Impossible Differential Cryptanalysis of Reduced-Round Tweakable TWINE

Mohamed Tolba, Muhammad ElSheikh, and Amr M. Youssef

Concordia Institute for Information Systems Engineering, Concordia University, Montréal, Québec, Canada
youssef@ciise.concordia.ca

Abstract. Tweakable TWINE (T-TWINE) is a new lightweight tweakable block cipher family proposed by Sakamoto et al. at IWSEC 2019. T-TWINE is the first Tweakable Block Cipher (TBC) that is built on Generalized Feistel Structure (GFS). It is based on the TWINE block cipher in addition to a simple tweak scheduling based on SKINNY’s tweakey schedule. Similar to TWINE, it has two versions, namely, T-TWINE-80 and T-TWINE-128, both have a block length of 64 bits and employ keys of length 80 and 128 bits, respectively. In this paper, we present impossible differential attacks against reduced-round versions of T-TWINE-80 and T-TWINE-128. First, we present an 18-round impossible differential distinguisher against T-TWINE. Then, using this distinguisher, we attack 25 and 27 rounds of T-TWINE-80 and T-TWINE-128, respectively.

Keywords: Cryptanalysis · Impossible differential attacks · Tweakable · Block ciphers · TWINE · T-TWINE

1 Introduction

Tweakable Block Ciphers (TBCs) [11] differ from the conventional block ciphers since they accept an additional input called a tweak. Different specific keyed instances of the cipher can be generated by varying this tweak. TBCs allow new interesting highly-secure modes of operation and applications to become possible as they are designed to allow changing the tweak very efficiently compared to the key setup operation.

Block ciphers can be used to build TBCs through modes of operation such as LRW (Liskov, Rivest, and Wagner) and XEX (Xor-Encrypt-Xor) [14]. These modes of operations, for one TBC encryption/decryption, require few cipher calls. Therefore, they are efficient. However, their provable security guarantee, which is $2^{n/2}$ for n-bit block cipher, is not enough, in particular, for TBCs employed in modes of operation aiming to achieve “beyond-the-birthday-bound” (BBB) security. As a result, less efficient modes of operations [9,10], compared to LRW and XEX, are proposed to achieve BBB security guarantee.

Dedicated constructions is another approach to build efficient TBCs with an acceptable level of security guarantee. HPC [16], one of the submission to the
AES competition, is the first proposal, where the tweak is called “spice”. Three-fish [4], Deoxys-BC [7], SKINNY [2] and QARMA [1] are examples of recently proposed dedicated TBCs. Challenges such as designing efficient dedicated TBCs while having sufficient security guarantee is solved by the tweakable framework [6] which is based on a Substitution Permutation Network (SPN).

Tweakable TWINE (T-TWINE) [15] is the first dedicated TBC that is based on Generalized Feistel Structure (GFS) [13,20]. The only work on GFS-based TBC, before the T-TWINE proposal, is done by Goldenberg et al. [5] and Mitsu and Iwata [12] who focused on studying the provable security of the round functions that are instantiated by PRFs. TWINE, which is a GFS-based block cipher, was proposed by Suzaki et al. [18] after a comprehensive study done by Suzuki and Minematsu [17] showing the effect of the choice of sub-block permutation on the diffusion, the number of differential/linear active S-boxes, and the maximum numbers of rounds for impossible differential characteristics and saturation characteristics. The choice of the permutation of TWINE was a result of the work done in [17], it permutes over 16 nibbles to achieve the best characteristics.

T-TWINE [15] is built with the goal of reducing the cost of design, security evaluation, and implementation. As a result, TWINE was selected to be the basic building block of T-TWINE with extremely simple tweak scheduling. This tweak schedule is based on the SKINNY’s [2] tweakey schedule. Similar to TWINE, T-TWINE has a block size of 64 bits and iterates using either 80-bit or 128-bit key over 36 rounds. It accepts an additional 64-bit tweak. It also uses independent key and tweak schedules where the tweak is mixed with the states by adding few nibble XORs to TWINE. Therefore, it has the same hardware cost of TWINE except for the additional tweak registers.

The designers of T-TWINE evaluated its security against differential, linear, impossible differential, and integral attacks in the chosen-tweak setting. However, they only presented distinguishers without converting any distinguisher to a key recovery attack. For impossible differential, they utilized the miss-in-the-middle approach to search the impossible differential characteristics that have one active nibble in the 16 tweak nibbles and one active nibble in 16 ciphertext nibbles at the decryption side. However, the 18-round impossible differential distinguisher that was proposed by the designers does not seem to be correct as we will illustrate in Sect. 3.

In this paper, we start by presenting an 18-round impossible differential distinguisher. Then, we use this distinguisher to launch a 25-round attack against T-TWINE-80 by pre-appending and appending 4 and 3 rounds, respectively. Finally, we launched a 27-round attack against T-TWINE-128, using the 18-round distinguisher, by pre-appending and appending 6 and 3 rounds, respectively. The data, time, and memory complexities of the 25-round (225-round) against T-TWINE-80 (T-TWINE-128) are 2^{51.5} (2^{60}) chosen plaintexts, 2^{70.86} 25-round (2^{120.83} 27-round) encryptions, 2^{66} (2^{118}) 64-bit block, respectively.

1 This has also been confirmed through personal communications with the designers.
The rest of the paper is organized as follows. Section 2 provides the notations used throughout the paper and a brief description of T-TWINE. In Sect. 3, we present the impossible differential distinguisher used in our attacks. The details of our attacks are presented in Sects. 4 and 5. Finally, the paper is concluded in Sect. 6.

## 2 Specifications of T-TWINE

The following notation will be used throughout the rest of the paper:

- $K$: The 80 or 128 bits master key.
- $K_j$: The $j^{th}$ nibble of $K$. The indices of the nibbles begin from 0.
- $RK^i$: The 32-bit round key used in round $i + 1$.
- $RKn$: The $n^{th}$ nibble of $RK^i$. The indices of the nibbles begin from 0.
- $T$: The 64-bit tweak.
- $T_i$: The $i^{th}$ nibble of the tweak $T$.
- $RT^i$: The 24-bit round tweak used in round $i + 1$, where $RT^i \leftarrow t_0 || t_1 || t_2 || t_3 || t_4 || t_5$, and $t_j$ is the $j^{th}$ nibble of $RT^i$.
- $X^i$: The 16 4-bit nibbles output of round $i$.
- $X^n_j$: $j^{th}$ nibble of $X^i$.
- $\Delta X^i, \Delta X^n$: The difference at state $X^i$ and nibble $X^n_j$, respectively.
- $\oplus$: The XOR operation.
- $||$: The concatenation operation.
- $\text{Rotz}(x)$: The $z$-bit left cyclic shift of $x$.

T-TWINE is based on TWINE [18]. T-TWINE-80/128 iterates 36 rounds over 64-bit block using 80/128-bit key, respectively, and 64-bit tweak $T$. The block cipher has three parts: data processing, key schedule, and tweak schedule. Except for the tweaks addition, T-TWINE-80/128 has the same data processing and key schedule of TWINE-80/128, respectively. Both T-TWINE-80 and T-TWINE-128 employ the same generalized Feistel structure and tweak schedule where the only difference between them is the key schedule.

**Data Processing Part.** As depicted in Fig. 1, the round function is based on a variant of Type-2 GFS with 16 4-bit nibbles [17]. It has four operations: 4-bit S-box ($S$, see Table 1), round key XOR, round tweak XOR, and a 16-nibble shuffle operation ($\pi$, see Table 2). Both versions of T-TWINE have the same number of rounds (36). The nibble shuffle operation in the last round is omitted.

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

**Key Schedule.** A round key $RK^i$ of 8 nibbles is generated from the master key $K$ for each round $i$, where $0 \leq i < 35$. Each version of T-TWINE has its own key.
5. For example, $t_0$ equivalent to $t'_0$.

Fig. 1. The T-TWINE round function, for simplicity we use $t_j$ instead of $t'_j$. For example, $t_0$ equivalent to $t'_0$.

Tweak Schedule. A round tweak $RT^i$ of 6 nibbles is generated from the tweak $T$ for each round $i$, where $0 ≤ i < 35$. Both versions of T-TWINE have the same tweak schedule, shown in Algorithm 3, where $π^t$ is a 6-nibble permutation s.t. $(0, 1, 2, 3, 4, 5) → (1, 0, 4, 2, 3, 5)$.

3 An Impossible Differential Distinguisher of T-TWINE

Impossible differential cryptanalysis was proposed independently by Knudsen [8] and Biham, Biryukov and Shamir [3]. It exploits a (truncated) differential characteristic of probability exactly 0 and thus acts as a distinguisher. Then, this distinguisher is turned into a key-recovery attack by prepending and/or appending additional rounds, which are usually referred to as the analysis rounds. The keys involved in the analysis rounds which lead to the impossible differential are wrong keys and thus are excluded. Miss-in-the-Middle is the general technique used to construct impossible differentials, where the cipher, $E$, is split such that $E = E_2 \circ E_1$, and we try to find two deterministic differentials, the first one covers $E_1$ and has the form $Δδ → Δγ$, and the second covers $E_2^{-1}$, and has the form $Δβ → Δζ$. When the intermediate differences $Δγ, Δζ$ do not match, the differential $Δδ → Δβ$ that covers the whole cipher $E$ holds with zero probability.

