Pr} \geq 2^{-68.99} \rightarrow \text{OA00 0000 0000 00AA}.
\end{align*}
\]

Through our analysis we also investigated the truncated differential behavior of optimum trails of fixed input/output differences. Interestingly, we observed that for any input/output differences with the optimum trails that we have checked (including the input/output differences of Figure 4 and Figure 5) the truncated pattern of all optimum trails of a fixed input/output difference is fixed. To verify this, for a given input/output difference for which there is an optimum trail, we forced the MILP and also SAT tools to finding an optimum trail with different truncated patterns. However, for all input/output differences that we checked, the programs returned infeasible. Hence, for any trail driven from Figure 4 or Figure 5, using our partitioning approach and the way that we have used to determine the probabilities of intermediate entries, we are able to count the exact number of the optimum trails for any number of rounds of CRAFT, starting from 9 and for the given differences; also, we can determine a lower bound of non-optimum trails. In the last column of Table 7, we reported the values of the optimum trails for the several numbers of the rounds.

On the other hand, for a fixed input/output difference, changing $r_{in}$, $r_m$, and $r_{out}$, has an influence on the number of non-optimum trails that are considered in the final differential effect. Hence, although the presented distinguishers are the best known distinguishers for the round reduced CRAFT in ST-mode, to improve the results more, we also evaluated other values for $r_{in}$, $r_m$ and $r_{out}$ (it is clear that extending the number of rounds of a partition increases the computational cost of producing the related joint probabilities matrix/vector). As a result, for $r_m = 4$ (for even/odd rounds) and $r_{out} = 6$ (for even rounds) we could improve the above bounds as follows:

\[
\begin{align*}
\text{OAAA 00AA 0000 00AA} & \quad \text{10-round; Pr} \geq 2^{-44.89} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{OAAA 00AA 0000 00AA} & \quad \text{12-round; Pr} \geq 2^{-54.48} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{AA0A AA00 0000 AA00} & \quad \text{13-round; Pr} \geq 2^{-59.13} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{OAAA 00AA 0000 00AA} & \quad \text{14-round; Pr} \geq 2^{-63.80} \rightarrow \text{OA00 0000 0000 00AA}, \\
\text{AA0A AA00 0000 AA00} & \quad \text{15-round; Pr} \geq 2^{-68.75} \rightarrow \text{OA00 0000 0000 00AA},
\end{align*}
\]

where, as it is also depicted in Table 7, for the 14 rounds trail we used the combination $E^{even}_{out, 6} \circ E^{even}_{m, 4} \circ E^{even}_{in, 4}$. The above distinguishers, to the best of our knowledge, are the best-known differential distinguishers for CRAFT in ST-model.

It should be noted that we also evaluated the differential effect when $r_{in} = 6$. However, it did not give better results.
Table 7: The values of $r_{in}$, $r_m$, and $r_{out}$ of the best differential trails of CRAFT that we have found. $Pr$ denotes the probability of the related trail.

<table>
<thead>
<tr>
<th>$r_{optimum}$ trails</th>
<th>$\gamma$</th>
<th>$r_{in}$</th>
<th>$r_m$</th>
<th>$r_{out}$</th>
<th>$Pr$</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>4</td>
<td>4 - 5</td>
<td></td>
<td></td>
<td>$2^{-40.20}$</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>4 - 6</td>
<td></td>
<td></td>
<td>$2^{-44.89}$</td>
</tr>
<tr>
<td>11</td>
<td>4</td>
<td>2 - 5</td>
<td></td>
<td></td>
<td>$2^{-49.79}$</td>
</tr>
<tr>
<td>12</td>
<td>4</td>
<td>2 - 6</td>
<td></td>
<td></td>
<td>$2^{-54.48}$</td>
</tr>
<tr>
<td>13</td>
<td>4</td>
<td>4 - 5</td>
<td></td>
<td></td>
<td>$2^{-59.13}$</td>
</tr>
<tr>
<td>14</td>
<td>4</td>
<td>4 - 6</td>
<td></td>
<td></td>
<td>$2^{-63.80}$</td>
</tr>
</tbody>
</table>