Table 2. Nibble shuffle $π$

| $h$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
|-----|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|
| $π[h]$ | 5 | 0 | 1 | 4 | 7 | 12 | 3 | 8 | 13 | 6 | 9 | 2 | 15 | 10 | 11 | 14 |
| $π^{-1}[h]$ | 1 | 2 | 11 | 6 | 3 | 0 | 9 | 4 | 7 | 10 | 13 | 14 | 5 | 8 | 15 | 12 |
Algorithm 1: Key Schedule of T-TWINE-80

Data: The 80-bit master key $K$

Result: The round keys $RK = RK^0 || RK^1 || \cdots || RK^{35}$

$k_0 || k_1 || \cdots || k_{19} \leftarrow K$

for $i \leftarrow 0$ to 34 do

$RK^i \leftarrow k_1 || k_3 || k_4 || k_6 || k_{13} || k_{14} || k_{15} || k_{16}$

$k_1 \leftarrow k_1 \oplus S(k_0)$

$k_4 \leftarrow k_4 \oplus S(k_{16})$

$k_7 \leftarrow k_7 \oplus (0||CON_H)$

$k_{19} \leftarrow k_{19} \oplus (0||CON_L)$

$k_0 || \cdots || k_3 \leftarrow Rot(4(k_0) || \cdots || k_3)$

$k_0 || \cdots || k_{19} \leftarrow Rot_{16}(k_0) || \cdots || k_{19}$

$RK^{35} \leftarrow k_1 || k_3 || k_4 || k_6 || k_{13} || k_{14} || k_{15} || k_{16}$

$RK \leftarrow RK^0 || RK^1 || \cdots || RK^{35}$

Algorithm 2: Key Schedule of T-TWINE-128

Data: The 128-bit master key $K$

Result: The round keys $RK = RK^0 || RK^1 || \cdots || RK^{35}$

$k_0 || k_1 || \cdots || k_{31} \leftarrow K$

for $i \leftarrow 0$ to 34 do

$RK^i \leftarrow k_2 || k_3 || k_4 || k_6 || k_{12} || k_{15} || k_{17} || k_{18} || k_{28} || k_{31}$

$k_1 \leftarrow k_1 \oplus S(k_0)$

$k_4 \leftarrow k_4 \oplus S(k_{16})$

$k_{23} \leftarrow k_{23} \oplus S(k_{30})$

$k_7 \leftarrow k_7 \oplus (0||CON_H)$

$k_{19} \leftarrow k_{19} \oplus (0||CON_L)$

$k_0 || \cdots || k_3 \leftarrow Rot(4(k_0) || \cdots || k_3)$

$k_0 || \cdots || k_{31} \leftarrow Rot_{16}(k_0) || \cdots || k_{31}$

$RK^{35} \leftarrow k_2 || k_3 || k_{12} || k_{15} || k_{17} || k_{18} || k_{28} || k_{31}$

$RK \leftarrow RK^0 || RK^1 || \cdots || RK^{35}$

Algorithm 3: Tweak Schedule of T-TWINE

Data: The 64-bit tweak $T$

Result: The round tweaks $RT = RT^0 || RT^1 || \cdots || RT^{35}$

$t_0^0 || t_1^0 || \cdots || t_{16}^0 \leftarrow T$

for $i \leftarrow 0$ to 35 do

$RT^i \leftarrow t_0^i || t_1^i || t_2^i || t_3^i || t_4^i || t_5^i$

for $h \leftarrow 0$ to 5 do

$t_{\pi^i[h]}^i \leftarrow t_h^i$

for $h \leftarrow 0$ to 15 do

$t_{(h-6) \mod 16}^{i+1} \leftarrow t_h^i$

$RT \leftarrow RT^0 || RT^1 || \cdots || RT^{35}$
The designers of T-TWINE in [15] presented an 18-round impossible differential distinguisher. They found this distinguisher using the Miss-in-the-Middle approach. The distinguisher begins at “1R” with zero differences and the tweak has a non-zero difference at the first nibble \( t_0 \). As mentioned above, this 18-round impossible differential distinguisher does not seem to be correct. In what follows, we list some of the problems (mistakes) we identified in this distinguisher (See Fig. 5): i) the numbers of rounds involved in the distinguisher is only 17 not 18 (as the plaintext is marked “1R” and the ciphertext is marked “18R”), ii) the tweaks used in the distinguisher are wrong. For example, the tweaks that are used in the seventh and ninth rounds are actually the tweaks of the sixth and seventh rounds, respectively, and iii) this distinguisher assumes that the tweak has difference at nibble “0” at the first round, then it appear again at nibble “0” at the nineteenth round, while it should appear again at the seventeenth round, after 16 rounds of the tweak schedule. Moreover, as shown in Figure 8 of [15] (See Fig. 5), the zero difference at “1R” associated with a non-zero difference at the first nibble \( t_0 \) of the tweak gives, after being propagated 7 rounds in the forward direction, the difference at “8R” in the form of \( (1, 1, 1, 0, 0, ?, 0, 1, 1, ?, 0, 1, ?, ?, ?, ?) \). However, the correct difference should be in the form of \( (?, 1, ?, 0, 1, ?, ?, 1, 1, ?, ?, 1, ?, ?, ?, ?) \).

In this section, we present an 18-round distinguisher that begins and ends with zero difference and has a difference at \( t_{12} \) at the first round, see Fig. 2. To the best of our knowledge, this is the first valid 18-round impossible differential distinguisher. This distinguisher is found using the Miss-in-the-Middle approach, where we propagate the difference in the tweak forward 8 rounds with probability 1 and propagate the difference in the tweak backward 10 rounds with probability 1, then match at the middle at the end of round 8. As seen in Fig. 2, there is a contradiction at nibble “6”, where in the forward path, it should have a zero difference, while in the backward path, it should have a non-zero difference.

### 3.1 Observations

In this section, we present some useful observations that will be utilized in our attack.

**Observation 1 [18,19].** For any input difference \( a(\neq 0) \) and output difference \( b(\in \Delta S[a]) \) of the S-box in TWINE, the average number of pairs that satisfy the differential characteristic \( (a \rightarrow b) \) is \( \frac{16}{7} \). Given an 8-bit pair \( (X_{2j}^{i} \oplus a, X_{2j+1}^{i} \oplus b) \), the probability that \( RK_{j}^{i} \) leads to the S-box differential characteristic \( (a \rightarrow b) \) is \( 7^{-1} \).
Fig. 2. An 18-round impossible differential distinguisher
Observation 2. Given two nonzero differences $\Delta i$ and $\Delta o$ in $\mathbb{F}_{16}$, the equation: $S(x) + S(x + \Delta i) = \Delta o$ has one solution on average. This property also applies to $S^{-1}$.

Observation 3. If the impossible differential illustrated in Fig. 2 is extended 6 rounds forward and 3 rounds backward, then we have the following relations, see Fig. 3: $\Delta X^0_9 \in S[\Delta X^0_2]$, $\Delta X^0_7 \in S[\Delta X^0_0]$, $\Delta X^0_{13} \in S[\Delta X^0_{12}]$, $\Delta X^0_6 \in S[\Delta X^0_{11}]$, $\Delta X^0_{11} \in S[\Delta X^0_2]$, $\Delta X^0_{27} \in S[\Delta T_2]$, $\Delta X^0_{25} \in S[\Delta X^0_{12}]$, $\Delta X^0_{14} \in S[\Delta X^0_{11}]$, $\Delta X^0_{27} \in S[\Delta T_2]$ that hold with probability $(\frac{7}{16})^9 = 2^{-10.734}$.

Observation 4. If the impossible differential illustrated in Fig. 2 is extended 4 rounds forward and 3 rounds backward, then we have the following relations, see Fig. 4: $\Delta X^1_1 \in S[\Delta X^0_0]$, $\Delta X^0_{11} \in S[\Delta X^0_{10}]$, $\Delta X^0_{15} \in S[\Delta X^0_{14}]$, $\Delta X^0_{14} \in S[\Delta T_7]$, $\Delta X^0_6 \in S[\Delta X^0_3]$, $\Delta X^0_{15} \in S[\Delta X^0_{10}]$, $\Delta X^0_{10} \in S[\Delta T_7]$, $\Delta X^0_{25} \in S[\Delta X^0_{25}]$, $\Delta X^0_{25} \in S[\Delta X^0_{11}]$, $\Delta X^0_{11} \in S[\Delta T_7]$ that hold with probability $(\frac{7}{16})^{11} = 2^{-13.119}$.

4 Impossible Differential Key-Recovery Attack on 27-Round T-TWINE-128

In this section, we present the first attack on 27-round T-TWINE-128 in the chosen-tweak model. We use the notion of data structures to generate enough pairs of messages to launch the attack. Our utilized structure takes all the possible values of the 12 nibbles $X^0_2$, $X^0_3$, $X^0_4$, $X^0_5$, $X^0_6$, $X^0_7$, $X^0_8$, $X^0_9$, $X^0_{10}$, $X^0_{11}$, $X^0_{12}$, $X^0_{13}$, $X^0_{15}$ while the remaining nibbles assume a fixed value. In addition, we choose the tweak $T_2$ such that it takes all its possible values. Thus, one structure generates $2^{14 \times 13} \times (2^{14 \times 13} - 1)/2 \approx 2^{103}$ possible pairs. Hence, we have $2^{103}$ possible pairs of messages satisfying the plaintext differences. In addition, we utilize the following pre-computation tables in order to efficiently extract/filter the round keys involved in the analysis rounds:

- $H_1$: For all the $2^{20}$ possible values of $X^1_1$, $\Delta X^1_1$, $X^1_4$, $t^0_0$ and $RK^0_0 = K_3$, compute $X^0_2$, $\Delta X^0_2$, $X^0_3$, and $\Delta X^0_3$. Then, store $X^0_1$, $\Delta X^0_1$, $X^0_4$, and $RK^0_0 = K_3$ in $H_1$ indexed by $X^0_2$, $\Delta X^0_2$, $X^0_3$, $\Delta X^0_3$, and $t^0_0$. $\Delta X^0_3$ is chosen such that $\Delta X^0_3 \in S[\Delta X^0_2]$, see Observation 3. Therefore, $H_1$ has $7 \times 2^{16}$ rows and on average about $2^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