5 Discussion

Through our analysis, we observed some typos in the designers’ analysis which reporting them could be useful for later analysis. We already mentioned one of them in Subsection 4.1, i.e., the minimum number of active S-boxes for 17 rounds in the case of RT1. In addition, the designers reported 12 zero-correlation masks for 13 rounds of the cipher. Although we found twelve zero-correlation linear hulls, based on our analysis with both MILP and SAT approaches, 2 of the reported masks are not valid, which are as follows, where $\gamma$ and $\delta$ are non-zero masks in $F_2^4$:

$$
\begin{align*}
0000 & 00 \gamma 0 0000 00 \gamma 0 \\
0000 & \gamma 000 0000 \gamma 000
\end{align*}
\xrightarrow{13\text{-round}}

\begin{align*}
0000 & \delta 000 0000 0000 0000, \\
0000 & 00 \delta 0 0000 0000 0000.
\end{align*}
$$

In order to verify this claim, for each one of the above linear hulls, a valid linear trail is displayed in Appendix B. We also found the following new zero-correlation linear hulls for 13 rounds of CRAFT, in ST-mode:

$$
\begin{align*}
0000 & 00 \gamma 0 0000 00 \gamma 0 \\
0000 & \gamma 000 0000 \gamma 000
\end{align*}
\xrightarrow{13\text{-round}}

\begin{align*}
0000 & 00 \delta 0 0000 0000 0000, \\
0000 & 00 \delta 0 0000 0000 0000.
\end{align*}
$$

We also checked the validity of the reported input/output patterns for the impossible differential covering 13 rounds of CRAFT. We observed that two of the input/output patterns are not valid in this case too, which are as follows, where $\gamma$ and $\delta$ are non-zero difference in $F_2^4$:

$$
\begin{align*}
00 \gamma 0 & 0000 00 \gamma 0 0000 00 \gamma 0 \\
\gamma 000 & 0000 \gamma 000 0000 \gamma 000
\end{align*}
\xrightarrow{13\text{-round}}

\begin{align*}
0000 & 00 \delta 0 0000 0000 0000, \\
0000 & 00 \delta 0 0000 0000 0000.
\end{align*}
$$

For each one of the input/output patterns above, one possible differential trail is displayed in Appendix C, which proves our claim. We also found the following two new valid impossible differential input/outputs for 13 rounds of CRAFT, in ST-mode:

$$
\begin{align*}
00 \gamma 0 & 0000 00 \gamma 0 0000 00 \gamma 0 \\
\gamma 000 & 0000 \gamma 000 0000 \gamma 000
\end{align*}
\xrightarrow{13\text{-round}}

\begin{align*}
0000 & 00 \delta 0 0000 0000 0000, \\
0000 & 00 \delta 0 0000 0000 0000.
\end{align*}
$$

In the case of RT-model of differential, designers reported the masks bellow:

$$
\begin{align*}
0000 & A000 0000 0000 0000 A000 0000 A000 0000 \\
0000 & A000 0000 0000 A000 0000 A000 0000
\end{align*}
\xrightarrow{15\text{-round-RT}_0; Pr \geq 2^{-55.14}}

\begin{align*}
0000 & 0000 0000 0000 0000 A000 0000 \\
0000 & 0000 0000 0000 A000 0000 A000 0000
\end{align*}
\xrightarrow{16\text{-round-RT}_1; Pr \geq 2^{-57.18}}
$$
Comprehensive security analysis of CRAFT

\[\begin{align*}
0000 & 0000 0000 0000 \quad 17\text{-round-}RT_2: \quad Pr \geq 2^{-60.14} \rightarrow 0000 0000 00AO \ A000, \\
0000 & 0000 0000 AA00 \quad 16\text{-round-}RT_2: \quad Pr \geq 2^{-55.14} \rightarrow 0000 0000 00AO \ A000,
\end{align*}\]

where in all cases, \(\Delta T = 0000 0000 00AO \ 0000\). However, for the provided difference for \(RT_1, RT_2\) and \(RT_3\), there are no trails for those differences with a reasonable number of active S-boxes. In addition, if the difference below is valid:

\[\begin{align*}
0000 & 0000 0000 0000 \quad 17\text{-round-}RT_2: \quad Pr \geq 2^{-60.14} \rightarrow 0000 0000 00AO \ A000,
\end{align*}\]