- $H_2$: For all the $2^{20}$ possible values of $X^1_3$, $\Delta X^1_3$, $X^1_8$, $t^0_3$, and $RK^0_3 = K_{15}$, compute $X^0_6$, $\Delta X^0_6$, $X^0_7$, and $\Delta X^0_7$. Then, store $X^1_3$, $\Delta X^1_3$, $X^1_8$, and $RK^0_3 = K_{15}$ in $H_1$ indexed by $X^0_6$, $\Delta X^0_6$, $X^0_7$, $\Delta X^0_7$, and $t^0_3$. $\Delta X^0_7$ is chosen such that $\Delta X^0_7 \in S[\Delta X^0_6]$, see Observation 3. Therefore, $H_2$ has $7 \times 2^{16}$ rows and on average about $2^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

- $H_3$: For all the $2^{16}$ possible values of $X^1_{10}$, $\Delta X^1_{15}$, $X^1_{15}$, and $RK^0_6 = K_{28}$, compute $X^0_{12}$, $\Delta X^0_{12}$, $X^0_{13}$, and $\Delta X^0_{13}$. Then, store $X^1_{10}$, $\Delta X^1_{15}$, $X^1_{15}$, and $RK^0_6 = K_{28}$ in $H_3$ indexed by $X^0_{12}$, $\Delta X^0_{12}$, $X^0_{13}$, and $\Delta X^0_{13}$. $\Delta X^0_{13}$ is chosen such that $\Delta X^0_{13} \in S[\Delta X^0_{12}]$, see Observation 3. Therefore, $H_3$ has $7 \times 2^{12}$ rows and on average about $2^{16}/(7 \times 2^{12}) = 16/7$ values in each row.
Fig. 3. Impossible differential attack on 27-round T-TWINE-128
Fig. 4. Impossible differential attack on 25-round T-TWINE-80
\(-H_4:\) For all the \(2^{32}\) possible values of \(X^1_2, \Delta X^2_2, X^2_4, t^1_4, RK^1_4 = K_7, X^1_9, t^0_9, \) and \(RK^5_0 = K_{18},\) compute \(X^1_3 = X^0_6, \Delta X^1_3 = \Delta X^0_6, X^0_{10}, X^1_{11}, \) and \(\Delta X^1_{11}.\) Then, store \(X^1_3, \Delta X^2_3, X^4_4, RK^1_4 = K_7, X^1_9, \) and \(RK^5_0 = K_{18}\) in \(H_4\) indexed by \(X^1_3 = X^0_6, \Delta X^1_3 = \Delta X^0_6, X^0_{10}, X^1_{11}, \Delta X^1_{11}, t^1_4, \) and \(t^0_1, \Delta X^1_6\) is chosen such that \(\Delta X^6_0 \in S[\Delta X^1_{11}],\) see Observation 3. Therefore, \(H_4\) has \(7 \times 2^{24}\) rows and on average about \(2^{32}/(7 \times 2^{24}) = (16/7) \times 2^4\) values in each row.

\(-H_5:\) For all the \(2^{40}\) possible values of \(X^3_2, \Delta X^2_2, X^2_4, t^1_3, RK^1_3 = K_{19}, X^1_{13}, \Delta X^1_{13}, t^0_2, \Delta T_2,\) and \(RK^4_0 = K_{17},\) compute \(X^1_4, \Delta X^1_4, X^8_8, \Delta X^8_8, X^6_9, \) and \(\Delta X^6_9.\) Then, store \(X^2_4, \Delta X^2_3, X^8_8, RK^1_3 = K_{19}, X^1_{13}, \Delta X^1_{13}, \) and \(RK^4_0 = K_{17}\) in \(H_5\) indexed by \(X^1_4, \Delta X^1_4, X^8_8, \Delta X^8_8, X^9_9, \Delta X^9_9, t^1_3, t^0_2,\) and \(t^2_2.\) \(H_5\) has \(2^{36}\) rows and on average about \(2^{40}/2^{36} = 2^4\) values in each row.

\(-H_6:\) For all the \(2^{44}\) possible values of \(X^3_0, X^3_3, \Delta X^3_3, t^2_5, RK^0_2 = K_{10}, X^2_5, t^5_1, RK^1_5 = K_6, X^1_4, t^0_5,\) and \(RK^0_4 = K_2,\) compute \(X^2_1, \Delta X^1_2 = \Delta X^0_{11}, X^1_1 = X^2_1, \Delta X^1_1 = \Delta X^0_{12}, X^0_{10}, \) and \(X^1_0.\) Then, store \(X^3_5, \Delta X^3_5, RK^2_0 = K_{10}, X^2_5, RK^0_0 = K_6, X^1_4, \) and \(RK^0_4 = K_2\) in \(H_6\) indexed by \(X^1_2, \Delta X^1_2 = \Delta X^1_{11}, X^1_1 = X^0_4, \Delta X^1_1 = \Delta X^0_{12}, X^0_{10}, \) and \(X^1_0.\) \(H_6\) has \(2^{24}\) rows and on average about \(2^{42}/2^{24} = 2^8\) values in each row.

\(-H_7:\) For all the \(2^{32}\) possible values of \(X^2_9, \Delta X^2_9, X^2_5, \Delta X^2_{12}, RK^6_6 = K_1 + S(K_0), X^1_4, \Delta X^1_4, \) and \(RK^1_3 = K_{12},\) compute \(X^1_{13}, \Delta X^1_{13}, X^4_4, \Delta X^4_4, X^6_5, \) and \(\Delta X^6_9.\) Then, store \(X^2_9, \Delta X^2_9, X^2_5, \Delta X^2_{12}, RK^6_6 = K_1 + S(K_0), X^1_4, \Delta X^1_4,\) and \(RK^1_3 = K_{12}\) in \(H_7\) indexed by \(X^1_{13}, \Delta X^1_{13}, X^4_4, \Delta X^4_4, X^6_5, \) and \(\Delta X^6_9.\) \(H_7\) has \(2^{24}\) rows and on average about \(2^{42}/2^{24} = 2^8\) values in each row.

\(-H_8:\) For all the \(2^{36}\) possible values of \(X^2_{12}, \Delta X^2_{12}, X^2_4, \Delta X^2_4, t^1_0, RK^7_4 = K_0, X^1_{11}, t^0_6,\) and \(RK^0_7 = K_{31},\) compute \(X^1_{15}, \Delta X^1_{15}, X^4_4, \Delta X^4_4, X^6_5, \) and \(\Delta X^6_9.\) Then, store \(X^2_{12}, \Delta X^2_{12}, X^2_4, \Delta X^2_4, RK^7_4 = K_0, X^1_{11}, \) and \(RK^0_7 = K_{31}\) in \(H_8\) indexed by \(X^1_{15}, \Delta X^1_{15}, X^4_4, \Delta X^4_4, X^6_5, \) and \(t^0_6.\) \(H_8\) has \(2^{28}\) rows and on average about \(2^{36}/2^{28} = 2^8\) values in each row.

\(-H_9:\) For all the \(2^{20}\) possible values of \(X^2_3, X^9_9, \Delta X^3_3, t^2_1,\) and \(RK^2_5 = K_{26},\) compute \(X^2_{10}, \Delta X^2_{10}, X^2_2, \) and \(\Delta X^2_{11}.\) Then, store \(X^3_3, \Delta X^3_3,\) and \(RK^2_5 = K_{26}\) in \(H_9\) indexed by \(X^2_{10}, \Delta X^2_{10}, X^2_2, \) and \(\Delta X^2_{11}.\) \(H_9\) has \(2^{20}\) rows and on average about \(2^{20}/2^{20} = 1\) value in each row.

\(-H_{10}:\) For all the \(2^{20}\) possible values of \(X^3_1, \Delta X^3_1, X^3_3, t^0_2,\) and \(RK^2_7 = K_4 + S(K_{16}),\) compute \(X^3_{14}, \Delta X^3_{14}, X^2_7, \) and \(\Delta X^2_{15}.\) Then, store \(X^3_{11}, \Delta X^3_{11}, X^3_{14},\) and \(RK^2_7 = K_4 + S(K_{16})\) in \(H_{10}\) indexed by \(X^3_{14}, \Delta X^3_{14}, X^2_7, \) and \(\Delta X^2_{15}.\) \(H_{10}\) has \(2^{20}\) rows and on average about \(2^{20}/2^{20} = 1\) value in each row.

\(-H_{11}:\) For all the \(2^{40}\) possible values of \(X^2_4, \Delta X^4_4, X^2_4, \Delta X^2_4, t^2_1, \) and \(RK^3_7 = K_1, X^2_9, t^1_1,\) and \(RK^3_1 = K_{22},\) compute \(X^3_3, \Delta X^3_3, X^3_3, \Delta X^2_3, X^1_{10},\) and \(X^1_{11}.\) Then, store \(X^4_4, \Delta X^2_4, RK^3_3 = K_{24}, RK^3_1 = K_{11},\) and \(RK^3_0 = K_{22}\) in \(H_{11}\) indexed by \(X^3_3, \Delta X^3_3, X^3_3, \Delta X^2_3, X^1_{10}, X^1_{11}, t^2_1,\) and \(t^1_1.\) \(H_{11}\) has \(2^{32}\) rows and on average about \(2^{40}/2^{32} = 2^8\) values in each row.

\(-H_{12}:\) For all the \(2^{12}\) possible values of \(X^2_7, X^2_{12},\) and \(RK^2_1 = K_{16},\) compute \(X^3_4,\) and \(X^3_5.\) Then, store \(X^3_7, X^3_2,\) and \(RK^3_5 = K_{16}\) in \(H_{12}\) indexed by \(X^1_{11},\) and \(X^1_{15}.\) \(H_{12}\) has \(2^8\) rows and on average about \(2^{12}/2^8 = 2^4\) value in each row.
For all the $2^{16}$ possible values of $X_0^2$, $X_3^2$, $t_1^2$, and $RK_1^4 = K_{21}$, compute $X_8^1$, and $X_9^1$. Then, store $X_8^2$, $X_{13}^2$, and $RK_1^4 = K_{21}$ in $H_{13}$ indexed by $X_8^1$, $X_9^1$, and $t_1^2$. $H_{13}$ has $2^{12}$ rows and on average about $2^{16}/2^{12} = 2^4$ value in each row.

For all the $2^{28}$ possible values of $X_2^4$, $X_9^4$, $t_1^4$, $\Delta T_2$, $RK_1^5 = K_{30}$, $X_5^3$, and $RK_2^5 = K_5 + S(K_4 + S(K_{16}))$, compute $X_{11}^3$, $\Delta X_{11}^3$, $X_2^3$, and $X_7^3$. Then, store $RK_3^5 = K_{30}$, and $RK_4^5 = K_5 + S(K_4 + S(K_{16}))$ in $H_{14}$ indexed by $X_{11}^3$, $\Delta X_{11}^3$, $X_{12}^3$, $t_1^3$, $\Delta T_2$, and $X_{13}^3$. $H_{14}$ has $2^{24}$ rows and on average about $2^{28}/2^{24} = 2^4$ values in each row.

For all the $2^{44}$ possible values of $X_3^5$, $\Delta X_3^5$, $X_8^5$, $t_1^5$, $RK_1^6 = K_{31} + S(K_7)$, $X_3^4$, $X_4^4$, $RK_3^4 = K_{29}$, $X_3^1$, $t_1^3$, and $RK_2^3 = K_{23} + S(K_{30})$, compute $X_7^4$, $\Delta X_7^4$, $X_8^3$, $\Delta X_8^3$, $X_6^3$, and $X_7^3$. Then, store $X_3^5$, $\Delta X_3^5$, $RK_4^4 = K_{29}$, and $RK_3^4 = K_{23} + S(K_{30})$ in $H_{15}$ indexed by $X_4^1$, $\Delta X_4^1$, $X_3^3$, $\Delta X_3^3$, $X_6^2$, $X_7^2$, and $t_1^2$. Then, store $RK_3^4 = K_{31} + S(K_7)$. $H_{15}$ has $2^{40}$ rows and on average about $2^{44}/2^{40} = 2^4$ values in each row.

For all the $2^{40}$ possible values of $X_6^5$, $X_6^5$, $t_1^5$, $\Delta T_3$, $RK_1^7 = K_{23} + S(K_{30})$, $X_9^5$, $X_9^5$, $RK_4^5 = K_3$, $X_{11}^5$, $RK_5^3 = K_9 + S(K_8 + S(K_{20}))$, $X_3^7$, and $RK_2^5 = K_{20}$, compute $X_5^3$, $\Delta X_5^3$, $X_4^3$, $X_3^1$, $X_2^1$, and $X_7^5$. Then, store $RK_5^7 = K_3$, $RK_6^7 = K_5 + S(K_8 + S(K_{20}))$, and $RK_2^5 = K_{20}$ in $H_{16}$ indexed by $X_3^3$, $\Delta X_3^3$, $X_4^3$, $X_5^3$, $X_4^2$, $X_2^2$, $RK_5^5 = K_{23} + S(K_{30})$, $RK_4^5 = K_3$, $t_1^4$, $\Delta T_2$, and $t_1^4$. $H_{16}$ has $2^{44}$ rows and on average about $2^{48}/2^{44} = 2^4$ values in each row.

For all the $2^{20}$ possible values of $X_1^{14}$, $\Delta X_1^{14}$, $X_4^{14}$, $t_1^5$, and $RK_1^{26} = f_1(K_0, K_1, K_4, K_5, K_6, K_7, RK_3^3, K_{10}, K_{16}, K_{17}, K_{18}, K_{19}, K_{20}, K_{21}, K_{28}, K_{29}, K_{30})$, compute $X_2^{14}$, $\Delta X_2^{14}$, $X_7^{14}$, and $\Delta X_7^{14}$. Then, store $X_1^{14}$ and $\Delta X_1^{14}$ in $H_{17}$ indexed by $X_1^{14}$, $\Delta X_1^{14}$, $X_7^{14}$, $\Delta X_7^{14}$, $RK_1^{26}$, and $t_1^{26}$. $\Delta X_1^{14}$ is chosen such that $\Delta X_1^{27} \in S(\Delta X_7^{14})$, see Observation 3. Therefore, $H_{17}$ has $7 \times 2^{20}$ rows and on average about $2^{20}/(7 \times 2^{20}) = (16/7) \times 2^{-4}$ values in each row.

For all the $2^{20}$ possible values of $X_0^{26}$, $X_3^{26}$, $t_1^{26}$, $\Delta T_2$, and $RK_0^{26} = f_2(K_0, K_1, K_3, K_{16}, K_{20}, K_{21}, RK_0^3, K_{27}, K_{28})$, compute $X_0^{27}$, $\Delta X_1^{27}$, and $X_7^{27}$. Then, store $RK_1^{26}$ in $H_{18}$ indexed by $X_7^{27}$, $\Delta X_1^{27}$, $X_0^{27}$, $t_1^{26}$, and $\Delta T_2$. $\Delta X_1^{27}$ is chosen such that $\Delta X_1^{27} \in S(\Delta T_2)$, see Observation 3. Therefore, $H_{18}$ has $7 \times 2^{16}$ rows and on average about $2^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

For all the $2^{20}$ possible values of $X_{10}^{25}$, $X_{11}^{25}$, $t_1^{25}$, $RK_2^{25} = f_3(K_0, K_1, K_2, K_4, K_{12}, K_{13}, RK_8^6, K_{15}, K_{16}, K_{20}, K_{21}, K_{24}, K_{28})$, $X_8^2$, $t_2^2$, and $RK_3^4 = f_4(K_0, K_4, K_5, K_{11}, K_{16}, K_{24})$, compute $X_2^{27}$, $X_7^{27}$, and $X_3^{27}$. Then, store $X_2^{27}$ and $RK_3^{25}$ in $H_{19}$ indexed by $X_2^{27}$, $X_9^3$, $X_8^3$, $RK_3^4$, $t_1^{27}$, and $t_2^2$. $H_{19}$ has $2^{24}$ rows and on average about $2^{28}/2^{24} = 2^4$ values in each row.

For all the $2^{24}$ possible values of $X_{14}^{24}$, $X_{15}^{24}$, $t_0^{24}$, $\Delta T_2$, $RK_4^{25} = f_5(K_0, K_1, K_2, K_{10}, K_{11}, K_{12}, K_{13}, RK_0^3, K_{20}, K_{21}, K_{22}, K_{24}, K_{28}, K_{29}, K_{30})$, $X_5^{25}$, $t_0^{25}$, $RK_7^{25} = f_6(K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_{12}, K_{13}, K_{14}, K_{15}, K_{16}, K_{17}, K_{24}, K_{25}, K_{26}, K_{28})$, $X_{16}^{26}$, $t_1^{26}$, and $RK_5^6 = f_7(K_0, K_1, K_4, K_5, K_6, K_{12}, K_{13}, K_{16}, K_{17}, K_{19}, K_{20}, K_{24}, K_{25}, K_{27}, K_{28})$, compute $X_1^{26}$, $X_{11}^{26}$, $\Delta X_1^{26}$, $X_{13}^{26}$, $\Delta X_{13}^{26}$, $X_{10}^{26}$, $t_0^{26}$, $\Delta T_2$, $RK_2^{24}$, $t_2^{25}$, and $t_1^{26}$. $\Delta X_{14}^{26}$ and
\( \Delta X_{11}^{27} \) are chosen such that \( \Delta X_{14}^{27} \in S[\Delta X_{11}^{27}] \) and \( \Delta X_{11}^{27} \in S[\Delta T_2] \), respectively, see Observation 3. Therefore, \( H_{19} \) has \( 7^2 \times 2^{36} \) rows and on average about \( 2^{244}/(7^2 \times 2^{36}) = (16/7)^2 \) values in each row.

In the general approach, the round keys involved in the analysis rounds are guessed and the plaintext/ciphertext pairs are filtered to satisfy the differential path leading to the impossible differential distinguisher. Here, we use the above proposed pre-computation tables to deduce the round keys that lead a specific pair of plaintext/ciphertext to the impossible differential. Then, we exclude the deduced keys as they are wrong keys. Our attack proceeds as follows. We initialize an array \( H \) of \( 2^{31} \times 4 = 124 \) entries to “0”, where each entry is 1-bit and the index of the array is 31 key nibbles involved in the attack, as we will see later. Then we generate \( 2^m \) structures as described above. Therefore, we have \( 2^{m+103} \) pairs of plaintext/ciphertext pairs generated using \( 2^{m+48} \) chosen plaintexts. Then, we ask the encryption oracle for their corresponding ciphertexts. The plaintext/ciphertext pairs that satisfy Observation 3 are \( 2^{m+103} \times 2^{-10.734} = 2^{m+92.266} \) pairs. After the ciphertext filtration, we have only \( 2^{m+92.266} \times 2^{-12 \times 4} = 2^{m+44.266} \) remaining pairs. For each remaining pair, we access the pre-computation tables in sequential order from table \( H_1 \) to \( H_{20} \) one by one in order to deduce 31 key nibbles that lead each remaining pair of plaintext/ciphertext to the impossible differential. Then, we mark them in \( H \) as invalid “1”. Table 3 summarize these steps by identifying which table will be used and which key nibble is involved in this step in addition to the time complexity of each step.