then, given that the input difference has no active nibble and in backward direction it first goes through S-box layers at the first, with probability 1. It is possible to present an 18 round trail for \(RT_1\) with the same probability, i.e., \(2^{-60.14}\). Hence, we also reevaluated the differential effect of CRAFT in RT-model, with the same \(\Delta T = 0000 0000 00AO \ 0000\). Our best results are as follows:

\[\begin{align*}
0000 & A000 0000 0000 \quad 15\text{-round-}RT_0: \quad Pr \geq 2^{-55.14} \rightarrow 0000 0000 00AO \ A000, \\
000A & 000A AA00 AA00 \quad 16\text{-round-}RT_1: \quad Pr \geq 2^{-62.68} \rightarrow 0000 0000 0000 0000, \\
A000 & AA00 0000 AA00 \quad 17\text{-round-}RT_2: \quad Pr \geq 2^{-60.14} \rightarrow 0000 0000 00AO \ A000, \\
A000 & 0000 00AO 0000 \quad 16\text{-round-}RT_3: \quad Pr \geq 2^{-55.14} \rightarrow 0000 0000 00AO \ A000.
\end{align*}\]

It can be seen that we could find other input/output differences for \(RT_2\) and \(RT_3\) that have identical probabilities as the probabilities reported by the designers. In the case of \(RT_0\), we received identical differential effect probability as the designers probability, for the same input/output differences. However, in the case of \(RT_1\) we could not find such differences. This distinction between our result, and those of the designers, in the case of \(RT_1\), motivated us to evaluate the differential effects for 15 and 17 rounds of this mode as follows:

\[\begin{align*}
AA00 & OAA0 000A OAA0 \quad 15\text{-round-}RT_1: \quad Pr \geq 2^{-56.31} \rightarrow 0000 0000 0000 000A, \\
\end{align*}\]

where \(\Delta T = 0000 0000 00AO \ 0000\), and,

\[\begin{align*}
050A & 000A OAA0 000A \quad 17\text{-round-}RT_1: \quad Pr \geq 2^{-65.34} \rightarrow 0000 A000 0000 0000,
\end{align*}\]

where \(\Delta T = 0000 0000 00AO \ 0000\).

It should be noted we also evaluated the security of CRAFT against linear hull, following the same approach as the differential effect. However, we could not beat the designers’ claim, which is \(2^{-62.12}\) for 14- rounds of CRAFT in ST-model.

6 Conclusion

In this work, we provided a detailed analysis of CRAFT against differential and related tweak zero-correlation and integral cryptanalysis. Our related tweak zero-correlation and integral cryptanalysis, which cover 14 rounds, are the first analysis of CRAFT against this attack, given that the designers analyzed its security against single tweak zero-correlation and integral cryptanalysis. While we found 14-round distinguishers in the related tweak zero-correlation/integral cryptanalysis for cases \(RT_0, RT_2\), and \(RT_3\), we could not find any related tweak zero-correlation/integral distinguisher for case \(RT_1\) for 14-rounds of the cipher.
Our differential analysis improved the designers’ results significantly. For example, the designers’ report include the lower bound of probability of differential effect for 10 rounds of the cipher in single tweak model to be $2^{-62.61}$ while we improved this bound and presented a differential distinguisher for the same number of rounds with probability $2^{-44.89}$ and a differential distinguisher for up to 14 rounds, with the probabilities beyond $2^{-64}$. This analysis shows that there is a huge gap between the differential effect and any differential trails in the round reduced CRAFT, similar to some other lightweight block ciphers already mentioned in [AK18].

Through our differential analysis, we observed that for many fixed input/output differentials, CRAFT included very strong clusters of high-probable trails that helped us to improve the probability of our differential distinguishers significantly.

In our differential effect analysis of the even/odd number of rounds, we fixed the input/output masks for even/odd number of rounds, and provided extendable truncated differential trails for the cipher and then partitioned those trails to estimate the differential effect of the whole target rounds. This approach helped us estimate the differential effect of the cipher more efficiently (in term of time and the used resources), compared to naive approaches based on counting trails. Thanks to the fixed truncated differential pattern of CRAFT for all optimum trails of a fixed input/output mask, partitioning works well to bound its differential effect and we were able to provide the exact number of optimum trails for a given fixed input/output difference; and for any number of rounds, larger than 9, it can be done for any other input/output mask. As a future work, it is worth investigating whether there is any other cipher with the same differential behavior, i.e., fixed truncated differential for dominant trails. If there is, then it should be possible to use the partitioning approach to evaluate its security against differential effect. In addition, while our bound for the number of optimal trails for any fixed input/output mask is tight, we were not able to bound the exact number of non-optimum trails for the used masks. Hence, as another future work, it is possible to improve the reported differential effects considering some missing non-optimum trails in our analysis.

The designer stated [BLMR19, Sec. 5.4] “For the key recovery the number of rounds that can be appended for an RTi differential is at most $4 + i$ rounds before and $7$ rounds after the differential”. However, given that the focus of this paper was to provide better distinguishers for CRAFT, we have not investigated the key recovery in this paper. Hence, as a future work, it worth to see how many rounds can be attacked based on the provided distinguishers in this paper.

Acknowledgment

The authors gratefully thank the use of School of Computer Science, Institute for Research in Fundamental Science (IPM) as the computations were partially done there. We would like to thank Christof Beierle for his invaluable comments and suggestions in preparing the final draft of this paper. We would like also to thank all the anonymous reviewers of ToSC for their valuable comments which helped us to improve the presentation of the work significantly. We would like also to thank Hadi Soleimany for his invaluable comments and suggestions in preparing this paper. We would like also to thank the designers team of CRAFT, specially Shahram Rasoolzadeh, for their valuable feedback during our communications. The work of the second author is supported by the ANR (DeCrypt ANR-18-CE39-0007). The third author was supported in part by the Iran National Science Foundation (INSF) under contract No. 96/53979. The fourth author was supported in part by the National Natural Science Foundation of China (Grants No. 61802399, 61732021).
References


A Supplementary information for optimized CryptoSMT

Let $a = (a_3, \ldots, a_0)$, and $b = (b_3, \ldots, b_0)$ denote the input and output differences respectively, where $a_0$, and $b_0$ are the least significant bits, and $p = (p_2, p_1, p_0)$ is also used to encode the probability of transition $a \rightarrow b$. We use the following CNF to model the differential behavior of CRAFT’s S-box in the SMT model:
Similar to the Boolean function which is used to model the differential behaviour of an Sbox, another Boolean function can be constructed to model the linear behaviour of the given Sbox, according to the related table of squared correlations. If \( a = (a_3, \ldots, a_0) \), and \( b = (b_3, \ldots, b_0) \) denote the input and output linear masks respectively, where \( a_0 \) and \( b_0 \) are the least significant bits, and \( p = (p_1, p_2, p_3, p_0) \) is used to encode the squared correlation of transition \( a \rightarrow b \), we use the following CNF to model the linear behavior of CRAFT’s S-box in the SMT model:

\[
( p_3 \lor p_2 ) \land ( p_1 \lor p_0 ) \land ( p_3 \lor p_2 ) \land ( p_2 \lor p_0 ) \land ( b_1 \lor p_0 ) \land ( b_3 \lor b_2 \lor b_1 \lor b_0 \lor p_1 ) \land ( b_3 \lor p_0 ) \land ( a_3 \lor a_2 \lor a_1 \lor a_0 \lor p_0 ) \land ( a_3 \lor a_2 \lor a_1 \lor a_0 \lor b_3 \lor b_2 \lor b_1 \lor b_0 ) \land ( a_1 \lor a_0 \lor b_3 \lor b_2 \lor b_1 \lor b_0 ) \land ( a_3 \lor a_2 \lor a_1 \lor a_0 \lor b_3 \lor b_2 \lor b_1 \lor b_0 ) \land ( a_3 \lor a_2 \lor a_1 \lor a_0 \lor b_3 \lor b_2 \lor b_1 \lor b_0 ) \land ( a_3 \lor a_2 \lor a_1 \lor a_0 \lor b_3 \lor b_2 \lor b_1 \lor b_0 ) \land ( a_3 \lor a_2 \lor a_1 \lor a_0 \lor b_3 \lor b_2 \lor b_1 \lor b_0 ) \land ( a_3 \lor a_2 \lor a_1 \lor a_0 \lor b_3 \lor b_2 \lor b_1 \lor b_0 )
\]

CryptoSMT, uses STP[HMS], as the default SMT solver to solve the obtained SMT problem, but it also supports another SMT solver, called Boolector[NPB15]. Table 8 shows that, our optimization improves the speed of solving the obtained SMT problem, for both SMT solvers used in CryptoSMT. Table 9, also shows the impact of our optimization on the solvers’ run-time for finding an optimum differential trail for \( r \) rounds of CRAFT, where the input, and output differences corresponding to the optimum trail are fixed.
Table 8: The impact of the CRAFT’s S-box optimization on the solvers’ run-time, where SW and MW respectively denote start-weight and minimum found weight through the search for the best single differential characteristic of $r$ rounds of CRAFT in the single tweak model.