Remarks on the analysis steps:

1. During steps 1–14 and step 18, we directly access the corresponding table to obtain the values of the involved key nibbles. For example, in step 1, we determine the number of possible values of \( RK_0^1 = K_3 \) that satisfy the path to the impossible differential by accessing \( H_1 \). Therefore, we have \((16/7)\) possible values for \( K_3 \).

2. During steps 15, 16, 17, 19, and 20, and because some combinations of the key nibbles determined during the previous steps are used in the indexing of the tables \( H_{15} \) to \( H_{20} \), we firstly deduce these indices and then access the corresponding table. For example, during step 15, we deduce the value of \( RK_3^4 = K_{31} + S(K_7) \) that is used in the indexing of table \( H_{15} \), then determine the number of possible values of \( RK_4^3 = K_{29} \) and \( RK_3^2 = K_{23} + S(K_{30}) \) that satisfy the path by accessing \( H_{15} \). After that, the value of \( RK_3^4 = K_{23} + S(K_{30}) \) is used to deduce the value of \( K_{23} \) using the determined value of \( K_{30} \) from Step 14.

3. During steps 7 and 8, we determine the possible values of \( RK_6^1 = K_1 + S(K_0) \) and \( RK_7^1 = K_0 \), respectively. Therefore, after step 8, we can deduce the values of \( K_1 \). In the same manner, we can deduce the values of \( K_4 \) and \( K_5 \) after steps 10, 12 and 14 where we determine the values of \( RK_7^2 = K_4 + S(K_{16}) \) and \( RK_6^2 = K_5 + S(K_4 + S(K_{16})) \), respectively.
4. During step 17, we deduce the value of $RK_7^{26} = f_1(K_0, K_1, K_4, K_5, K_6, K_7, RK_6^3, K_{10}, K_{16}, K_{17}, K_{18}, K_{19}, K_{20}, K_{21}, K_{28}, K_{29}, K_{30})$, then determine the values of $X_{11}^6$ and $\Delta X_{24}^6$ that satisfy the path by accessing $H_{17}$. Therefore, no new key nibbles are involved during this step but there is a filtration of some keys.

5. During steps 18 and 19, we can determine the values of $RK_9^{26} = f_2(K_0, K_1, K_3, K_{16}, K_{20}, K_{21}, RK_6^3, K_{27}, K_{28})$ and $RK_5^{25} = f_3(K_0, K_1, K_2, K_4, K_{12}, K_{13}, RK_6^3, K_{15}, K_{16}, K_{20}, K_{21}, K_{24}, K_{28})$, respectively. Therefore, we can deduce the values of $K_{27}$ and $K_{13}$, respectively, since all the other key nibbles in $f_2$ and $f_3$ are determined during the previous steps.

6. After step 20, we have $2^{60} \times (16/7)^9$ possible values for $K_0, K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_9 + S(K_8 + S(K_{20})), K_{10}, K_{11}, K_{12}, K_{13}, K_{15}, K_{16}, K_{17}, K_{18}, K_{19}, K_{20}, K_{21}, K_{22}, K_{23}, K_{24}, K_{26}, K_{27}, K_{28}, K_{29}, K_{30}, K_{31}, RK_7^{25} = f_6(K_{14}, K_{25}), RK_5^{26} = f_7(K_8, K_{25})$. Hence, we marks them in $H$ as invalid “1” in step 21.

**Attack Complexity.** As depicted in Fig. 3, we have 37 round keys involved in the analysis rounds. According to the key schedule, these 37 round keys take only $2^{124}$ possible values (see step 21 in Table 3). As mentioned in step 21, we remove on average $2^{60} \times (16/7)^9 = 2^{70.734}$ out of $2^{124}$ possible values of these 37 round keys involved in the attack for each pair of the $2^{m+44.266}$ remaining pairs. Hence, a wrong key is not discarded using one pair with probability $1 - 2^{70.734-124} = 1 - 2^{-53.266}$. Therefore, we have $2^{124} \times (1 - 2^{-53.266})^{2^{m+44.266}} \approx 2^{124} \times (e^{-1})^{2^{m+44.266}-53.266} \approx 2^{124} \times 2^{-1.4 \times 2^m-9}$ remaining candidates for 124-bit of the key, after processing all the $2^{m+44.266}$ remaining pairs. We evaluated the computational complexity of the attack as a function of $m$, as illustrated in Table 3, to determine the optimal value of $m$ that leads to the best computational complexity. As steps 20 and 21 dominate the time complexity of the attack, see Table 3, we choose $m = 12$ in order to optimize the time complexity of the attack. Therefore, we have $2^{124} \times 2^{-1.4 \times 2^{12-9-3}} = 2^{124-11.2} = 2^{112.8}$ remaining candidates for 124-bit of the key. The remaining key nibbles can be retrieved by guessing $K_8$ and exhaustively searching the $2^{112.8}$ remaining key candidates using 2 plaintext/ciphertext pairs. This step requires $2 \times 2^4 \times 2^{112.8} = 2^{117.8}$ encryptions. Therefore, the time complexity of the attack is $2^{120.245} + 2^{119.245} + 2^{117.8} \approx 2^{120.83}$ encryptions. The data complexity of the attack is $2^{m+4 \times 13} = 2^{64}$ chosen tweak/plaintext combinations that can be generated using $2^{m+48} = 2^{60}$ chosen plaintexts. The memory complexity of the attack is dominated by the memory that is required to store $H$. Hence, the memory complexity is $2^{124} \times 2^{-6} = 2^{118}$ 64-bit blocks.
5 Impossible Differential Key-Recovery Attack on 25-Round T-TWINE-80

In this section, we present the first attack on 25-round T-TWINE-80 in the chosen-tweak model. We use the notion of data structures to generate enough pairs of messages to launch the attack. Our utilized structure takes all the possible values in 7 nibbles $X_0^T$, $X_1^T$, $X_3^T$, $X_{10}^T$, $X_{11}^T$, $X_{14}^T$, $X_{15}^T$ while the remaining nibbles take a fixed value. In addition, we choose the tweak $T_7$ such that it takes all the values. Thus, one structure generates $2^{4x8} \times (2^{4x8} - 1)/2 \approx 2^{63}$ possible pairs. Hence, we have $2^{63}$ possible pairs of messages satisfying the plaintext differences. In addition, we utilize the following pre-computation tables in order

Table 3. Time complexity of the different steps of the attack on 27-round T-TWINE-128, where NK denotes the number of keys to be excluded.

| Step | Table | Key nibbles | Time complexity (in 27-round encryptions) | NK | $m = 12$ |
|------|-------|-------------|------------------------------------------|----|---------|
| 1    | $H_1$ | $K_3$       | $2^{m+44} \times (16/7) \times \frac{4}{8 \times 27} \approx 2^{m+39.704}$ | (16/7) | 251.704 |
| 2    | $H_2$ | $K_{15}$    | $2^{m+44} \times (16/7)^2 \times \frac{4}{8 \times 27} \approx 2^{m+40.896}$ | (16/7)$^2$ | 252.896 |
| 3    | $H_3$ | $K_{28}$    | $2^{m+44} \times (16/7)^3 \times \frac{4}{8 \times 27} \approx 2^{m+42.089}$ | (16/7)$^3$ | 254.089 |
| 4    | $H_4$ | $K_7, K_{18}$ | $2^{m+44} \times 2^4 \times (16/7)^4 \times \frac{6}{8 \times 27} \approx 2^{m+47.867}$ | $2^4 \times (16/7)^4$ | 259.867 |
| 5    | $H_5$ | $K_{17}, K_{19}$ | $2^{m+44} \times 2^8 \times (16/7)^4 \times \frac{7}{8 \times 27} \approx 2^{m+52.089}$ | $2^8 \times (16/7)^4$ | 264.089 |
| 6    | $H_6$ | $K_2, K_6, K_{10}$ | $2^{m+44} \times 2^{16} \times (16/7)^5 \times \frac{8}{8 \times 27} \approx 2^{m+61.282}$ | $2^{16} \times (16/7)^5$ | 273.282 |
| 7    | $H_7$ | $K_1 + S(K_0), K_{12}$ | $2^{m+44} \times 2^{24} \times (16/7)^5 \times \frac{8}{8 \times 27} \approx 2^{m+69.474}$ | $2^{24} \times (16/7)^5$ | 281.474 |
| 8    | $H_8$ | $K_0, K_1, K_{31}$ | $2^{m+44} \times 2^{32} \times (16/7)^5 \times \frac{8}{8 \times 27} \approx 2^{m+77.282}$ | $2^{32} \times (16/7)^5$ | 289.282 |
| 9    | $H_9$ | $K_{26}$ | $2^{m+44} \times 2^{32} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+76.059}$ | $2^{32} \times (16/7)^5$ | 288.059 |
| 10   | $H_{10}$ | $K_4 + S(K_{16})$ | $2^{m+44} \times 2^{32} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+76.474}$ | $2^{32} \times (16/7)^5$ | 288.474 |
| 11   | $H_{11}$ | $K_{11}, K_{22}, K_{24}$ | $2^{m+44} \times 2^{40} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+84.796}$ | $2^{40} \times (16/7)^5$ | 296.796 |
| 12   | $H_{12}$ | $K_4, K_{16}$ | $2^{m+44} \times 2^{44} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+88.059}$ | $2^{44} \times (16/7)^5$ | 300.059 |
| 13   | $H_{13}$ | $K_{21}$ | $2^{m+44} \times 2^{48} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+92.059}$ | $2^{48} \times (16/7)^5$ | 304.059 |
| 14   | $H_{14}$ | $K_5, K_{30}$ | $2^{m+44} \times 2^{52} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+95.474}$ | $2^{52} \times (16/7)^5$ | 307.474 |
| 15   | $H_{15}$ | $K_{23}, K_{29}$ | $2^{m+44} \times 2^{56} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+100.474}$ | $2^{56} \times (16/7)^5$ | 312.474 |
| 16   | $H_{16}$ | $R K_{3}^{7} + S(K_8 + S(K_{20}))$, $K_{20}$ | $2^{m+44} \times 2^{60} \times (16/7)^5 \times \frac{9}{8 \times 27} \approx 2^{m+104.059}$ | $2^{60} \times (16/7)^5$ | 316.059 |
| 17   | $H_{17}$ | $-$ | $2^{m+44} \times 2^{56} \times (16/7)^6 \times \frac{9}{8 \times 27} \approx 2^{m+100.667}$ | $2^{56} \times (16/7)^6$ | 312.667 |
| 18   | $H_{18}$ | $K_{27}$ | $2^{m+44} \times 2^{56} \times (16/7)^7 \times \frac{9}{8 \times 27} \approx 2^{m+100.860}$ | $2^{56} \times (16/7)^7$ | 312.860 |
| 19   | $H_{19}$ | $K_{13}$ | $2^{m+44} \times 2^{60} \times (16/7)^7 \times \frac{9}{8 \times 27} \approx 2^{m+105.860}$ | $2^{60} \times (16/7)^7$ | 317.860 |
| 20   | $H_{20}$ | $R K_{3}^{k_5} + f_5(K_{14}, K_{25}), R K_{5}^{k_7} = f_7(K_8, K_{25})$ | $2^{m+44} \times 2^{60} \times (16/7)^9 \times \frac{9}{8 \times 27} \approx 2^{m+108.245}$ | $2^{60} \times (16/7)^9$ | 320.245 |
| 21   | $H$ | $-$ | $2^{m+44} \times 2^{60} \times (16/7)^9 \times \frac{1}{8 \times 27} \approx 2^{m+107.245}$ | $2^{60} \times (16/7)^9$ | 319.245 |
to efficiently extract/filter the round keys involved in the analysis rounds. Note that, for the 7 round keys that are involved in the 3 rounds below the distinguisher, we wrote them as 7 functions $f_1, f_2, f_3, f_4, f_5, f_6, f_7$ of the key nibbles that are not involved in the above analysis rounds, $K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13}$, and ignored the other key nibbles as they are known.