<table>
<thead>
<tr>
<th>$r$</th>
<th>SW</th>
<th>MW</th>
<th>Optimized STP</th>
<th>Optimized Boolector</th>
<th>Unoptimized STP</th>
<th>Unoptimized Boolector</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>2($2^{-2}$)</td>
<td>0.36 s</td>
<td>0.52 s</td>
<td>34.2 s</td>
<td>13.55 s</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4($2^{-4}$)</td>
<td>0.80 s</td>
<td>1.07 s</td>
<td>75.07 s</td>
<td>29.69 s</td>
</tr>
<tr>
<td>3</td>
<td>4</td>
<td>8($2^{-8}$)</td>
<td>2.25 s</td>
<td>2.79 s</td>
<td>195.67 s</td>
<td>74.78 s</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
<td>12($2^{-12}$)</td>
<td>3.25 s</td>
<td>4.18 s</td>
<td>313.44 s</td>
<td>100.83 s</td>
</tr>
<tr>
<td>5</td>
<td>12</td>
<td>20($2^{-20}$)</td>
<td>10.84 s</td>
<td>13.92 s</td>
<td>831.86 s</td>
<td>234.95 s</td>
</tr>
<tr>
<td>6</td>
<td>20</td>
<td>28($2^{-28}$)</td>
<td>20.55 s</td>
<td>20.14 s</td>
<td>1249.29 s</td>
<td>296.06 s</td>
</tr>
<tr>
<td>7</td>
<td>28</td>
<td>40($2^{-30}$)</td>
<td>69.03 s</td>
<td>58.7 s</td>
<td>2703.25 s</td>
<td>512.25 s</td>
</tr>
<tr>
<td>8</td>
<td>40</td>
<td>52($2^{-32}$)</td>
<td>179.63 s</td>
<td>100.07 s</td>
<td>5526.63 s</td>
<td>664.21 s</td>
</tr>
<tr>
<td>9</td>
<td>52</td>
<td>64($2^{-34}$)</td>
<td>501.68 s</td>
<td>190.35 s</td>
<td>9739.49 s</td>
<td>831.22 s</td>
</tr>
</tbody>
</table>

Table 9: The impact of the CRAFT’s S-box optimization on the solvers’ run-time, to find an optimum differential trail with fixed input, and output differences for $r$ rounds of CRAFT.

<table>
<thead>
<tr>
<th>$r$</th>
<th>Optimized STP</th>
<th>Optimized Boolector</th>
<th>Unoptimized STP</th>
<th>Unoptimized Boolector</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>0.40 s</td>
<td>0.11 s</td>
<td>34.2 s</td>
<td>15.53 s</td>
</tr>
<tr>
<td>9</td>
<td>1.44 s</td>
<td>0.66 s</td>
<td>116.56 s</td>
<td>42.91 s</td>
</tr>
<tr>
<td>10</td>
<td>1.61 s</td>
<td>1.44 s</td>
<td>130.38 s</td>
<td>49.3 s</td>
</tr>
<tr>
<td>11</td>
<td>2.11 s</td>
<td>1.84 s</td>
<td>147.54 s</td>
<td>55.32 s</td>
</tr>
<tr>
<td>12</td>
<td>2.53 s</td>
<td>2.07 s</td>
<td>204.66 s</td>
<td>60.55 s</td>
</tr>
<tr>
<td>13</td>
<td>2.76 s</td>
<td>2.53 s</td>
<td>266.03 s</td>
<td>68.30 s</td>
</tr>
<tr>
<td>14</td>
<td>3.99 s</td>
<td>3.75 s</td>
<td>319.30 s</td>
<td>74.72 s</td>
</tr>
<tr>
<td>15</td>
<td>4.13 s</td>
<td>3.78 s</td>
<td>313.45 s</td>
<td>81.16 s</td>
</tr>
</tbody>
</table>
## B Valid linear trails

### Table 10: A valid linear trail with weight 124, corresponding to the linear hull
0000 00\gamma 0 0000 00\gamma 0 ^{13\text{-round}} 0000 0000 0000

<table>
<thead>
<tr>
<th>(i)</th>
<th>(\Gamma X^i)</th>
<th>(\Gamma Y^i)</th>
<th>(\Gamma Z^i)</th>
<th>(w)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000 0050 0000 0050</td>
<td>0000 0050 0000 0050</td>
<td>0000 0000 5000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>1</td>
<td>0000 0000 A000 0000</td>
<td>0000 0000 A000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>2</td>
<td>0000 0000 00A0 0000</td>
<td>0000 00A0 0000 00A0</td>
<td>00A0 0000 A000 0000</td>
<td>-4</td>
</tr>
<tr>
<td>3</td>
<td>0000 0000 00A0 0000</td>
<td>0000 00A0 0000 00A0</td>
<td>0000 00A0 A000 0000</td>
<td>-8</td>
</tr>
<tr>
<td>4</td>
<td>0000 00A0 0000 00A0</td>
<td>0000 00A0 0000 00A0</td>
<td>AA00 00A0 A000 0000</td>
<td>-12</td>
</tr>
<tr>
<td>5</td>
<td>A500 00A0 0000 0050</td>
<td>A500 00A0 0050 A5A5</td>
<td>5A5A 05FA A000 5000</td>
<td>-20</td>
</tr>
<tr>
<td>6</td>
<td>A5A5 05A5 A000 00F0</td>
<td>A5A5 05A5 0A55 05FA</td>
<td>A5FF 5A05 5A0A 5A5A</td>
<td>-28</td>
</tr>
<tr>
<td>7</td>
<td>00A5 00A0 A05F 05AA</td>
<td>00A5 00A0 A500 0A00</td>
<td>0000 0000 0000 0000</td>
<td>-12</td>
</tr>
<tr>
<td>8</td>
<td>00A5 00A0 A05F 05AA</td>
<td>00A5 00A0 A500 0A00</td>
<td>0000 0000 0000 0000</td>
<td>-4</td>
</tr>
<tr>
<td>9</td>
<td>00A5 00A0 A05F 05AA</td>
<td>00A5 00A0 A500 0A00</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>10</td>
<td>00A5 00A0 A05F 05AA</td>
<td>00A5 00A0 A500 0A00</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>11</td>
<td>00A5 00A0 A05F 05AA</td>
<td>00A5 00A0 A500 0A00</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>12</td>
<td>00A5 00A0 A05F 05AA</td>
<td>00A5 00A0 A500 0A00</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>13</td>
<td>00A5 00A0 A05F 05AA</td>
<td>00A5 00A0 A500 0A00</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
</tbody>
</table>

### Table 11: A valid linear trail with weight 124, corresponding to the linear hull
0000 \gamma 0000 \gamma 0000 \gamma 0000 \gamma 0000 0000