- $H_1$: For all the 2$^{20}$ possible values of $X_0^1, X_1^1, \Delta X_1^1, t_0^1$ and $RK_0^1 = K_1$, compute $X_0^0, \Delta X_0^0, X_1^0$, and $\Delta X_0^0$. Then, store $X_1^1, \Delta X_1^1, \Delta X_0^0$, and $t_0^1$. $\Delta X_0^0$ is chosen such that $\Delta X_0^0 \in S[\Delta X_0^0]$, see Observation 4. Therefore, $H_1$ has 7 $\times$ 2$^{16}$ rows and on average about 2$^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

- $H_2$: For all the 2$^{20}$ possible values of $X_2^1, X_3^1, \Delta X_3^1, t_1^1$, and $RK_0^1 = K_{14}$, compute $X_0^2, X_2^1, X_3^1, \Delta X_0^2, \Delta X_2^1, \Delta X_3^1$, and $\Delta X_2^1$. Then, store $X_1^1, X_2^1, X_3^1, and$ $RK_0^1 = K_{14}$ in $H_2$ indexed by $X_0^2, \Delta X_0^2, X_1^2, X_2^1, X_3^1$, and $t_1^1$. $\Delta X_2^1$ is such that $\Delta X_2^1 \in S[\Delta X_2^1]$, see Observation 4. Therefore, $H_2$ has 7 $\times$ 2$^{16}$ rows and on average about 2$^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

- $H_3$: For all the 2$^{20}$ possible values of $X_1^1, \Delta X_1^1, X_1^4, t_0^4$, and $RK_0^1 = K_{16}$, compute $X_0^1, \Delta X_0^1, X_1^1, \Delta X_2^1$, and $\Delta X_0^1$. Then, store $X_1^1, \Delta X_1^1, X_1^4$, and $RK_0^1 = K_{16}$ in $H_3$ indexed by $X_0^1, \Delta X_0^1, X_1^4, \Delta X_2^1$, and $t_0^4$. $\Delta X_0^1$ is chosen such that $\Delta X_0^1 \in S[\Delta X_0^1]$, see Observation 4. Therefore, $H_3$ has 7 $\times$ 2$^{16}$ rows and on average about 2$^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

- $H_4$: For all the 2$^{28}$ possible values of $X_2^1, X_3^1, \Delta X_3^1, t_1^1, \Delta T_7, RK_0^1 = K_{18}$, $X_1^1$, and $RK_0^1 = K_{16}$, compute $X_0^1 = X_1^1, \Delta X_1^1 = \Delta X_2^1 = X_1^4, X_1^2$, and $X_1^3$. Then, store $X_0^1, X_1^2, X_1^3, RK_0^1 = K_{18}$, and $RK_0^1 = K_{16}$ in $H_4$ indexed by $X_0^1 = X_1^1, \Delta X_1^1 = \Delta X_2^1 = X_1^4, X_1^2$, and $X_1^3$. Then, store $RK_0^1 = K_{18}$ and $RK_0^1 = K_{16}$ in $H_5$ indexed by $X_1^1, \Delta X_1^1, X_1^2, X_1^3$, and $t_1^1$, and $\Delta T_7, \Delta X_1^1$ is chosen such that $\Delta X_1^1 \in S[\Delta T_7]$, see Observation 4. Therefore, $H_4$ has 7 $\times$ 2$^{20}$ rows and on average about 2$^{28}/(7 \times 2^{20}) = (16/7) \times 2^4$ values in each row.

- $H_5$: For all the 2$^{28}$ possible values of $X_2^1, X_3^1, \Delta T_7, RK_0^1 = K_{18}, X_1^1$, and $RK_0^1 = K_{16}$, compute $X_0^1 = X_1^1, \Delta X_1^1 = \Delta X_2^1 = X_1^4, X_1^2$, and $X_1^3$. Then, store $RK_0^1 = K_{18}$ and $RK_0^1 = K_{16}$ in $H_5$ indexed by $X_1^1, \Delta X_1^1, X_1^2, X_1^3$, and $t_1^1$, and $\Delta T_7, \Delta X_1^1$ is chosen such that $\Delta X_1^1 \in S[\Delta T_7]$, see Observation 4. Therefore, $H_5$ has 7 $\times$ 2$^{20}$ rows and on average about 2$^{28}/(7 \times 2^{20}) = (16/7) \times 2^4$ values in each row.

- $H_6$: For all the 2$^{44}$ possible values of $X_3^1, \Delta X_3^1, X_3^3, t_2^3, RK_3^1 = K_{14}, X_2^3, t_1^2, RK_4^1 = K_{17}, X_3^3, t_0^3$, and $RK_0^3 = K_6$, compute $X_2^1, \Delta X_2^1 = \Delta X_0^3, X_1^3$, $\Delta X_0^3 = \Delta X_3^0, X_0^3$, and $X_0^3$. Then, store $X_3^1, \Delta X_3^3, RK_3^1 = K_{14}, RK_1^3 = K_{17}$, and $RK_0^3 = K_6$ in $H_6$ indexed by $X_2^1, \Delta X_2^1 = \Delta X_0^3, X_1^3, \Delta X_0^3 = \Delta X_3^0, X_0^3, X_0^3$, $t_0^3, t_1^2$, and $t_2^3$. $\Delta X_0^3$ is chosen such that $\Delta X_0^3 \in S[\Delta X_0^3]$, see Observation 4. Therefore, $H_6$ has 7 $\times$ 2$^{36}$ rows and on average about 2$^{44}/(7 \times 2^{36}) = (16/7) \times 2^4$ values in each row.

- $H_7$: For all the 2$^{48}$ possible values of $X_4^1, X_4^2, \Delta T_7, RK_1^3 = K_{15}, X_3^3, t_1^2, RK_2^3 = K_3, X_2^2, RK_1^6 = K_{19}, X_1^1$, and $RK_0^2 = K_4$, compute $X_3^3, \Delta X_3^0 = \Delta X_3^3, X_1^4, X_0^4, X_0^3$, and $X_5^0$. Then, store $RK_3^1 = K_{15}, RK_2^3 = K_3, RK_1^6 = K_{19}$, and $RK_2^3 = K_{14}$ in $H_7$ indexed by $X_3^3, \Delta X_0^3 = \Delta X_3^3, X_1^4, X_0^4, X_0^3, \Delta X_0^3 = K_{15}, RK_2^3 = K_3, t_0^4, \Delta T_7$, and $t_0^2$. $\Delta X_1^0$ is chosen such that $\Delta X_1^0 \in S[\Delta T_7]$, see Observation 4. Therefore, $H_7$ has 7 $\times$ 2$^{40}$ rows and on average about 2$^{48}/(7 \times 2^{40}) = (16/7) \times 2^4$ values in each row.
- $H_8$: For all the $2^{20}$ possible values of $X^{24}_0$, $X^{24}_1$, $t^{24}_0$, $\Delta T_7$, and $RK^{24}_0 = f_1(K_0, K_2, K_5, K_9, K_{10}, K_{12}, K_{13})$, compute $X^{25}_0$, $\Delta X^{25}_1$, and $X^{25}_1$. Then, store $RK^{24}_8$ in $H_8$ indexed by $X^{20}_0$, $X^{25}_0$, $X^{25}_1$, $t^{24}_1$, and $\Delta T_7$. $\Delta X^{25}_1$ is chosen such that $\Delta X^{25}_1 \in S[\Delta T_7]$, see Observation 4. Therefore, $H_8$ has $7 \times 2^{16}$ rows and on average about $2^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

- $H_9$: For all the $2^{20}$ possible values of $X^{24}_{14}$, $\Delta X^{24}_{14}$, $X^{24}_{15}$, $t^{24}_0$, and $RK^{24}_7 = f_2(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$, compute $X^{25}_{14}$, $\Delta X^{25}_{14}$, $X^{25}_{15}$, and $\Delta X^{25}_{15}$. Then, store $X^{24}_{14}$, $\Delta X^{24}_{14}$, and $RK^{24}_7 = f_2(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$ in $H_9$ indexed by $X^{25}_{14}$, $\Delta X^{25}_{14}$, $X^{25}_{15}$, and $\Delta X^{25}_{15}$. $\Delta X^{25}_{15}$ is chosen such that $\Delta X^{25}_{15} \in S[\Delta X^{25}_{14}]$, see Observation 4. Therefore, $H_9$ has $7 \times 2^{16}$ rows and on average about $2^{20}/(7 \times 2^{16}) = 16/7$ values in each row.