<table>
<thead>
<tr>
<th>(i)</th>
<th>(\Gamma X^i)</th>
<th>(\Gamma Y^i)</th>
<th>(\Gamma Z^i)</th>
<th>(w)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0000 5000 0000 5000</td>
<td>0000 5000 0000 5000</td>
<td>0000 0000 0050 0000</td>
<td>-2</td>
</tr>
<tr>
<td>1</td>
<td>0000 0000 00F0 0000</td>
<td>0000 0000 00F0 0000</td>
<td>0000 F000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>2</td>
<td>0000 F000 0000 0000</td>
<td>0000 F000 0000 0000</td>
<td>0000 F000 0000 0000</td>
<td>-4</td>
</tr>
<tr>
<td>3</td>
<td>0500 0000 0050 0000</td>
<td>0500 0000 0050 0050</td>
<td>0500 5500 0000 5000</td>
<td>-8</td>
</tr>
<tr>
<td>4</td>
<td>00A0 AF00 0000 A000</td>
<td>00A0 AF00 0000 A000</td>
<td>00FA AF00 00A0 A000</td>
<td>-12</td>
</tr>
<tr>
<td>5</td>
<td>05A5 5000 05A0 0500</td>
<td>05A5 5000 05A0 0500</td>
<td>555A F5A0 0050 05A0</td>
<td>-20</td>
</tr>
<tr>
<td>6</td>
<td>AFBF FA0A 00B0 0A50</td>
<td>AFBF FA0A 00F0 5FE5</td>
<td>55FF OFAF 0AF0 FBFA</td>
<td>-28</td>
</tr>
<tr>
<td>7</td>
<td>AAFF OFA5 OFA5 555A</td>
<td>AAFF OFA5 OFA5 555A</td>
<td>AAFF OFA5 OFA5 555A</td>
<td>-20</td>
</tr>
<tr>
<td>8</td>
<td>A500 00A0 550F A5A5</td>
<td>A500 00A0 550F A5A5</td>
<td>A500 00A0 550F A5A5</td>
<td>-12</td>
</tr>
<tr>
<td>9</td>
<td>A500 00A0 550F A5A5</td>
<td>A500 00A0 550F A5A5</td>
<td>A500 00A0 550F A5A5</td>
<td>-4</td>
</tr>
<tr>
<td>10</td>
<td>005A 0000 0050 0000</td>
<td>005A 0000 0050 0050</td>
<td>005A 0000 0050 0050</td>
<td>-2</td>
</tr>
<tr>
<td>11</td>
<td>005A 0000 0050 0000</td>
<td>005A 0000 0050 0050</td>
<td>005A 0000 0050 0050</td>
<td>-2</td>
</tr>
<tr>
<td>12</td>
<td>005A 0000 0050 0000</td>
<td>005A 0000 0050 0050</td>
<td>005A 0000 0050 0050</td>
<td>-2</td>
</tr>
<tr>
<td>13</td>
<td>005A 0000 0050 0000</td>
<td>005A 0000 0050 0050</td>
<td>005A 0000 0050 0050</td>
<td>-2</td>
</tr>
</tbody>
</table>
C Possible differential trails

Table 12: A possible differential trail with weight 124, corresponding to the input/output
pattern $00\gamma 0 0000 00\gamma 0 0000 \overrightarrow{13\text{-round}} 0000 0000 0000 0000$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$\Delta X^i$</th>
<th>$\Delta Y^i$</th>
<th>$\Delta Z^i$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00AO 0000 00AO 0000</td>
<td>0000 00AO 0000 00AO 0000</td>
<td>00AO 0000 00AO 0000</td>
<td>-2</td>
</tr>
<tr>
<td>1</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>2</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-4</td>
</tr>
<tr>
<td>3</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-8</td>
</tr>
<tr>
<td>4</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-12</td>
</tr>
<tr>
<td>5</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-20</td>
</tr>
<tr>
<td>6</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-28</td>
</tr>
<tr>
<td>7</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-40</td>
</tr>
<tr>
<td>8</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-56</td>
</tr>
<tr>
<td>9</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-72</td>
</tr>
<tr>
<td>10</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-88</td>
</tr>
<tr>
<td>11</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-104</td>
</tr>
<tr>
<td>12</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-120</td>
</tr>
<tr>
<td>13</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>0000 00AO 0000 0000</td>
<td>-136</td>
</tr>
</tbody>
</table>

Table 13: A possible differential trail with weight 124, corresponding to the input/output
pattern $\gamma 0000 0000 0000 0000 \overrightarrow{13\text{-round}} 0000 0000 0000 0000$

<table>
<thead>
<tr>
<th>$i$</th>
<th>$\Delta X^i$</th>
<th>$\Delta Y^i$</th>
<th>$\Delta Z^i$</th>
<th>$w$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>A000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>1</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-2</td>
</tr>
<tr>
<td>2</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-4</td>
</tr>
<tr>
<td>3</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-8</td>
</tr>
<tr>
<td>4</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-12</td>
</tr>
<tr>
<td>5</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-20</td>
</tr>
<tr>
<td>6</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-28</td>
</tr>
<tr>
<td>7</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-40</td>
</tr>
<tr>
<td>8</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-56</td>
</tr>
<tr>
<td>9</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-72</td>
</tr>
<tr>
<td>10</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-88</td>
</tr>
<tr>
<td>11</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-104</td>
</tr>
<tr>
<td>12</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-120</td>
</tr>
<tr>
<td>13</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>0000 0000 0000 0000</td>
<td>-136</td>
</tr>
</tbody>
</table>