- $H_{10}$: For all the $2^{22}$ possible values of $X^{23}_{14}$, $\Delta X^{23}_{14}$, $X^{23}_{15}$, $t^{23}_0$, $RK^{23}_7 = f_3(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$, compute $X^{25}_{14} = X^{24}_{14}$, $X^{25}_{15} = X^{24}_{15}$, $\Delta X^{25}_{11}$, and $X^{25}_{10}$. Then, store $X^{23}_{14}$, $\Delta X^{23}_{14}$, $RK^{23}_7 = f_3(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$, and $RK^{23}_5 = f_4(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$ in $H_{10}$ indexed by $X^{25}_{14} = X^{24}_{14}$, $\Delta X^{25}_{14} = \Delta X^{24}_{14}$, $X^{25}_{11}$, $\Delta X^{25}_{10}$, $\Delta X^{25}_{10}$, $t^{23}_0$, and $t^{24}_1$. $\Delta X^{25}_{15}$ is chosen such that $\Delta X^{25}_{15} \in S[\Delta X^{25}_{14}]$, see Observation 4. Therefore, $H_{10}$ has $7 \times 2^{24}$ rows and on average about $2^{32}/(7 \times 2^{24}) = (16/7) \times 2^4$ values in each row.

- $H_{11}$: For all the $2^{44}$ possible values of $X^{22}_{14}$, $X^{15}_{15}$, $t^{22}_0$, $\Delta T_7$, $RK^{22}_7 = f_5(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{12}, K_{13})$, $X^{28}_{10}$, $t^{23}_1$, $RK^{23}_5 = f_6(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$, $X^{28}_{8}$, $t^{24}_1$, and $RK^{24}_7 = f_7(K_0, K_2, K_5, K_9, K_{10}, K_{12}, K_{13})$, compute $X^{23}_{14}$, $\Delta X^{23}_{15} = \Delta X^{23}_{15}$, $X^{25}_{2}$, $X^{25}_{9}$, and $X^{25}_8$. Then, store $RK^{22}_7 = f_5(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$, $RK^{23}_5 = f_6(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$, $RK^{23}_5 = f_6(K_0, K_2, K_5, K_7, K_9, K_{10}, K_{11}, K_{12}, K_{13})$, and $RK^{24}_7 = f_7(K_0, K_2, K_5, K_9, K_{10}, K_{12}, K_{13})$ in $H_{11}$ indexed by $X^{23}_{14}$, $\Delta X^{23}_{15} = \Delta X^{23}_{15}$, $X^{25}_{2}$, $X^{25}_{9}$, $X^{25}_8$, $t^{22}_0$, $\Delta T_7$, $t^{23}_1$, and $t^{24}_1$. $\Delta X^{25}_{15}$ is chosen such that $\Delta X^{25}_{15} \in S[\Delta T_7]$, see Observation 4. Therefore, $H_{11}$ has $7 \times 2^{22}$ rows and on average about $2^{32}/(7 \times 2^{22}) = (16/7) \times 2^8$ values in each row.

Our attack proceeds as follows. We initialize an array $H$ of $2^{18 \times 4^{7} = 72}$ entries to “0”, where each entry is 1-bit and the index of the array is 16 key nibbles involved in the attack, as we will see later. Then, we generate $2^m$ structures as described above. Therefore, we have $2^{m+63}$ pairs of plaintext/ciphertext pairs generated using $2^{m+28}$ chosen plaintexts. Next, we ask the encryption oracle for their corresponding ciphertexts. The plaintext/ciphertext pairs that satisfy Observation 4 are $2^{m+63} \times 2^{-13.119} = 2^{m+49.881}$ pairs. After the ciphertext filtration, we have only $2^{m+49.881} \times 2^{-12.4} = 2^{m+1.881}$ remaining pairs. For each remaining pair, we perform the following steps:

1. Determine the number of possible values of $RK^0_0 = K_1$ that satisfy the path by accessing $H_1$. Therefore, we have $(16/7)$ possible values for $K_1$.
2. Determine the number of possible values of $RK^0_0 = K_{14}$ that satisfy the path by accessing $H_2$. Therefore, we have $(16/7)^2$ possible values for $K_1, K_{14}$.
3. Determine the number of possible values of $RK^0_0 = K_{16}$ that satisfy the path by accessing $H_3$. Therefore, we have $(16/7)^3$ possible values for $K_1, K_{14}, K_{16}$. 
4. Determine the number of possible values of $RK_2^1 = K_8, RK_0^0 = K_3$ that satisfy the path by accessing $H_4$. Therefore, we have $2^4 \times (16/7)^4$ possible values for $K_1, K_3, K_8, K_{14}, K_{16}$.

5. Determine the number of possible values of $RK_3^1 = K_{18}, RK_0^0 = K_{15}$ that satisfy the path by accessing $H_5$. Therefore, we have $2^8 \times (16/7)^5$ possible values for $K_1, K_3, K_8, K_{14}, K_{15}, K_{16}$.

6. Determine the number of possible values of $RK_3^2 = K_{14}, RK_4^1 = K_{17}, RK_0^0 = K_6$ that satisfy the path by accessing $H_6$. Therefore, we have $2^{12} \times (16/7)^6$ possible values for $K_1, K_3, K_6, K_8, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}$.

7. Determine the number of possible values of $RK_3^3 = K_{15}, RK_2^2 = K_3, RK_6^1 = K_{19}, RK_0^0 = K_4$ that satisfy the path by accessing $H_7$. Therefore, we have $2^{16} \times (16/7)^7$ possible values for $K_1, K_3, K_4, K_6, K_8, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}, K_{19}$.

8. Determine the number of possible values of $RK_0^{24}$ that satisfy the path by accessing $H_8$. Therefore, we have $2^{20} \times (16/7)^8$ possible values for $K_1, K_3, K_4, K_6, K_8, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}, K_{19}, K_2^{24}$.

9. Determine the number of possible values of $RK_7^{24}$ that satisfy the path by accessing $H_9$. Therefore, we have $2^{24} \times (16/7)^9$ possible values for $K_1, K_3, K_4, K_6, K_8, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}, K_{19}, K_0^{24}, K_2^{24}, K_7^{24}, K_5^{24}$. 

10. Determine the number of possible values of $RK_7^{23}, RK_6^{24}$ that satisfy the path by accessing $H_{10}$. Therefore, we have $2^{28} \times (16/7)^{10}$ possible values for $K_1, K_3, K_4, K_6, K_8, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}, K_{19}, K_0^{24}, K_7^{24}, K_2^{23}, K_5^{24}$.

11. Determine the number of possible values of $RK_7^{22}, RK_5^{23}, RK_4^{24}$ that satisfy the path by accessing $H_{11}$. Therefore, we have $2^{28} \times (16/7)^{11}$ possible values for $K_1, K_3, K_4, K_6, K_8, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}, K_{19}, K_0^{24}, K_7^{24}, K_5^{23}, K_2^{22}, K_5^{23}, K_4^{24}$.

12. The deduced $2^{28} \times (16/7)^{11}$ values for 18 key nibbles, $K_1, K_3, K_4, K_6, K_8, K_{14}, K_{15}, K_{16}, K_{17}, K_{18}, K_{19}, K_0^{24}, K_7^{24}, K_5^{23}$, involved in the attack are wrong keys. Hence, mark them in $H$ invalid “1”.

**Attack Complexity.** As depicted in Fig. 4, we have 22 round keys involved in the analysis rounds. According to the key schedule, these 22 round keys take only $2^{72}$ possible values (see step 12 in Table 4). As mentioned in step 12, we remove on average $2^{28} \times (16/7)^{11} = 2^{41.119}$ out of $2^{72}$ possible values of these 22 round keys involved in the attack for each pair of the $2^{m+1.881}$ remaining pairs. Hence, a wrong key is not discarded using one pair with probability $1 - 2^{41.119-72} = 1 - 2^{-30.881}$. Therefore, we have $2^{72} \times (1 - 2^{-30.881})^{2^{m+1.881}} \approx 2^{72} \times (e^{-1})^{2^{m+1.881-30.881}} \approx 2^{72} \times 2^{-1.4 \times 2^{m-29}}$ remaining candidates for 72-bit
of the key, after processing all the $2^{m+1.881}$ remaining pairs. We evaluated the computational complexity of the attack as a function of $m$, as illustrated in Table 4, to determine the optimal value of $m$ that leads to the best computational complexity. As steps 11 and 12 dominate the time complexity of the attack, see Table 4, we choose $m = 33.5$ in order to optimize the time complexity of the attack. Therefore, we have $2^{72} \times 2^{-1.4} \times 2^{31.5-29-4.5} = 2^{72-31.678} = 2^{40.322}$ remaining candidates for 72-bit of the key. These 72-bit of the key include 11 master key nibbles and 7 round key nibbles. To retrieve the whole master key, we perform the following steps:

1. Retrieve $K_{10}$ from $RK_{24}^{1}$ by guessing the 6 key nibbles $K_0, K_2, K_5, K_9, K_{12}, K_{13}$. Since this step includes 18 S-box operations, it requires $2^{40.322+24 = 64.322} \times \frac{18}{8 \times 25} \approx 2^{60.848}$ encryptions. Since $RK_{24}^{4}$ and $RK_{24}^{0}$ are functions in the same nibbles of the master key, we can compute $RK_{24}^{0}$ using the retrieved $K_{10}$ and then match the computed value with its value in the remaining candidate key. As a result, we have 4-bit filtration. Hence, we have only $2^{40.322+24-4 = 60.322}$ remaining key candidates. This step requires $2^{40.322+24 = 64.322} \times \frac{37}{8 \times 25} \approx 2^{61.888}$ encryptions.

2. Using the same technique, retrieve $K_7$ from $RK_{23}^{5}$ by guessing $K_{11}$. This step requires $2^{60.322+4 = 64.322} \times \frac{90}{8 \times 25} \approx 2^{63.167}$ encryptions. Since $RK_{24}^{5}$ is also a function in the same nibbles of the master key, we can compute it using the retrieved $K_7$ and compare it with its value in the remaining candidate. As a result, we have 4-bit filtration. Hence, we have only $2^{60.322+4-4 = 60.322}$ remaining key candidates. This step requires $2^{60.322+4 = 64.322} \times \frac{112}{8 \times 25} \approx 2^{63.485}$. Then, we perform the previous filtration to the following round key nibbles $RK_{22}^{7}$, $RK_{23}^{7}$, and $RK_{24}^{24}$. Finally, we have another 3 4-bit filtrations. Therefore, we have only $2^{60.322-12} = 2^{48.322}$ remaining candidates for the whole master key. The time complexity of this step is dominated by $2^{64.335}$ encryptions.

The right master key can be retrieved by exhaustively searching the $2^{48.322}$ remaining key candidates using 2 plaintext/ciphertext pairs. This step requires $2 \times 2^{48.322} = 2^{49.322}$ encryptions. Therefore, the time complexity of the attack is dominated by steps 11 and 12 in Table 4 which requires $2^{70.441} + 2^{68.856} \approx 2^{70.86}$ encryptions, see Table 4. The data complexity of the attack is $2^{m+4 \times 8} = 2^{65.5}$ chosen tweak/plaintext combinations that can be generated using $2^{m+28} = 2^{61.5}$ chosen plaintexts. The memory complexity of the attack is dominated by the memory that is required to store $H$. Hence, the memory complexity is $2^{72} \times 2^{-6} = 2^{66}$ 64-bit blocks.
6 Conclusion

In this work, we presented two impossible differential attacks against reduced-round versions of T-TWINE. Both attacks use our proposed 18-round impossible differential distinguisher. To the best of our knowledge, this distinguisher is the first valid 18-round distinguisher. Utilizing this distinguisher, we launched 25-round and 27-round attacks on T-WINE-80 and T-TWINE-128, respectively. The presented attacks are the first published attacks against both versions of T-TWINE.

Table 4. Time complexity of the different steps of the attack on 25-round T-TWINE-80, where NK denotes the number of keys to be excluded.

| Step | Time complexity (in 25-round encryptions) | NK | $m = 33.5$ |
|------|------------------------------------------|----|-----------|
| 1    | $2^{m+1.881} \times (16/7) \times \frac{3}{8 \times 25} \approx 2^{m-2.985}$ | $(16/7)$ | $2^{30.515}$ |
| 2    | $2^{m+1.881} \times (16/7)^2 \times \frac{3}{8 \times 25} \approx 2^{m-1.793}$ | $(16/7)^2$ | $2^{31.707}$ |
| 3    | $2^{m+1.881} \times (16/7)^3 \times \frac{4}{8 \times 25} \approx 2^{m-0.185}$ | $(16/7)^3$ | $2^{33.315}$ |
| 4    | $2^{m+1.881} \times 2^4 \times (16/7)^4 \times \frac{4}{8 \times 25} \approx 2^{m+5.008}$ | $2^4 \times (16/7)^4$ | $2^{38.508}$ |
| 5    | $2^{m+1.881} \times 2^5 \times (16/7)^5 \times \frac{2}{8 \times 25} \approx 2^{m+9.200}$ | $2^8 \times (16/7)^5$ | $2^{42.700}$ |
| 6    | $2^{m+1.881} \times 2^{12} \times (16/7)^6 \times \frac{5}{8 \times 25} \approx 2^{m+15.715}$ | $2^{12} \times (16/7)^6$ | $2^{49.215}$ |
| 7    | $2^{m+1.881} \times 2^{16} \times (16/7)^7 \times \frac{4}{8 \times 25} \approx 2^{m+20.586}$ | $2^{16} \times (16/7)^7$ | $2^{54.086}$ |
| 8    | $2^{m+1.881} \times 2^{16} \times (16/7)^8 \times \frac{1}{8 \times 25} \approx 2^{m+19.778}$ | $2^{16} \times (16/7)^8$ | $2^{53.278}$ |
| 9    | $2^{m+1.881} \times 2^{16} \times (16/7)^9 \times \frac{3}{8 \times 25} \approx 2^{m+22.556}$ | $2^{16} \times (16/7)^9$ | $2^{56.056}$ |
| 10   | $2^{m+1.881} \times 2^{20} \times (16/7)^{10} \times \frac{4}{8 \times 25} \approx 2^{m+28.164}$ | $2^{20} \times (16/7)^{11}$ | $2^{61.664}$ |
| 11   | $2^{m+1.881} \times 2^{28} \times (16/7)^{11} \times \frac{3}{8 \times 25} \approx 2^{m+36.941}$ | $2^{28} \times (16/7)^{11}$ | $2^{70.441}$ |
| 12   | $2^{m+1.881} \times 2^{28} \times (16/7)^{11} \times \frac{1}{8 \times 25} \approx 2^{m+35.356}$ | $2^{28} \times (16/7)^{11}$ | $2^{68.856}$ |
A 18-round Impossible Differential Characteristic as Depicted in Figure 8 of [15]

![Diagram of 18-round impossible differential characteristic](image)

**Fig. 5.** 18-round impossible differential characteristic as depicted in Figure 8 of [15] with our comments.

References

1. Avanzi, R.: The QARMA block cipher family. Almost MDS matrices over rings with zero divisors, nearly symmetric even-mansour constructions with non-involuntary central rounds, and search heuristics for low-latency S-boxes. IACR Trans. Symmetric Cryptol. 4–44 (2017)

2. Beierle, C., et al.: The SKINNY family of block ciphers and its low-latency variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9815, pp. 123–153. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53008-5_5

3. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_2
4. Ferguson, N., et al.: The SKEIN hash function family (2010). http://www.skeinhash.info

5. Goldenberg, D., Hohenberger, S., Liskov, M., Schwartz, E.C., Seyalioglu, H.: On tweaking Luby-Rackoff blockciphers. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 342–356. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_21

6. Jean, J., Nikolić, I., Peyrin, T.: Tweaks and keys for block ciphers: the TWEAK framework. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 274–288. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45608-8_15

7. Jean, J., Nikolić, I., Peyrin, T., Seurin, Y.: Deoxys v1.41. Submitted to CAESAR Competition (2016). https://competitions.cr.yp.to/round3/deoxysv141.pdf

8. Knudsen, L.: DEAL: a 128-bit block cipher. Complexity 258(2), 216 (1998). NIST AES Proposal

9. Lampe, R., Seurin, Y.: Tweakable blockciphers with asymptotically optimal security. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 133–151. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43933-3_8

10. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable blockciphers with beyond birthday-bound security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_2

11. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. J. Cryptol. 24(3), 588–613 (2010)

12. Mitsuda, A., Iwata, T.: Tweakable pseudorandom permutation from generalized feistel structure. In: Baek, J., Bao, F., Chen, K., Lai, X. (eds.) ProvSec 2008. LNCS, vol. 5324, pp. 22–37. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-88733-1_2

13. Nyberg, K.: Generalized feistel networks. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 91–104. Springer, Heidelberg (1996). https://doi.org/10.1007/BFb0034838

14. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30539-2_2

15. Sakamoto, K., et al.: Tweakable TWINE: building a tweakable block cipher on generalized feistel structure. In: Attrapadung, N., Yagi, T. (eds.) IWSEC 2019. LNCS, vol. 11689, pp. 129–145. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-26834-3_8

16. Schroeppel, R.: An overview of the hasty pudding cipher (1998). http://www.cs.arizona.edu/rcs/hpc

17. Suzuki, T., Minematsu, K.: Improving the generalized feistel. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 19–39. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13858-4_2

18. Suzuki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: a lightweight block cipher for multiple platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 339–354. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-35999-6_22
19. Zheng, X., Jia, K.: Impossible differential attack on reduced-round TWINE. In: Lee, H.-S., Han, D.-G. (eds.) ICISC 2013. LNCS, vol. 8565, pp. 123–143. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-12160-4_8

20. Zheng, Y., Matsumoto, T., Imai, H.: Impossibility and optimality results on constructing pseudorandom permutations. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 412–422. Springer, Heidelberg (1990). https://doi.org/10.1007/3-540-46885-4_41